Dateizugriff mit SMB verwalten

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/local-users-groups-concepts-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Dateizugriff mit SMB verwalten . . . 1
Lokale Benutzer und Gruppen für Authentifizierung und Autorisierung verwenden . . . 1
Informationen zu lokalen ONTAP SMB-Benutzern und -Gruppen . . . 1
Informationen zur lokalen ONTAP SMB-Benutzerauthentifizierung . . . 3
Die Auswirkungen der Löschung von ONTAP SMB-Servern auf Benutzer und Gruppen . . . 4
Die Verwendung der Microsoft Management Console mit lokalen ONTAP SMB-Benutzern und -Gruppen wird erläutert. . . . 4
Informationen zur Verwendung von SnapMirror auf ONTAP SMB SVMs, die lokale Gruppen enthalten . . . 5
Erfahren Sie mehr über ONTAP SMB-Berechtigungen . . . 5
Informationen zu BUILTIN Gruppen und lokalen Administrator Konten auf ONTAP SMB Servern . . . 6
Anforderungen an lokale ONTAP SMB-Benutzerpasswörter . . . 6
Vordefinierte BUILTIN Gruppen und standardmäßige ONTAP SMB-Berechtigungen . . . 7
Aktivieren oder Deaktivieren der lokalen ONTAP SMB-Benutzer- und Gruppenfunktionalität . . . 8
Lokale ONTAP SMB-Benutzerkonten verwalten . . . 11
Lokale ONTAP SMB-Gruppen verwalten . . . 14
Berechtigungen für ONTAP SMB lokale oder Domänenbenutzer oder -gruppen verwalten . . . 21
Umgehungsüberprüfung konfigurieren . . . 25
Informationen zur Konfiguration der ONTAP SMB Bypass Traverse-Prüfung . . . 25
Benutzern oder Gruppen erlauben, die ONTAP SMB-Verzeichnisdurchlaufprüfung zu umgehen . . . 26
Benutzern oder Gruppen das Umgehen der ONTAP SMB-Verzeichnisdurchlaufprüfung untersagen . . . 27
Informationen zu Dateisicherheit und Überwachungsrichtlinien . . . 28
Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien . . . 28
Informationen zur ONTAP SMB-Dateisicherheit auf NTFS Security-Style-Volumes anzeigen . . . 29
Informationen zur ONTAP SMB-Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen . . . 35
Informationen zur ONTAP SMB-Dateisicherheit auf UNIX Security-Style-Volumes anzeigen . . . 38
ONTAP Befehle zur Anzeige von Informationen über NTFS-Überwachungsrichtlinien auf SMB FlexVol Volumes . . . 40
ONTAP Befehle zur Anzeige von Informationen zu NFSv4-Überwachungsrichtlinien auf SMB FlexVol volumes . . . 42
Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien . . . 44
NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und Storage-Level Access Guard auf SVMs mithilfe der CLI verwalten . . . 46
ONTAP Befehle zur Verwaltung der SMB NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und des Storage-Level Access Guard . . . 46
ONTAP Befehle zum Festlegen der SMB-Datei- und Ordnersicherheit . . . 47
Informationen zu den Grenzen bei der Verwendung von ONTAP Befehlen zum Festlegen der SMB-Datei- und Ordnersicherheit . . . 48
Sicherheitsdeskriptoren werden verwendet, um die ONTAP SMB Datei- und Ordnersicherheit anzuwenden. . . . 48
Informationen zur Anwendung von Dateiverzeichnisrichtlinien, die lokale SMB-Benutzer oder -Gruppen auf dem ONTAP SVM Disaster Recovery-Ziel verwenden . . . 49
Dateisicherheit für NTFS-Dateien und Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden . . . 51

Erstellen von NTFS-Sicherheitsdeskriptoren auf ONTAP SMB Servern . . . 51
NTFS-DACL-Zugriffssteuerungseinträge zu den NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern hinzufügen . . . 52
ONTAP SMB Sicherheitsrichtlinien erstellen . . . 53
Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen . . . 54
ONTAP SMB-Sicherheitsrichtlinien anwenden . . . 56
ONTAP SMB-Sicherheitsrichtlinienaufträge überwachen . . . 56
Die Sicherheit von ONTAP SMB-Dateien überprüfen . . . 57
Überwachungsrichtlinien für NTFS-Dateien und -Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden . . . 60
ONTAP Befehle zum Konfigurieren und Anwenden von SMB-Überwachungsrichtlinien auf NTFS-Dateien und Ordner . . . 60
Erstellen von NTFS-Sicherheitsdeskriptoren auf ONTAP SMB Servern . . . 61
NTFS-SACL-Zugriffssteuerungseinträge zu den NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern hinzufügen . . . 62
ONTAP SMB Sicherheitsrichtlinien erstellen . . . 63
Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen . . . 64
ONTAP SMB-Sicherheitsrichtlinien anwenden . . . 65
ONTAP SMB-Sicherheitsrichtlinienaufträge überwachen . . . 66
ONTAP SMB Auditrichtlinien überprüfen . . . 67
Informationen zur Verwaltung von ONTAP SMB-Sicherheitsrichtlinienjobs . . . 68
ONTAP Befehle zur Verwaltung von NTFS- und SMB-Sicherheitsrichtlinien und Zugriffskontrolleinträgen . . . 68
ONTAP Befehle zur Verwaltung von NTFS-Sicherheitsdeskriptoren auf SMB-Servern . . . 68
ONTAP Befehle zur Verwaltung von NTFS DACL-Zugriffskontrolleinträgen auf SMB-Servern . . . 69
ONTAP Befehle zur Verwaltung von NTFS SACL-Zugriffskontrolleinträgen auf SMB-Servern . . . 69
ONTAP Befehle zur Verwaltung von SMB-Sicherheitsrichtlinien . . . 70
ONTAP Befehle zur Verwaltung von SMB-Sicherheitsrichtlinienaufgaben . . . 70
ONTAP Befehle zur Verwaltung von SMB Security Policy Jobs . . . 70
Den Metadatencache für SMB-Freigaben konfigurieren . . . 71
Der ONTAP SMB-Metadaten-Cache kann aktiviert werden. . . . 71
Die Lebensdauer von ONTAP SMB Metadaten-Cache-Einträgen konfigurieren . . . 72
Dateisperren verwalten . . . 72
Informationen zur ONTAP SMB-Dateisperrung zwischen Protokollen . . . 72
Informationen zu schreibgeschützten Bits in ONTAP SMB . . . 73
Wie ONTAP sich von Windows bei der Handhabung von Sperren auf freigegebenen Pfadkomponenten unterscheidet . . . 74
Informationen zu ONTAP SMB-Sperren anzeigen . . . 75
ONTAP SMB-Sperren aufheben . . . 77
SMB-Aktivitäten überwachen . . . 78
ONTAP SMB-Sitzungsinformationen anzeigen . . . 78
Informationen zu geöffneten ONTAP SMB-Dateien . . . 81
Festgestellt werden kann, welche Statistiken, Objekte und Zähler auf ONTAP SMB-Servern verfügbar sind. . . . 84
ONTAP SMB Statistiken anzeigen . . . 86

Dateizugriff mit SMB verwalten

Lokale Benutzer und Gruppen für Authentifizierung und Autorisierung verwenden

Informationen zu lokalen ONTAP SMB-Benutzern und -Gruppen

Es ist hilfreich, vor der Entscheidung, ob lokale Benutzer und Gruppen in Ihrer Umgebung konfiguriert und verwendet werden, zu wissen, was lokale Benutzer und Gruppen sind und einige grundlegende Informationen darüber zu kennen.

- **Lokaler Benutzer**

  Ein Benutzerkonto mit einer eindeutigen Sicherheitskennung (SID), das nur auf der Storage Virtual Machine (SVM) sichtbar ist, auf der es erstellt wurde. Lokale Benutzerkonten verfügen über eine Reihe von Attributen, darunter Benutzername und SID. Ein lokales Benutzerkonto authentifiziert sich lokal auf dem CIFS-Server mithilfe von NTLM-Authentifizierung.

  Benutzerkonten haben verschiedene Verwendungszwecke:

  - Wird verwendet, um einem Benutzer *User Rights Management*-Berechtigungen zu gewähren.
  - Dient zur Steuerung des Share-Level- und des Zugriffs auf Dateiebene auf Datei- und Ordnerressourcen, die sich im Besitz der SVM befinden.

- **Lokale Gruppe**

  Eine Gruppe mit einer eindeutigen SID ist nur auf der SVM sichtbar, auf der sie erstellt wurde. Gruppen enthalten eine Reihe von Mitgliedern. Mitglieder können lokale Benutzer, Domänenbenutzer, Domänengruppen und Domänencomputerkonten sein. Gruppen können erstellt, geändert oder gelöscht werden.

  Gruppen haben verschiedene Einsatzmöglichkeiten:

  - Wird verwendet, um Mitgliedern *User Rights Management*-Berechtigungen zu gewähren.
  - Dient zur Steuerung des Share-Level- und des Zugriffs auf Dateiebene auf Datei- und Ordnerressourcen, die sich im Besitz der SVM befinden.

- **Lokale Domäne**

  Eine Domäne mit lokalem Geltungsbereich, die durch die SVM begrenzt ist. Der Name der lokalen Domäne ist der CIFS-Servername. Lokale Benutzer und Gruppen sind innerhalb der lokalen Domäne enthalten.

- **Sicherheitskennung (SID)**

  Eine SID ist ein numerischer Wert variabler Länge, der Sicherheitsprinzipale im Windows-Stil identifiziert. Beispielsweise hat eine typische SID 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 auf jedem Knoten eines Clusters. Lokale Benutzer- und Gruppenobjekte werden in der RDB gespeichert.

Gründe für die Erstellung lokaler ONTAP SMB Benutzer und lokaler Gruppen

Es gibt mehrere Gründe für die Erstellung lokaler Benutzer und lokaler Gruppen auf Ihrer Storage Virtual Machine (SVM). Beispielsweise ist der Zugriff auf einen SMB-Server über ein lokales Benutzerkonto möglich, wenn die Domänencontroller (DCs) nicht verfügbar sind, lokale Gruppen können zur Zuweisung von Berechtigungen genutzt werden, oder der SMB-Server befindet sich in einer Arbeitsgruppe.

Aus folgenden Gründen kann ein oder mehrere lokale Benutzerkonten erstellt werden:

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

  In Arbeitsgruppenkonfigurationen sind lokale Benutzer erforderlich.

- Es soll möglich sein, sich beim SMB-Server zu authentifizieren und anzumelden, falls die Domänencontroller nicht verfügbar sind.

  Lokale Benutzer können sich beim SMB-Server mittels NTLM-Authentifizierung anmelden, wenn der Domänencontroller ausgefallen ist oder wenn Netzwerkprobleme verhindern, dass der SMB-Server den Domänencontroller kontaktiert.

- Es besteht der Wunsch, einem lokalen Benutzer die Berechtigungen für die *User Rights Management* -Verwaltung zuzuweisen.

  User Rights Management ist die Fähigkeit eines SMB-Serveradministrators, die Rechte von Benutzern und Gruppen auf der SVM zu steuern. Sie können einem Benutzer Berechtigungen zuweisen, indem Sie die Berechtigungen dem Benutzerkonto zuweisen oder den Benutzer einer lokalen Gruppe hinzufügen, die über diese Berechtigungen verfügt.

Aus folgenden Gründen kann eine oder mehrere lokale Gruppen erstellt werden:

- 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 der Zugriffsrechte lokaler Arbeitsgruppenbenutzer nützlich sein.

- Der Zugriff auf Datei- und Ordnerressourcen soll mithilfe lokaler Gruppen für die Freigabe- und Zugriffskontrolle auf Dateiebene gesteuert werden.
- Es besteht der Wunsch, lokale Gruppen mit individuell angepassten *User Rights Management* -Berechtigungen zu erstellen.

  Einige integrierte Benutzergruppen verfügen über vordefinierte Berechtigungen. Um eine benutzerdefinierte Gruppe von Berechtigungen zuzuweisen, kann eine lokale Gruppe erstellt und mit den erforderlichen Berechtigungen versehen werden. Lokale Benutzer, Domänenbenutzer und Domänengruppen können anschließend zu der lokalen Gruppe hinzugefügt werden.

Verwandte Informationen

- Informationen zur lokalen Benutzerauthentifizierung
- Liste der unterstützten Berechtigungen

Informationen zur lokalen ONTAP SMB-Benutzerauthentifizierung

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

Da SMB sitzungsbasiert ist, kann die Identität des Benutzers nur einmalig beim ersten Sitzungsaufbau ermittelt werden. Der CIFS-Server verwendet NTLM-basierte Authentifizierung bei der Authentifizierung lokaler Benutzer. Sowohl NTLMv1 als auch NTLMv2 werden unterstützt.

ONTAP verwendet die lokale Authentifizierung in drei Anwendungsfällen. Jeder Anwendungsfall hängt davon ab, ob der Domänenteil des Benutzernamens (im Format DOMAIN\user) mit dem lokalen Domänennamen des CIFS-Servers (dem CIFS-Servernamen) übereinstimmt:

- Der Domänenteil stimmt überein

  Benutzer, die bei der Anforderung des Datenzugriffs lokale Benutzeranmeldeinformationen angeben, werden lokal auf dem CIFS-Server authentifiziert.

- Der Domänenteil stimmt nicht überein

  ONTAP versucht, die NTLM-Authentifizierung mit einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört, durchzuführen. Bei erfolgreicher Authentifizierung ist die Anmeldung abgeschlossen. Wenn die Authentifizierung nicht erfolgreich ist, hängt das weitere Vorgehen davon ab, warum die Authentifizierung nicht erfolgreich war.

  Existiert der Benutzer beispielsweise in Active Directory, das Passwort ist jedoch ungültig oder abgelaufen, versucht ONTAP nicht, das entsprechende lokale Benutzerkonto auf dem CIFS-Server zu verwenden. Stattdessen schlägt die Authentifizierung fehl. Es gibt weitere Fälle, in denen ONTAP das entsprechende lokale Konto auf dem CIFS-Server für die Authentifizierung verwendet, sofern es existiert, auch wenn die NetBIOS-Domänennamen nicht übereinstimmen. Existiert beispielsweise ein passendes Domänenkonto, ist dieses jedoch deaktiviert, verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server für die Authentifizierung.

- Der Domänenteil ist nicht angegeben

  ONTAP versucht zunächst die Authentifizierung als lokaler Benutzer. Schlägt die Authentifizierung als lokaler Benutzer fehl, authentifiziert ONTAP den Benutzer bei einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört.

Nach erfolgreicher lokaler oder Domänen-Benutzerauthentifizierung erstellt ONTAP ein vollständiges Benutzerzugriffstoken, das die lokale Gruppenzugehörigkeit und Berechtigungen berücksichtigt.

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

Verwandte Informationen

Lokale Benutzerauthentifizierung auf Servern aktivieren oder deaktivieren

Informationen zu ONTAP SMB-Benutzerzugriffstoken

Wenn ein Benutzer eine Freigabe zuordnet, wird eine authentifizierte SMB-Sitzung hergestellt und ein Benutzerzugriffstoken erstellt, das Informationen über den Benutzer, die Gruppenzugehörigkeit des Benutzers und seine kumulativen Berechtigungen sowie den zugeordneten UNIX-Benutzer enthält.

Sofern diese Funktion nicht deaktiviert ist, werden dem Benutzerzugriffstoken auch lokale Benutzer- und

Gruppeninformationen hinzugefügt. Die Art, wie Zugriffstoken erstellt werden, hängt davon ab, ob die Anmeldung für einen lokalen Benutzer oder einen Active Directory-Domänenbenutzer erfolgt:

- Lokale Benutzeranmeldung

  Obwohl lokale Benutzer Mitglieder verschiedener lokaler Gruppen sein können, können lokale Gruppen nicht Mitglieder anderer lokaler Gruppen sein. Das Zugriffstoken eines lokalen Benutzers setzt sich aus der Vereinigung aller Berechtigungen zusammen, die den Gruppen zugewiesen sind, denen der jeweilige lokale Benutzer angehört.

- Domänenbenutzeranmeldung

  Wenn sich ein Domänenbenutzer anmeldet, erhält ONTAP ein Benutzerzugriffstoken, das die Benutzer-SID und die SIDs aller Domänengruppen enthält, denen der Benutzer angehört. ONTAP verwendet die Vereinigung des Domänenbenutzerzugriffstokens mit dem Zugriffstoken, das durch lokale Mitgliedschaften der Domänengruppen des Benutzers bereitgestellt wird (sofern vorhanden), sowie alle direkt dem Domänenbenutzer oder einer seiner Domänengruppenmitgliedschaften zugewiesenen Berechtigungen.

Sowohl für die lokale als auch für die Domänenbenutzeranmeldung wird die primäre Gruppen-RID für das Benutzerzugriffstoken festgelegt. Die Standard-RID ist `Domain Users` (RID 513). Die Standardeinstellung kann nicht geändert werden.

Der Namenszuordnungsprozess zwischen Windows und UNIX sowie zwischen UNIX und Windows folgt für lokale und Domänenkonten denselben Regeln.

> Es gibt keine implizite, automatische Zuordnung eines UNIX-Benutzers zu einem lokalen Konto. Wenn dies erforderlich ist, muss eine explizite Zuordnungsregel mit den vorhandenen Namenszuordnungsbefehlen angegeben werden.

Die Auswirkungen der Löschung von ONTAP SMB-Servern auf Benutzer und Gruppen

Die Standardmenge an lokalen Benutzern und Gruppen wird bei der Erstellung eines CIFS-Servers angelegt und der Storage Virtual Machine (SVM) zugeordnet, die den CIFS-Server hostet. SVM-Administratoren können lokale Benutzer und Gruppen jederzeit erstellen. Es sollte beachtet werden, was mit den lokalen Benutzern und Gruppen geschieht, wenn der CIFS-Server gelöscht wird.

Lokale Benutzer und Gruppen sind SVMs zugeordnet, daher werden sie aus Sicherheitsgründen beim Löschen von CIFS-Servern nicht gelöscht. Obwohl lokale Benutzer und Gruppen beim Löschen des CIFS-Servers nicht gelöscht werden, sind sie ausgeblendet. Lokale Benutzer und Gruppen können erst wieder angezeigt oder verwaltet werden, nachdem ein CIFS-Server auf der SVM neu erstellt wurde.

> Der administrative Status des CIFS-Servers hat keinen Einfluss auf die Sichtbarkeit lokaler Benutzer oder Gruppen.

Die Verwendung der Microsoft Management Console mit lokalen ONTAP SMB-Benutzern und -Gruppen wird erläutert.

Informationen zu lokalen Benutzern und Gruppen können in der Microsoft Management Console angezeigt werden. Mit dieser Version von ONTAP ist es nicht möglich, andere

Verwaltungsaufgaben für lokale Benutzer und Gruppen über die Microsoft Management Console durchzuführen.

Informationen zur Verwendung von SnapMirror auf ONTAP SMB SVMs, die lokale Gruppen enthalten

Es sind die Richtlinien zu beachten, wenn SnapMirror auf Volumes konfiguriert wird, die SVMs gehören und lokale Gruppen enthalten.

Lokale Gruppen können nicht in ACEs verwendet werden, die auf Dateien, Verzeichnisse oder Freigaben angewendet werden, die von SnapMirror auf eine andere SVM repliziert werden. Wenn die SnapMirror Funktion verwendet wird, um ein DR-Mirror für ein Volume auf einer anderen SVM zu erstellen und das Volume eine ACE für eine lokale Gruppe enthält, ist die ACE auf dem Mirror ungültig. Wenn Daten auf eine andere SVM repliziert werden, gelangen die Daten effektiv in eine andere lokale Domäne. Die Berechtigungen, die lokalen Benutzern und Gruppen gewährt werden, sind nur innerhalb des Gültigkeitsbereichs der SVM gültig, auf der sie ursprünglich erstellt wurden.

Erfahren Sie mehr über ONTAP SMB-Berechtigungen

Sie können Berechtigungen direkt lokalen Benutzern oder Domänenbenutzern zuweisen. Alternativ können Benutzer lokalen Gruppen zugeordnet werden, deren Berechtigungen den gewünschten Benutzerfunktionen entsprechen.

- Sie können einer von Ihnen erstellten Gruppe eine Reihe von Berechtigungen zuweisen.

  Anschließend wird ein Benutzer zu der Gruppe hinzugefügt, die über die Berechtigungen verfügt, die dieser Benutzer erhalten soll.

- Sie können außerdem lokale Benutzer und Domänenbenutzer vordefinierten Gruppen zuordnen, deren Standardberechtigungen den Berechtigungen entsprechen, die Sie diesen Benutzern gewähren möchten.

Verwandte Informationen

- Berechtigungen für lokale oder Domänenbenutzer oder Gruppen hinzufügen, entfernen oder zurücksetzen
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung

Liste der unterstützten ONTAP SMB Berechtigungen

ONTAP verfügt über einen vordefinierten Satz unterstützter Berechtigungen. Bestimmten vordefinierten lokalen Gruppen sind einige dieser Berechtigungen standardmäßig zugewiesen. Es besteht außerdem die Möglichkeit, Berechtigungen zu den vordefinierten Gruppen hinzuzufügen oder zu entfernen oder neue lokale Benutzer oder Gruppen zu erstellen und den von Ihnen erstellten Gruppen oder bestehenden Domänenbenutzern und -gruppen Berechtigungen zuzuweisen.

Die folgende Tabelle listet die unterstützten Berechtigungen auf der Storage Virtual Machine (SVM) auf und enthält eine Liste der BUILTIN-Gruppen mit zugewiesenen Berechtigungen:

Berechtigungsname	Standard-Sicherheitseinstellung	Beschreibung
`SeTcbPrivilege`	Keine	Als Teil des Betriebssystems
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Dateien und Verzeichnisse sichern und dabei alle ACLs überschreiben

Berechtigungsname	Standard-Sicherheitseinstellung	Beschreibung
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Dateien und Verzeichnisse wiederherstellen und dabei alle ACLs überschreiben. Eine gültige Benutzer- oder Gruppen-SID als Dateibesitzer festlegen
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Besitz von Dateien oder anderen Objekten übernehmen
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Auditierung verwalten Dies umfasst das Anzeigen, Sichern und Löschen des Sicherheitsprotokolls.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Umgehung der Traversierungsprüfung Benutzer mit dieser Berechtigung benötigen keine Traverse-(x)-Berechtigungen, um Ordner, Symlinks oder Junctions zu durchlaufen.

Verwandte Informationen

- Informationen zur Zuweisung von Berechtigungen
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung

Informationen zu BUILTIN Gruppen und lokalen Administrator Konten auf ONTAP SMB Servern

Bestimmte Richtlinien sind zu beachten, wenn integrierte Gruppen und das lokale Administratorkonto verwendet werden. Beispielsweise kann das lokale Administratorkonto umbenannt, jedoch nicht gelöscht werden.

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

  Nach der Umbenennung der BUILTIN-Gruppe kann ein weiteres lokales Objekt mit dem bekannten Namen erstellt werden; dem Objekt wird jedoch eine neue RID zugewiesen.

- Es existiert kein lokales Gastkonto.

Verwandte Informationen

Vordefinierte BUILTIN Gruppen und Standardberechtigungen

Anforderungen an lokale ONTAP SMB-Benutzerpasswörter

Standardmäßig müssen Passwörter lokaler Benutzer die Komplexitätsanforderungen erfüllen. Die Anforderungen an die Passwortkomplexität ähneln den in der Microsoft

Windows *Lokalen Sicherheitsrichtlinie* definierten Anforderungen.

Das Passwort muss folgende Kriterien erfüllen:

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

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

Verwandte Informationen

- Passwortkomplexität für lokale Benutzer konfigurieren
- Informationen zu den Server-Sicherheitseinstellungen
- Passwörter lokaler Benutzerkonten ändern

Vordefinierte BUILTIN Gruppen und standardmäßige ONTAP SMB-Berechtigungen

Sie können einem lokalen Benutzer oder Domänenbenutzer die Mitgliedschaft in einer vordefinierten Gruppe von BUILTIN-Gruppen zuweisen, die von ONTAP bereitgestellt werden. Vordefinierte Gruppen haben vordefinierte Berechtigungen zugewiesen.

Die folgende Tabelle beschreibt die vordefinierten Gruppen:

Vordefinierte BUILTIN Gruppe	Standardberechtigungen
`BUILTIN\Administrators`RID 544 Wenn das lokale `Administrator` Konto mit einer RID von 500 erstmals erstellt wird, wird es automatisch Mitglied dieser Gruppe. Wenn die Storage Virtual Machine (SVM) einer Domäne beitritt, wird die `domain\Domain Admins` Gruppe zur Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird die `domain\Domain Admins` Gruppe aus der Gruppe entfernt.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`

Vordefinierte BUILTIN Gruppe	Standardberechtigungen
`BUILTIN\Power Users`RID 547 Diese Gruppe hat bei ihrer Erstellung keine Mitglieder. Mitglieder dieser Gruppe weisen die folgenden Merkmale auf: • Kann lokale Benutzer und Gruppen erstellen und verwalten. • Kann sich selbst oder andere Objekte nicht zur `BUILTIN\Administrators` Gruppe hinzufügen.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 Diese Gruppe hat bei ihrer Erstellung keine Mitglieder. Mitglieder dieser Gruppe können die Lese- und Schreibberechtigungen für Dateien oder Ordner überschreiben, wenn sie mit Backup-Absicht geöffnet werden.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Diese Gruppe hat nach ihrer Erstellung keine Mitglieder (abgesehen von der impliziten `Authenticated Users` Sondergruppe). Wenn die SVM einer Domäne beitritt, wird die `domain\Domain Users` Gruppe zu dieser Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird die `domain\Domain Users` Gruppe aus dieser Gruppe entfernt.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Diese Gruppe umfasst alle Benutzer, einschließlich Gäste (jedoch keine anonymen Benutzer). Es handelt sich um eine implizite Gruppe mit impliziter Mitgliedschaft.	`SeChangeNotifyPrivilege`

Verwandte Informationen

- Informationen zu BUILTIN Gruppen und lokalen Administrator Konten auf Servern
- Liste der unterstützten Berechtigungen
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung

Aktivieren oder Deaktivieren der lokalen ONTAP SMB-Benutzer- und Gruppenfunktionalität

Bevor Sie lokale Benutzer und Gruppen für die Zugriffskontrolle von NTFS-Sicherheitsstil-Daten verwenden können, muss die Funktionalität für lokale Benutzer und Gruppen aktiviert sein. Zusätzlich muss die Funktionalität für die lokale Benutzerauthentifizierung aktiviert sein, wenn lokale Benutzer für die SMB-Authentifizierung verwendet werden sollen.

Die Funktionen für lokale Benutzer und Gruppen sowie die lokale Benutzerauthentifizierung sind standardmäßig aktiviert. Falls sie nicht aktiviert sind, müssen sie aktiviert werden, bevor lokale Benutzer und Gruppen konfiguriert und verwendet werden können. Die Funktionen für lokale Benutzer und Gruppen können jederzeit deaktiviert werden.

Zusätzlich zur expliziten Deaktivierung der lokalen Benutzer- und Gruppenfunktionalität deaktiviert ONTAP die lokale Benutzer- und Gruppenfunktionalität auch, wenn ein Knoten im Cluster auf eine ONTAP Version zurückgesetzt wird, die diese Funktionalität nicht unterstützt. Die lokale Benutzer- und Gruppenfunktionalität ist erst aktiviert, wenn auf allen Knoten im Cluster eine Version von ONTAP ausgeführt wird, die sie unterstützt.

Verwandte Informationen

- Lokale Benutzerkonten ändern
- Lokale Gruppen ändern
- Berechtigungen für lokale oder Domänenbenutzer oder -gruppen hinzufügen

Lokale Benutzer und Gruppen auf ONTAP SMB-Servern aktivieren oder deaktivieren

Sie können lokale Benutzer und Gruppen für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Die Funktionalität für lokale Benutzer und Gruppen ist standardmäßig aktiviert.

Über diese Aufgabe

Sie können lokale Benutzer und Gruppen bei der Konfiguration von SMB-Freigaben und NTFS-Dateiberechtigungen verwenden und optional lokale Benutzer für die Authentifizierung beim Erstellen einer SMB-Verbindung nutzen. Um lokale Benutzer für die Authentifizierung zu verwenden, muss außerdem die Option zur Authentifizierung lokaler Benutzer und Gruppen aktiviert werden.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Lokale Benutzer und Gruppen aktivieren oder deaktivieren:
   - Lokale Benutzer und Gruppen aktivieren:

```
vserver cifs options modify -vserver <SVM_name> -is-local-users-and
-groups-enabled true
```

   - Lokale Benutzer und Gruppen deaktivieren:

```
vserver cifs options modify -vserver <SVM_name> -is-local-users-and
-groups-enabled false
```

3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Beispiel

Das folgende Beispiel aktiviert die Funktionalität für lokale Benutzer und Gruppen 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

- Lokale Benutzerkonten verwalten == Lokale Benutzerauthentifizierung auf ONTAP SMB-Servern aktivieren oder deaktivieren

Sie können die lokale Benutzerauthentifizierung für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Standardmäßig ist die lokale Benutzerauthentifizierung erlaubt, was nützlich ist, wenn die SVM keinen Domänencontroller erreichen kann oder wenn keine Zugriffskontrollen auf Domänenebene verwendet werden.

Bevor Sie beginnen

Die Funktionalität für lokale Benutzer und Gruppen muss auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Sie können die lokale Benutzerauthentifizierung jederzeit aktivieren oder deaktivieren. Wenn Sie lokale Benutzer für die Authentifizierung beim Erstellen einer SMB-Verbindung verwenden möchten, muss außerdem die Option „Lokale Benutzer und Gruppen“ des CIFS-Servers aktiviert werden.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Lokale Benutzerauthentifizierung aktivieren oder deaktivieren:
   - Lokale Benutzerauthentifizierung aktivieren:

     ```
     vserver cifs options modify -vserver <SVM_name> -is-local-auth
     -enabled true
     ```

   - Lokale Benutzerauthentifizierung deaktivieren:

     ```
     vserver cifs options modify -vserver <SVM_name> -is-local-auth
     ```

```
-enabled false
```

3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Beispiel

Das folgende Beispiel aktiviert 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

- Informationen zur lokalen Benutzerauthentifizierung
- Lokale Benutzer und Gruppen auf Servern aktivieren oder deaktivieren

Lokale ONTAP SMB-Benutzerkonten verwalten

Sie können ein lokales Benutzerkonto aktivieren, um den Zugriff auf SVM-Daten über SMB zu ermöglichen, oder das Konto deaktivieren, um den Zugriff zu verhindern. Sie können das Konto auch bearbeiten, um den vollständigen Namen, die Beschreibung oder den Aktivierungsstatus des Benutzers zu aktualisieren. Bei Bedarf können Sie das Konto aus administrativen Gründen umbenennen, beispielsweise bei einem kompromittierten Benutzernamen. Sie können außerdem die lokalen Gruppen anzeigen, denen ein Benutzer angehört, was hilft, den Datei- und Ordnerzugriff zu ermitteln und Zugriffsprobleme zu beheben.

Wenn Sie möchten…	Geben Sie den Befehl ein…
Ändern Sie das Passwort des lokalen Benutzers	`vserver cifs users-and-groups local-user set-password -vserver <SVM_name> -user-name <user_name>`
Lokales Benutzerkonto aktivieren oder deaktivieren	`vserver cifs users-and-groups local-user modify -vserver <SVM_name> -user-name <user_name> -is-account-disabled {true`
false}`	Detaillierte Kontoinformationen für einen Benutzer anzeigen

Wenn Sie möchten…	Geben Sie den Befehl ein…
`vserver cifs users-and-groups local-user show -instance -vserver <SVM_name> -user-name <user_name>`	Informationen zur lokalen Benutzermitgliedschaft für einen bestimmten lokalen Benutzer anzeigen
`vserver cifs users-and-groups local-user show-membership -user-name <user_name>`	Anzeige der Mitgliedschaftsinformationen des lokalen Benutzers für die lokale Gruppe, der dieser lokale Benutzer angehört
`vserver cifs users-and-groups local-user show-membership -membership` *group_name*	Benutzermitgliedschaftsinformationen für lokale Benutzer, die einer bestimmten Storage Virtual Machine (SVM) zugeordnet sind, anzeigen
`vserver cifs users-and-groups local-user show-membership -vserver <SVM_name>`	Detaillierte Informationen zu allen lokalen Benutzern auf einer bestimmten SVM
`vserver cifs users-and-groups local-user show-membership -instance -vserver <SVM_name>`	Informationen zu allen Benutzern auf der Storage Virtual Machine (SVM) anzeigen
`vserver cifs users-and-groups local-user show -vserver <SVM_name>`	Die Beschreibung des lokalen Benutzers ändern
`vserver cifs users-and-groups local-user modify -vserver <SVM_name> -user -name <user_name> -description text` Enthält die Beschreibung ein Leerzeichen, so muss sie in doppelte Anführungszeichen gesetzt werden.	Den vollständigen Namen des lokalen Benutzers anpassen
`vserver cifs users-and-groups local-user modify -vserver <SVM_name> -user -name <user_name> -full-name text` Enthält der vollständige Name ein Leerzeichen, so muss er in doppelte Anführungszeichen gesetzt werden.	Das lokale Benutzerkonto umbenennen

Beispiel

Im folgenden Beispiel wird der lokale Benutzer “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1 in “CIFS_SERVER\sue_new” umbenannt:

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

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
```

Beispiel

Im folgenden Beispiel wird das Passwort für den lokalen Benutzer “CIFS_SERVER\sue” festgelegt, der der Storage Virtual Machine (SVM, früher bekannt als Vserver) vs1 zugeordnet 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:
```

Beispiel

Das folgende Beispiel zeigt die Mitgliedschaftsinformationen für alle lokalen Benutzer auf SVM vs1; 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
```

Verwandte Informationen

- Weitere Informationen zu `vserver cifs` finden sich in der "ONTAP-Befehlsreferenz".
- Passwortkomplexität für lokale Benutzer konfigurieren
- Informationen zu den Server-Sicherheitseinstellungen

Lokale ONTAP SMB-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 Ermittlung der Zugriffsrechte auf die auf Ihrer SVM enthaltenen Daten benötigt werden.

Über diese Aufgabe

Folgendes ist beim Löschen lokaler Benutzer zu beachten:

- Das Dateisystem bleibt unverändert.

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

- Sämtliche Verweise auf lokale Benutzer werden aus den Mitgliedschafts- und Berechtigungsdatenbanken

entfernt.

- Standardmäßige, bekannte Benutzer wie Administrator können nicht gelöscht werden.

Schritte

1. Ermitteln Sie den Namen des lokalen Benutzerkontos, das Sie löschen möchten:

```
vserver cifs users-and-groups local-user show -vserver <SVM_name>
```

2. Löschen Sie den lokalen Benutzer:

```
vserver cifs users-and-groups local-user delete -vserver <SVM_name>
-user-name <user_name>
```

3. Überprüfen Sie, ob das Benutzerkonto gelöscht wurde:

```
vserver cifs users-and-groups local-user show -vserver <SVM_name>
```

Das folgende Beispiel löscht den lokalen Benutzer “CIFS_SERVER\sue”, der mit der 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
```

Lokale ONTAP SMB-Gruppen verwalten

Sie können eine lokale Gruppe ändern, indem Sie ihre Beschreibung aktualisieren oder sie umbenennen. Sie können auch alle lokalen Gruppen im Cluster oder auf einer bestimmten Storage Virtual Machine (SVM) anzeigen und sehen, wer zu welcher Gruppe gehört. Diese Informationen können Ihnen bei der Fehlerbehebung von Dateizugriffs- und Benutzerrechtenproblemen auf der SVM helfen.

Wenn Sie möchten…	Verwenden Sie den Befehl…
Alle lokalen Gruppen im Cluster anzeigen	`vserver cifs users-and-groups local-group show`
Alle lokalen Gruppen auf der SVM anzeigen	`vserver cifs users-and-groups local-group show -vserver <SVM_name>`
Mitglieder aller lokalen Gruppen im Cluster anzeigen	`vserver cifs users-and-groups local-group show-members`
Mitglieder aller lokalen Gruppen auf der SVM anzeigen	`vserver cifs users-and-groups local-group show-members -vserver <SVM_name>`
Die Beschreibung der lokalen Gruppe ändern	`vserver cifs users-and-groups local-group modify -vserver <SVM_name> -group-name <group_name> -description text` Enthält die Beschreibung ein Leerzeichen, so muss sie in doppelte Anführungszeichen gesetzt werden.
Die lokale Gruppe umbenennen	`vserver cifs users-and-groups local-group rename -vserver <SVM_name> -group-name <group_name> -new -group-name <new_group_name>`

▼ **Befehlsbeispiele**

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
```

Das folgende Beispiel ändert die Beschreibung der lokalen Gruppe “CIFS_SERVER\engineering”:

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

Beispiel

Das folgende Beispiel zeigt Informationen über alle 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
```

Beispiel

Das folgende Beispiel zeigt Informationen über Mitglieder aller lokalen Gruppen auf SVM vs1:

```
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 ONTAP SMB-Gruppen löschen

Eine lokale Gruppe kann aus der Storage Virtual Machine (SVM) gelöscht werden, wenn sie nicht mehr für die Bestimmung der Zugriffsrechte auf Daten, die dieser SVM zugeordnet sind, benötigt wird oder wenn sie nicht mehr für die Zuweisung von SVM Benutzerrechten (Berechtigungen) an Gruppenmitglieder erforderlich ist.

Über diese Aufgabe

Folgendes ist beim Löschen lokaler Gruppen zu beachten:

- Das Dateisystem bleibt unverändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die auf diese Gruppe verweisen, sind nicht angepasst.

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

Schritte

1. Ermitteln Sie den Namen der lokalen Gruppe, die Sie löschen möchten, indem Sie die Liste der lokalen Gruppen auf dem SVM anzeigen:

   ```
   vserver cifs users-and-groups local-group show -vserver <SVM_name>
   ```

2. Lokale Gruppe löschen:

   ```
   vserver cifs users-and-groups local-group delete -vserver <SVM_name>
   ```

```
-group-name <group_name>
```

3. Überprüfen Sie, ob die Gruppe gelöscht wurde:

```
vserver cifs users-and-groups local-group show -vserver <SVM_name>
```

▼ **Befehlsbeispiel**

Das folgende Beispiel löscht die lokale Gruppe “CIFS_SERVER\sales”, 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
```

Fügen Sie ein Mitglied zu einer lokalen ONTAP SMB-Gruppe hinzu

Sie können die Mitgliedschaft in lokalen Gruppen verwalten, indem Sie lokale Benutzer, Domänenbenutzer oder Domänengruppen hinzufügen. Dies ist hilfreich, wenn Sie den Zugriff auf Daten basierend auf den für die Gruppe festgelegten Zugriffskontrollen steuern oder wenn Sie möchten, dass Benutzer die mit dieser Gruppe verbundenen Berechtigungen erhalten.

Über diese Aufgabe

- Sie können keine Benutzer zur speziellen Gruppe *Everyone* hinzufügen.
- Die lokale Gruppe muss existieren, bevor Sie einen Benutzer hinzufügen können.
- Der Benutzer muss existieren, bevor Sie ihn einer lokalen Gruppe hinzufügen können.

- Sie können keine lokale Gruppe zu einer anderen lokalen Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Domänengruppe zu einer lokalen Gruppe hinzuzufügen, muss Data ONTAP den Namen in eine SID auflösen können.

Schritt

1. Füge ein Mitglied zu einer Gruppe hinzu:

```
vserver cifs users-and-groups local-group add-members -vserver
_vserver_name_ -group-name _group_name_ -member-names name[,...]
```

Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die zur angegebenen lokalen Gruppe hinzugefügt werden.

▼ Befehlsbeispiel

Das folgende Beispiel fügt den lokalen Benutzer “SMB_SERVER\sue” und die Domänengruppe “AD_DOM\dom_eng” der lokalen Gruppe “SMB_SERVER\engineering” auf SVM vs1 hinzu:

```
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
```

Ein Mitglied aus einer lokalen ONTAP SMB-Gruppe entfernen

Sie können die Mitgliedschaft in lokalen Gruppen verwalten, indem Sie lokale Benutzer, Domänenbenutzer oder Domänengruppen entfernen. Dies ist hilfreich, wenn Sie den Zugriff auf Daten basierend auf den für die Gruppe festgelegten Zugriffskontrollen steuern oder wenn Sie möchten, dass Benutzer die mit dieser Gruppe verbundenen Berechtigungen erhalten.

Über diese Aufgabe

- Sie können keine Mitglieder aus der speziellen Gruppe *Everyone* entfernen.
- Die Gruppe, aus der Sie ein Mitglied entfernen möchten, muss existieren.
- ONTAP muss in der Lage sein, die Namen der Mitglieder, die aus der Gruppe entfernt werden sollen, in eine entsprechende SID aufzulösen.

Schritt

1. Ein Mitglied aus einer Gruppe entfernen:

```
vserver cifs users-and-groups local-group remove-members -vserver
_vserver_name_ -group-name _group_name_ -member-names name[,...]
```

Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden.

▼ Befehlsbeispiel

Das folgende Beispiel entfernt die lokalen Benutzer “SMB_SERVER\sue” und “SMB_SERVER\james” aus der lokalen Gruppe “SMB_SERVER\engineering” auf SVM vs1:

```
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
```

ONTAP SMB-Domänenbenutzer- und Gruppennamen in lokalen Datenbanken aktualisieren

Sie können Domänenbenutzer und -gruppen zu den lokalen Gruppen eines CIFS-Servers hinzufügen. Diese Domänenobjekte werden in lokalen Datenbanken im 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 die Domänennamen aktualisieren möchten.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Aktualisieren Sie die Namen der Domänenbenutzer und -gruppen, die der Storage Virtual Machine zugeordnet sind:

   ```
   vserver cifs users-and-groups update-names -vserver <SVM_name>
   ```

3. Anzeige der Domänenbenutzer und -gruppen, deren Aktualisierung erfolgreich war und deren Aktualisierung fehlgeschlagen ist:

   ```
   vserver cifs users-and-groups update-names -vserver <SVM_name> -display
   -failed-only false|true
   ```

4. Um alle Statusinformationen zu Aktualisierungen zu unterdrücken, verwenden Sie folgenden Befehl:

   ```
   vserver cifs users-and-groups update-names -vserver <SVM_name> -suppress
   -all-output true
   ```

5. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

▼ **Befehlsbeispiel**

Das folgende Beispiel aktualisiert die Namen der Domänenbenutzer und -gruppen, die der Storage Virtual Machine (SVM, ehemals Vserver) vs1 zugeordnet sind. Für die letzte Aktualisierung besteht eine abhängige

Namenskette, die aktualisiert werden muss:

```
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
```

Verwandte Informationen

Weitere Informationen zu `vserver cifs` finden sich in der "ONTAP-Befehlsreferenz".

Berechtigungen für ONTAP SMB lokale oder Domänenbenutzer oder -gruppen verwalten

Berechtigungen zu ONTAP SMB lokalen oder Domänenbenutzern oder -gruppen hinzufügen

Sie können die Benutzerrechte für lokale oder Domänenbenutzer oder -gruppen verwalten, indem Sie Berechtigungen hinzufügen. Die hinzugefügten Berechtigungen überschreiben die standardmäßig zugewiesenen Berechtigungen für eines dieser Objekte. Dies bietet eine verbesserte Sicherheit, da sich individuell festlegen lässt, über welche Berechtigungen ein Benutzer oder eine Gruppe verfügt.

Bevor Sie beginnen

Der lokale oder Domänenbenutzer bzw. die Gruppe, zu der Berechtigungen hinzugefügt werden, muss bereits existieren.

Über diese Aufgabe

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

Beim Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -gruppen ist Folgendes zu beachten:

- Sie können eine oder mehrere Berechtigungen hinzufügen.
- Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren.

  Der Befehl kann fehlschlagen, wenn ONTAP keinen Kontakt zum Domänencontroller herstellen kann.

Schritte

1. Fügen Sie einem lokalen Benutzer, einem Domänenbenutzer oder einer Gruppe eine oder mehrere Berechtigungen hinzu:

   ```
   vserver cifs users-and-groups privilege add-privilege -vserver
   <SVM_name> -user-or-group-name <name> -privileges <privilege>[,...]
   ```

2. Überprüfen Sie, ob dem Objekt die gewünschten Berechtigungen zugewiesen wurden:

   ```
   vserver cifs users-and-groups privilege show -vserver <SVM_name> -user
   -or-group-name <name>
   ```

Beispiel

Das folgende Beispiel fügt die Berechtigungen “SeTcbPrivilege” und “SeTakeOwnershipPrivilege” dem Benutzer “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1 hinzu:

```
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
```

Berechtigungen von ONTAP SMB lokalen oder Domänenbenutzern oder -gruppen entfernen

Sie können die Benutzerrechte für lokale oder Domänenbenutzer oder -gruppen verwalten, indem Sie Berechtigungen entfernen. Dies bietet eine höhere Sicherheit, da Sie die maximalen Berechtigungen von Benutzern und Gruppen individuell anpassen können.

Bevor Sie beginnen

Der lokale oder Domänenbenutzer oder die Gruppe, von der Berechtigungen entfernt werden, muss bereits existieren.

Über diese Aufgabe

Beim Entfernen von Berechtigungen für lokale oder Domänenbenutzer oder -gruppen ist Folgendes zu beachten:

- Sie können eine oder mehrere Berechtigungen entfernen.
- Beim Entfernen von Berechtigungen von einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren.

  Der Befehl kann fehlschlagen, wenn ONTAP keinen Kontakt zum Domänencontroller herstellen kann.

Schritte

1. Einem lokalen Benutzer, einem Domänenbenutzer oder einer Gruppe eine oder mehrere Berechtigungen entziehen:

   ```
   vserver cifs users-and-groups privilege remove-privilege -vserver
   <SVM_name> -user-or-group-name <name> -privileges <privilege>[,...]
   ```

2. Überprüfen Sie, ob die gewünschten Berechtigungen vom Objekt entfernt wurden:

   ```
   vserver cifs users-and-groups privilege show -vserver <SVM_name> -user
   -or-group-name <name>
   ```

Beispiel

Das folgende Beispiel entfernt die Berechtigungen “SeTcbPrivilege” und “SeTakeOwnershipPrivilege” vom Benutzer “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1:

```
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 ONTAP SMB lokale oder Domänenbenutzer und -gruppen zurücksetzen

Sie können die Berechtigungen für lokale oder Domänenbenutzer und -gruppen zurücksetzen. Dies kann hilfreich sein, wenn Berechtigungen für einen lokalen oder Domänenbenutzer oder eine Gruppe geändert wurden und diese Änderungen nicht mehr gewünscht oder benötigt werden.

Über diese Aufgabe

Das Zurücksetzen der Berechtigungen für einen lokalen oder Domänenbenutzer oder eine lokale oder Domänengruppe entfernt sämtliche Berechtigungseinträge für dieses Objekt.

Schritte

1. Setzen Sie die Berechtigungen für einen lokalen oder Domänenbenutzer oder eine lokale oder Domänengruppe zurück:

   ```
   vserver cifs users-and-groups privilege reset-privilege -vserver
   <SVM_name> -user-or-group-name <name>
   ```

2. Überprüfen Sie, ob die Berechtigungen für das Objekt zurückgesetzt wurden:

   ```
   vserver cifs users-and-groups privilege show -vserver <SVM_name> -user
   -or-group-name <name>
   ```

Beispiele

Das folgende Beispiel setzt die Berechtigungen des Benutzers “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals Vserver) vs1 zurück. Standardmäßig sind normalen Benutzern keine Berechtigungen zugeordnet:

```
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, wodurch der Berechtigungseintrag entfernt wird:

```
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.
```

Informationen zu ONTAP SMB-Berechtigungsüberschreibungen

Sie können Informationen über benutzerdefinierte Berechtigungen anzeigen, die Domänen- oder lokalen Benutzerkonten oder Gruppen zugewiesen sind. Diese Informationen helfen Ihnen festzustellen, ob die gewünschten Benutzerrechte angewendet werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	Geben Sie diesen Befehl ein…
Benutzerdefinierte Berechtigungen für alle Domänen- und lokalen Benutzer und Gruppen auf der Storage Virtual Machine (SVM)	`vserver cifs users-and-groups privilege show -vserver <SVM_name>`
Benutzerdefinierte Berechtigungen für eine bestimmte Domäne oder einen lokalen Benutzer und eine Gruppe auf der SVM	`vserver cifs users-and-groups privilege show -vserver <SVM_name> -user-or-group-name <name>`

   Es gibt weitere optionale Parameter, die Sie beim Ausführen dieses Befehls auswählen können. Weitere Informationen zu `vserver cifs users-and-groups privilege show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel

Der folgende Befehl zeigt alle Berechtigungen an, die lokalen oder Domänenbenutzern und -gruppen für SVM vs1 explizit 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
```

Umgehungsüberprüfung konfigurieren

Informationen zur Konfiguration der ONTAP SMB Bypass Traverse-Prüfung

Die Umgehung der Pfadprüfung ist ein Benutzerrecht (auch als Berechtigung bezeichnet), das festlegt, ob ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen kann, selbst wenn er keine Berechtigung für das durchlaufene Verzeichnis besitzt. Es ist wichtig zu verstehen, was geschieht, wenn die Umgehung der Pfadprüfung erlaubt oder nicht erlaubt wird, und wie die Umgehung der Pfadprüfung für Benutzer auf Storage Virtual Machines (SVMs) konfiguriert werden kann.

Was geschieht beim Zulassen oder Verweigern der Bypass Traverse-Prüfung

- Sofern zulässig, prüft ONTAP beim Versuch eines Benutzers, auf eine Datei zuzugreifen, nicht die Traverse-Berechtigung für die Zwischenverzeichnisse, wenn entschieden wird, ob der Zugriff auf die Datei gewährt oder verweigert wird.
- Falls dies nicht zulässig ist, prüft ONTAP die Ausführungsberechtigung für alle Verzeichnisse im Pfad zur Datei.

  Wenn eines der Zwischenverzeichnisse nicht über die Berechtigung “X” (Durchlaufberechtigung) verfügt, verweigert ONTAP den Zugriff auf die Datei.

Umgehungsüberprüfung konfigurieren

Die Umgehung der Traverse-Prüfung kann mithilfe der ONTAP CLI oder durch die Konfiguration von Active Directory Gruppenrichtlinien mit diesem Benutzerrecht eingerichtet werden.

Die `SeChangeNotifyPrivilege`Berechtigung steuert, ob Benutzern das Umgehen der Traverse-Prüfung erlaubt ist.

- Das Hinzufügen zu lokalen SMB-Benutzern oder -Gruppen auf der SVM oder zu Domänenbenutzern oder -gruppen ermöglicht das Umgehen der Traverse-Prüfung.
- Das Entfernen aus den lokalen SMB-Benutzern oder Gruppen auf der SVM oder aus den Domänenbenutzern oder Gruppen verhindert die Umgehung der Traverse-Prüfung.

Standardmäßig haben die folgenden BUILTIN-Gruppen auf dem SVM das Recht, die Traversierungsprüfung zu umgehen:

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

Wenn nicht gewünscht ist, dass Mitglieder einer dieser Gruppen die Traverse-Prüfung umgehen, muss dieser Gruppe diese Berechtigung entzogen werden.

Bei der Konfiguration der Umgehung der Traverse-Prüfung für lokale SMB-Benutzer und -Gruppen auf der SVM mithilfe der CLI ist Folgendes zu beachten:

- Wenn Mitglieder einer benutzerdefinierten lokalen oder Domänengruppe die Traverse-Prüfung umgehen dürfen, muss der Gruppe die `SeChangeNotifyPrivilege` Berechtigung hinzugefügt werden.
- Wenn einem einzelnen lokalen Benutzer oder Domänenbenutzer erlaubt werden soll, die Überprüfung der Zugriffsrechte zu umgehen, und dieser Benutzer kein Mitglied einer Gruppe mit dieser Berechtigung ist, kann die `SeChangeNotifyPrivilege` Berechtigung diesem Benutzerkonto hinzugefügt werden.
- Sie können die Umgehung der Traverse-Prüfung für lokale oder Domänenbenutzer oder -gruppen deaktivieren, indem Sie die `SeChangeNotifyPrivilege`Berechtigung jederzeit entfernen.

> Um die Überprüfung von Bypass-Travers für bestimmte lokale oder Domänenbenutzer oder -gruppen zu deaktivieren, muss außerdem die `SeChangeNotifyPrivilege` Berechtigung aus der `Everyone` Gruppe entfernt werden.

Verwandte Informationen

- Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung erlauben
- Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung untersagen
- Zeichenzuordnung für die Dateinamenübersetzung auf Volumes konfigurieren
- Freigabe-Zugriffskontrolllisten erstellen
- Sicherer Dateizugriff mit Storage Level Access Guard
- Liste der unterstützten Berechtigungen
- Berechtigungen für lokale oder Domänenbenutzer oder -gruppen hinzufügen

Benutzern oder Gruppen erlauben, die ONTAP SMB-Verzeichnisdurchlaufprüfung zu umgehen

Wenn ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen können soll, auch wenn er für ein durchlaufenes Verzeichnis keine Berechtigungen hat, kann die `SeChangeNotifyPrivilege` Berechtigung lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs) hinzugefügt werden. Standardmäßig können Benutzer die Überprüfung des Verzeichnisdurchlaufs umgehen.

Bevor Sie beginnen

- Auf der SVM muss ein SMB Server vorhanden sein.
- Die Option „Lokale Benutzer und Gruppen SMB-Server“ muss aktiviert sein.

- Der lokale oder Domänenbenutzer bzw. die Gruppe, zu der die `SeChangeNotifyPrivilege`Berechtigung hinzugefügt wird, muss bereits existieren.

Über diese Aufgabe

Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren. Der Befehl kann fehlschlagen, wenn ONTAP den Domänencontroller nicht erreichen kann.

Schritte

1. Die Umgehung der Traverse-Prüfung kann aktiviert werden, indem die `SeChangeNotifyPrivilege` -Berechtigung einem lokalen oder Domänenbenutzer oder einer Gruppe hinzugefügt wird: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group -name` *`name`* `-privileges SeChangeNotifyPrivilege`

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

2. Es sollte überprüft werden, ob für den angegebenen Benutzer oder die Gruppe die Umgehung der Traversierungsprüfung aktiviert ist: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Der folgende Befehl ermöglicht es Benutzern der Gruppe “EXAMPLE\eng”, die Verzeichnisdurchsuchungsprüfung zu umgehen, indem die `SeChangeNotifyPrivilege` Berechtigung der Gruppe hinzugefügt wird:

```
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

Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung untersagen

Benutzern oder Gruppen das Umgehen der ONTAP SMB-Verzeichnisdurchlaufprüfung untersagen

Wenn nicht gewünscht ist, dass ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchläuft, weil der Benutzer keine Berechtigungen für das durchlaufene Verzeichnis hat, kann die `SeChangeNotifyPrivilege` Berechtigung von lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs) entfernt werden.

Bevor Sie beginnen

Der lokale oder Domänenbenutzer oder die Gruppe, von der Berechtigungen entfernt werden, muss bereits existieren.

Über diese Aufgabe

Beim Entfernen von Berechtigungen von einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren. Der Befehl kann fehlschlagen, wenn ONTAP den Domänencontroller nicht erreichen kann.

Schritte

1. Umgehung der Traversierungsprüfung nicht zulassen: `vserver cifs users-and-groups privilege remove-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   Der Befehl entfernt die `SeChangeNotifyPrivilege`Berechtigung vom lokalen oder Domänen-Benutzer oder der Gruppe, die mit dem Wert für den `-user-or-group-name *name*`Parameter angegeben wird.

2. Es sollte überprüft werden, ob für den angegebenen Benutzer oder die Gruppe die Umgehung der Traversierungsprüfung deaktiviert ist: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Der folgende Befehl verhindert, dass Benutzer der Gruppe “EXAMPLE\eng” die Verzeichnisdurchsuchungsprüfung umgehen:

```
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 das Umgehen der Verzeichnisdurchlaufprüfung erlauben

Informationen zu Dateisicherheit und Überwachungsrichtlinien

Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien

Informationen zur Dateisicherheit von Dateien und Verzeichnissen in Volumes auf Storage Virtual Machines (SVMs) können angezeigt werden. Informationen zu Überwachungsrichtlinien auf FlexVol volumes können angezeigt werden. Wenn

konfiguriert, können Informationen zu Storage-Level Access Guard und Dynamic Access Control Sicherheitseinstellungen auf FlexVol volumes angezeigt werden.

Anzeige von Informationen zur Dateisicherheit

Es lassen sich Informationen über die auf Daten in Volumes und Qtrees (für FlexVol volumes) angewendete Dateisicherheit mit den folgenden Sicherheitsstilen anzeigen:

- NTFS
- UNIX
- Gemischt

Anzeige von Informationen über Prüfungsrichtlinien

Informationen zu Überwachungsrichtlinien für die Überwachung von Zugriffsereignissen auf FlexVol volumes über die folgenden NAS-Protokolle können angezeigt werden:

- SMB (alle Versionen)
- NFSv4.x

Anzeige von Informationen zur Storage-Level Access Guard (SLAG) Sicherheit

Die Storage-Level Access Guard-Sicherheit kann auf FlexVol volumes und qtree-Objekte mit den folgenden Sicherheitsstilen angewendet werden:

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

Anzeigen von Informationen zur Dynamic Access Control (DAC) Sicherheit

Die Dynamic Access Control-Sicherheit kann auf ein Objekt innerhalb eines FlexVol volume mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt (wenn das Objekt über effektive NTFS-Sicherheit verfügt)

Verwandte Informationen

- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard
- Informationen zu Storage-Level Access Guard auf Servern

Informationen zur ONTAP SMB-Dateisicherheit auf NTFS Security-Style-Volumes anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf NTFS-Sicherheitsstil-Volumes anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu DOS-Attributen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Ordnersicherheitsinformationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- Da NTFS Security-Style Volumes und Qtrees ausschließlich NTFS-Dateiberechtigungen sowie Windows-Benutzer und -Gruppen zur Bestimmung der Dateizugriffsrechte verwenden, enthalten UNIX-bezogene Ausgabefelder lediglich zur Anzeige bestimmte UNIX-Dateiberechtigungsinformationen.
- Die ACL-Ausgabe wird für Dateien und Ordner mit NTFS-Sicherheit angezeigt.
- Da die Storage-Level Access Guard Sicherheit auf dem Volume-Root oder Qtree konfiguriert werden kann, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre Datei-ACLs als auch Storage-Level Access Guard ACLs anzeigen.
- Die Ausgabe zeigt außerdem Informationen über die ACEs der Dynamic Access Control an, falls Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit erweiterten Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/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
```

Das folgende Beispiel zeigt die Sicherheitsinformationen mit erweiterten Masken zum Pfad `/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
```

Das folgende Beispiel zeigt Sicherheitsinformationen, einschließlich Storage-Level Access Guard-Sicherheitsinformationen, für das Volume mit dem Pfad `/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

- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

Informationen zur ONTAP SMB-Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu UNIX-Besitzern und Gruppen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Ordnersicherheitsinformationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Ordner enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.
- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder effektive UNIX- oder NTFS-Sicherheit 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 und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl UNIX-Dateiberechtigungen als auch Storage-Level Access Guard ACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit effektiver NTFS-Sicherheit führt, werden in der Ausgabe auch Informationen über Dynamic Access Control ACEs angezeigt, sofern Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Mit erweiterten Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/projects` in SVM vs1 in erweiterter Maskenform. Dieser Pfad mit gemischtem Security-Style hat 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: -
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/data` in SVM vs1. Dieser Pfad mit gemischtem Sicherheitsstil hat eine effektive NTFS-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
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Volume am Pfad `/datavol5` in SVM vs1. Die oberste Ebene dieses Mixed Security-Style Volumes verfügt über effektive UNIX-Sicherheit. Das Volume verfügt über Storage-Level Access Guard-Sicherheit.

```
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

- Informationen zur Dateisicherheit auf NTFS Security-Style-Volumes
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

Informationen zur ONTAP SMB-Dateisicherheit auf UNIX Security-Style-Volumes anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf UNIX Security-Style-Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu UNIX-Besitzern und -Gruppen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Verzeichnissicherheitsinformationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- UNIX Security-Style-Volumes und Qtrees verwenden zur Bestimmung der Dateizugriffsrechte ausschließlich UNIX-Dateiberechtigungen, entweder Modusbits 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 und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Eigentümer“ und „Gruppe“ in der ACL-Ausgabe gelten nicht für NFSv4-Sicherheitsdeskriptoren.

  Sie sind nur für NTFS-Sicherheitsdeskriptoren aussagekräftig.

- Da die Storage-Level Access Guard-Sicherheit auf einem UNIX-Volume oder Qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die auf das im `-path` Parameter angegebene Volume oder den Qtree angewendete Storage-Level Access Guard-Sicherheit enthalten.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit erweiterten Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/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: -
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/home` in SVM vs1 in erweiterter Maskenform:

```
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

- Informationen zur Dateisicherheit auf Security-Style-Volumes anzeigen
- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen

ONTAP Befehle zur Anzeige von Informationen über NTFS-Überwachungsrichtlinien auf SMB FlexVol Volumes

Sie können Informationen zu NTFS-Überwachungsrichtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu Systemzugriffskontrolllisten. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Ordnern angeben, deren Audit-Informationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- NTFS Security-Style Volumes und Qtrees verwenden ausschließlich NTFS-Systemzugriffskontrolllisten (SACLs) für Audit-Richtlinien.
- Auf Dateien und Ordner in einem Volume mit gemischtem Sicherheitsstil und effektiver NTFS-Sicherheit können NTFS-Überwachungsrichtlinien angewendet werden.

  Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder UNIX- oder NTFS-effektive Sicherheit aufweisen und kann NTFS-SACLs enthalten oder auch nicht.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre Datei- und Ordner-NFSv4-SACLs als auch Storage-Level Access Guard NTFS-SACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS effektiver Sicherheit führt, werden in der Ausgabe auch Informationen über Dynamic Access Control ACEs angezeigt, sofern Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Bei der Anzeige von Sicherheitsinformationen zu Dateien und Ordnern mit NTFS effektiver Sicherheit enthalten die UNIX-bezogenen Ausgabefelder nur Anzeigeinformationen zu UNIX-Dateiberechtigungen.

  Dateien und Ordner im NTFS-Sicherheitsstil verwenden ausschließlich NTFS-Dateiberechtigungen sowie Windows-Benutzer und -Gruppen zur Bestimmung der Dateizugriffsrechte.

- 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 und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige der Überwachungsrichtlinieneinstellungen für Dateien und Verzeichnisse mit dem gewünschten Detaillierungsgrad:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`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

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/corp` in SVM vs1. Der Pfad verfügt über effektive NTFS-Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen SUCCESS- als auch einen SUCCESS/FAIL-SACL-Eintrag.

```
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
```

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/datavol1` in SVM vs1. Der Pfad enthält sowohl reguläre Datei- und Ordner-SACLs als auch Storage-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
```

ONTAP Befehle zur Anzeige von Informationen zu NFSv4-Überwachungsrichtlinien auf SMB FlexVol volumes

Es lassen sich Informationen zu NFSv4-Auditrichtlinien auf FlexVol volumes mithilfe der

ONTAP CLI anzeigen, darunter die Sicherheitsstile und effektiven Sicherheitsstile, die angewendeten Berechtigungen sowie Informationen zu Systemzugriffskontrolllisten (SACLs). Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen verwendet werden.

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. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- UNIX Security-Style Volumes und Qtrees verwenden ausschließlich NFSv4 SACLs für Audit-Richtlinien.
- Auf Dateien und Verzeichnisse in einem Volume mit gemischtem Sicherheitsstil, die dem UNIX-Sicherheitsstil entsprechen, können NFSv4-Auditrichtlinien angewendet werden.

  Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder UNIX- oder NTFS-effektive Sicherheit aufweisen und kann NFSv4-SACLs enthalten oder auch nicht.
- 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 und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre NFSv4-Datei- und Verzeichnis-SACLs als auch Storage-Level Access Guard NTFS-SACLs anzeigen.
- Da die Storage-Level Access Guard-Sicherheit auf einem UNIX-Volume oder Qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die auf das im `-path` Parameter angegebene Volume oder den Qtree angewendete Storage-Level Access Guard-Sicherheit enthalten.

Schritte

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Mit erweiterten Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/lab` in SVM vs1. Dieser UNIX-

Sicherheitsstil-Pfad 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
```

Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien

Sie können das Platzhalterzeichen (*) verwenden, um Informationen über die Dateisicherheit und die Revisionsprotokollrichtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Stammvolume anzuzeigen.

Das Platzhalterzeichen (**) kann als letzter Bestandteil eines angegebenen Verzeichnispfads verwendet werden, unterhalb dessen Informationen zu allen Dateien und Verzeichnissen angezeigt werden. Wenn Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen „**“ angezeigt werden sollen, ist der vollständige Pfad in doppelte Anführungszeichen („``“) anzugeben.

Beispiel

Der folgende Befehl mit dem Platzhalterzeichen zeigt die Informationen zu allen Dateien und Verzeichnissen unterhalb des Pfads `/1/` von SVM vs1 an:

```
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)
```

Der folgende Befehl zeigt die Informationen einer Datei mit dem Namen "*" unter dem Pfad `/vol1/a` von SVM vs1 an. 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
```

NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und Storage-Level Access Guard auf SVMs mithilfe der CLI verwalten

ONTAP Befehle zur Verwaltung der SMB NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und des Storage-Level Access Guard

Die NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und Storage-Level Access Guard auf Storage Virtual Machines (SVMs) lassen sich mithilfe der CLI verwalten.

Die NTFS-Dateisicherheit und Überwachungsrichtlinien können von SMB-Clients oder über die CLI verwaltet werden. Die Verwendung der CLI zur Konfiguration von Dateisicherheit und Überwachungsrichtlinien macht es jedoch unnötig, einen Remote-Client zur Verwaltung der Dateisicherheit zu nutzen. Die Nutzung der CLI kann die Zeit, die für das Anwenden von Sicherheitsmaßnahmen auf viele Dateien und Ordner mit einem einzigen Befehl benötigt wird, erheblich verkürzen.

Sie können Storage-Level Access Guard konfigurieren, eine zusätzliche Sicherheitsebene, die von ONTAP auf SVM-Volumes angewendet wird. Storage-Level Access Guard gilt für Zugriffe aller NAS-Protokolle auf das Speicherobjekt, auf das Storage-Level Access Guard angewendet wird.

Storage-Level Access Guard kann nur über die ONTAP-Befehlszeile konfiguriert und verwaltet werden. Einstellungen von Storage-Level Access Guard können nicht von SMB-Clients aus verwaltet werden. Zudem wird beim Anzeigen der Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client die Storage-Level Access Guard-Sicherheit nicht angezeigt. Die Storage-Level Access Guard-Sicherheit kann von einem Client, selbst durch einen Systemadministrator (Windows oder UNIX), nicht aufgehoben werden. Storage-Level Access Guard bietet daher eine zusätzliche Sicherheitsebene für den Datenzugriff, die unabhängig vom Speicheradministrator festgelegt und verwaltet wird.

> Auch wenn für Storage-Level Access Guard nur NTFS-Zugriffsberechtigungen 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 zugeordnet ist, der das Volume besitzt.

NTFS Security-Style Volumes

Alle Dateien und Ordner in NTFS Security-Style-Volumes und Qtrees verfügen über effektive NTFS-Sicherheit. Die `vserver security file-directory` Befehlsfamilie ermöglicht die Implementierung der folgenden

Sicherheitsarten auf NTFS Security-Style-Volumes:

- Dateiberechtigungen und Überwachungsrichtlinien für Dateien und Ordner im Volume
- Storage-Level Access Guard-Sicherheit auf Volumes

Volumes mit gemischtem Security-Style

Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Ordner enthalten, die über UNIX-effektive Sicherheit verfügen und UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4.x-ACLs und NFSv4.x-Überwachungsrichtlinien, sowie einige Dateien und Ordner, die über NTFS-effektive Sicherheit verfügen und NTFS-Dateiberechtigungen und Überwachungsrichtlinien verwenden. Mit der `vserver security file-directory`Befehlsfamilie lassen sich die folgenden Sicherheitstypen auf Daten mit gemischtem Security-Style anwenden:

- Dateiberechtigungen und Überwachungsrichtlinien für Dateien und Ordner mit NTFS-Effektivsicherheitsstil im gemischten Volume oder qtree
- Storage-Level Access Guard für Volumes mit entweder NTFS- oder UNIX-effektivem Sicherheitsstil

UNIX Security-Style Volumes

UNIX Security-Style-Volumes und Qtrees enthalten Dateien und Ordner mit effektiver UNIX-Sicherheit (entweder Mode-Bits oder NFSv4.x-ACLs). Folgendes ist zu beachten, wenn die `vserver security file-directory` Command-Family zur Implementierung von Sicherheit auf UNIX Security-Style-Volumes verwendet wird:

- Die `vserver security file-directory`Befehlsfamilie kann nicht zur Verwaltung von UNIX-Dateisicherheits- und Überwachungsrichtlinien auf UNIX Security-Style Volumes und qtrees verwendet werden.
- Die `vserver security file-directory`Befehlsfamilie kann zur Konfiguration von Storage-Level Access Guard auf UNIX-Sicherheitsvolumes verwendet werden, sofern die SVM mit dem Ziel-Volume einen CIFS-Server enthält.

Verwandte Informationen

- Informationen zur Anzeige von Dateisicherheits- und Prüfrichtlinien
- NTFS-Sicherheitsdeskriptoren auf Servern erstellen
- Befehle zum Konfigurieren und Anwenden von Überwachungsrichtlinien auf Dateien und Ordner
- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard

ONTAP Befehle zum Festlegen der SMB-Datei- und Ordnersicherheit

Da Sie die Datei- und Ordnersicherheit lokal anwenden und verwalten können, ohne dass ein Remote-Client beteiligt ist, kann die Zeit für die Massensicherheitsfestlegung bei einer großen Anzahl von Dateien oder Ordnern erheblich reduziert werden.

Die Verwendung der Befehlszeilenschnittstelle (CLI) zum Festlegen der Datei- und Ordnersicherheit kann in folgenden Anwendungsfällen von Vorteil sein:

- Speicherung von Dateien in großen Unternehmensumgebungen, wie zum Beispiel Dateispeicherung in Home-Verzeichnissen
- Migration von Daten

- Änderung der Windows-Domäne
- Standardisierung von Dateisicherheits- und Überwachungsrichtlinien für NTFS-Dateisysteme

Informationen zu den Grenzen bei der Verwendung von ONTAP Befehlen zum Festlegen der SMB-Datei- und Ordnersicherheit

Bei der Verwendung der CLI zum Festlegen der Datei- und Ordnersicherheit sind bestimmte Einschränkungen zu beachten.

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

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

Sicherheitsdeskriptoren werden verwendet, um die ONTAP SMB Datei- und Ordnersicherheit anzuwenden.

Sicherheitsdeskriptoren enthalten die Zugriffskontrolllisten, die festlegen, welche Aktionen ein Benutzer an Dateien und Ordnern durchführen kann und was protokolliert wird, wenn ein Benutzer auf Dateien und Ordner zugreift.

- **Berechtigungen**

  Berechtigungen werden vom Besitzer eines Objekts erteilt oder verweigert und bestimmen, welche Aktionen ein Objekt (Benutzer, Gruppen oder Computerobjekte) für bestimmte Dateien oder Ordner ausführen kann.

- **Sicherheitsdeskriptoren**

  Sicherheitsdeskriptoren sind Datenstrukturen, die Sicherheitsinformationen enthalten, die die Berechtigungen für eine Datei oder einen Ordner definieren.

- **Zugriffskontrolllisten (ACLs)**

  Zugriffssteuerungslisten (ACLs) sind Listen innerhalb eines Sicherheitsdeskriptors, die Informationen darüber enthalten, welche Aktionen Benutzer, Gruppen oder Computerobjekte für die Datei oder den Ordner ausführen dürfen, auf den der Sicherheitsdeskriptor angewendet wird. Der Sicherheitsdeskriptor kann die folgenden zwei Arten von ACLs enthalten:

  - Diskretionäre Zugriffskontrolllisten (DACLs)
  - Systemzugriffskontrolllisten (SACLs)

- **Diskretionäre Zugriffskontrolllisten (DACLs)**

  DACLs enthalten die Liste der SIDS für die Benutzer, Gruppen und Computerobjekte, denen der Zugriff auf Dateien oder Ordner erlaubt oder verweigert wird. DACLs enthalten null oder mehr Zugriffssteuerungseinträge (ACEs).

- **Systemzugriffskontrolllisten (SACLs)**

  SACLs enthalten die Liste der SIDS für die Benutzer, Gruppen und Computerobjekte, für die erfolgreiche oder fehlgeschlagene Überwachungsereignisse protokolliert werden. SACLs enthalten null oder mehr Zugriffssteuerungseinträge (ACEs).

- **Zugriffskontrolleinträge (ACEs)**

  ACEs sind einzelne Einträge entweder in DACLs oder SACLs:

  - Ein DACL-Zugriffskontrolleintrag legt die Zugriffsrechte fest, die für bestimmte Benutzer, Gruppen oder Computerobjekte erlaubt oder verweigert werden.
  - Ein SACL-Zugriffskontrolleintrag gibt an, welche Erfolgs- oder Fehlerereignisse beim Überwachen bestimmter Aktionen von bestimmten Benutzern, Gruppen oder Computerobjekten protokolliert werden.

- **Berechtigungsvererbung**

  Die Berechtigungsvererbung beschreibt, wie Berechtigungen, die in Sicherheitsdeskriptoren definiert sind, von einem übergeordneten Objekt auf ein Objekt übertragen werden. Nur vererbbare Berechtigungen werden von untergeordneten Objekten übernommen. Beim Festlegen von Berechtigungen für das übergeordnete Objekt kann festgelegt werden, ob Ordner, Unterordner und Dateien diese mit „Apply to `this-folder`, `sub-folders` und `files`“ erben können.

Verwandte Informationen

- "SMB und NFS Auditierung und Sicherheitsverfolgung"
- Befehle zum Konfigurieren und Anwenden von Überwachungsrichtlinien auf Dateien und Ordner

Informationen zur Anwendung von Dateiverzeichnisrichtlinien, die lokale SMB-Benutzer oder -Gruppen auf dem ONTAP SVM Disaster Recovery-Ziel verwenden

Bestimmte Richtlinien sind zu beachten, bevor Dateiverzeichnisrichtlinien auf der Storage Virtual Machine (SVM) Disaster Recovery Ziel in einer ID Discard Konfiguration angewendet werden, wenn die Dateiverzeichnisrichtlinienkonfiguration lokale Benutzer oder Gruppen entweder im Sicherheitsdeskriptor oder in den DACL- oder SACL-Einträgen verwendet.

Eine Disaster Recovery-Konfiguration kann für eine SVM eingerichtet werden, bei der die Quell-SVM im Quell-Cluster die Daten und die Konfiguration von der Quell-SVM auf eine Ziel-SVM in einem Ziel-Cluster repliziert.

Es stehen zwei Arten der SVM-Notfallwiederherstellung zur Verfügung:

- Identität gewahrt

  Bei dieser Konfiguration bleibt die Identität der SVM und des CIFS-Servers erhalten.

- Identität verworfen

  Bei dieser Konfiguration bleibt die Identität der SVM und des CIFS-Servers nicht erhalten. In diesem Szenario unterscheiden sich die Namen der SVM und des CIFS-Servers auf der Ziel-SVM von den Namen der SVM und des CIFS-Servers auf der Quell-SVM.

Richtlinien für verworfene Identitätskonfigurationen

In einer Konfiguration mit verworfener Identität muss für eine SVM-Quelle, die lokale Benutzer-, Gruppen- und Berechtigungskonfigurationen enthält, der Name der lokalen Domäne (lokaler CIFS-Servername) so geändert werden, dass er mit dem CIFS-Servernamen auf der SVM-Ziel übereinstimmt. Beispielsweise, wenn der Name der Quell-SVM „vs1“ und der CIFS-Servername „CIFS1“ ist, und der Name der Ziel-SVM „vs1_dst“ und der CIFS-Servername „CIFS1_DST“ ist, wird der lokale Domänenname für einen lokalen Benutzer mit dem Namen

„CIFS1\user1“ auf der Ziel-SVM automatisch in „CIFS1_DST\user1“ geändert:

```
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          -              -
```

Obwohl lokale Benutzer- und Gruppennamen in den lokalen Benutzer- und Gruppendatenbanken automatisch geändert werden, werden lokale Benutzer- oder Gruppennamen in Dateiverzeichnisrichtlinienkonfigurationen (Richtlinien, die auf der CLI mit der `vserver security file-directory` Befehlfamilie konfiguriert werden) nicht automatisch geändert.

Wenn beispielsweise für “vs1” ein DACL-Eintrag konfiguriert wurde, bei dem der `-account` Parameter auf “CIFS1\user1” gesetzt ist, wird die Einstellung auf der Ziel-SVM nicht automatisch geändert, um den Namen des CIFS-Servers des Ziels widerzuspiegeln.

```
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
```

Es sind die `vserver security file-directory modify` Befehle zu verwenden, um den CIFS-Server-Namen manuell in den Namen des Ziel CIFS-Servers zu ändern.

Datei Verzeichnis-Richtlinienkonfigurationskomponenten, die Kontoparameter enthalten

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

- Sicherheitsdeskriptor

  Optional kann der Besitzer des Sicherheitsdeskriptors und die primäre Gruppe des Besitzers des Sicherheitsdeskriptors angegeben werden. Wenn der Sicherheitsdeskriptor einen lokalen Benutzer oder eine lokale Gruppe für die Einträge Besitzer und primäre Gruppe verwendet, muss der Sicherheitsdeskriptor so geändert werden, dass im Kontonamen die Ziel-SVM verwendet wird. Mit dem `vserver security file-directory ntfs modify` Befehl können alle erforderlichen Änderungen an den Kontonamen vorgenommen werden.

- DACL-Einträge

  Jeder DACL-Eintrag muss einem Konto zugeordnet sein. Alle DACLs, die lokale Benutzer- oder Gruppenkonten verwenden, sind so zu ändern, dass sie den Ziel-SVM-Namen verwenden. Da der Kontoname für bestehende DACL-Einträge nicht geändert werden kann, sind alle DACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren zu entfernen, neue DACL-Einträge mit den korrigierten Zielkontonamen zu erstellen und diese neuen DACL-Einträge den entsprechenden Sicherheitsdeskriptoren zuzuordnen.

- SACL-Einträge

  Jeder SACL-Eintrag muss einem Konto zugeordnet sein. Alle SACLs, die lokale Benutzer- oder Gruppenkonten verwenden, sind so zu ändern, dass sie den Ziel-SVM-Namen verwenden. Da der Kontoname für bestehende SACL-Einträge nicht geändert werden kann, sind alle SACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren zu entfernen, neue SACL-Einträge mit den korrigierten Zielkontonamen zu erstellen und diese neuen SACL-Einträge den entsprechenden Sicherheitsdeskriptoren zuzuordnen.

Alle notwendigen Änderungen an den lokalen Benutzern oder Gruppen, die in der Dateiverzeichnisrichtlinienkonfiguration verwendet werden, sind vorzunehmen, bevor die Richtlinie angewendet wird; andernfalls schlägt der Anwendungsvorgang fehl.

Dateisicherheit für NTFS-Dateien und Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden

Erstellen von NTFS-Sicherheitsdeskriptoren auf ONTAP SMB Servern

Das Erstellen eines NTFS-Sicherheitsdeskriptors (Dateisicherheitsrichtlinie) ist der erste Schritt beim Konfigurieren und Anwenden von NTFS-Zugriffssteuerungslisten (ACLs) auf Dateien und Ordner innerhalb von Storage Virtual Machines (SVMs). Der Sicherheitsdeskriptor kann in einer Richtlinienaufgabe dem Datei- oder Ordnerpfad

zugeordnet werden.

Über diese Aufgabe

Sie können NTFS-Sicherheitsdeskriptoren für Dateien und Ordner erstellen, die sich in NTFS-Sicherheitsstil-Volumes befinden, oder für Dateien und Ordner, die sich auf Volumes mit gemischtem Sicherheitsstil befinden.

Standardmäßig werden beim Erstellen eines Sicherheitsdeskriptors vier Einträge in der diskretionären Zugriffssteuerungsliste (DACL-ACEs) zu diesem Sicherheitsdeskriptor hinzugefügt. Die vier Standard-ACEs sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Wo die Berechtigungen angewendet werden
BUILTIN\Administratoren	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
BUILTIN\Users	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
ERSTELLER-BESITZER	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Eigentümer des Sicherheitsdeskriptors
- Primärgruppe des Eigentümers
- Rohsteuer-Flags

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen befinden sich in der "ONTAP-Befehlsreferenz".

NTFS-DACL-Zugriffssteuerungseinträge zu den NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern hinzufügen

Das Hinzufügen von DACL (discretionary access control list) Zugriffssteuerungsliste-Zugriffssteuerungseinträgen (ACEs) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Konfiguration und Anwendung von NTFS-ACLs auf eine Datei oder einen Ordner. Jeder Eintrag legt fest, welchem Objekt der Zugriff erlaubt oder verweigert wird, und definiert, was das Objekt mit den in der ACE definierten Dateien oder Ordnern tun darf oder nicht tun darf.

Über diese Aufgabe

Der DACL des Sicherheitsdeskriptors kann um eine oder mehrere ACEs ergänzt werden.

Enthält der Sicherheitsdeskriptor eine DACL mit bereits vorhandenen ACEs, wird die neue ACE der DACL hinzugefügt. Enthält der Sicherheitsdeskriptor keine DACL, wird die DACL erstellt und die neue ACE hinzugefügt.

Sie können DACL-Einträge optional anpassen, indem Sie festlegen, welche Rechte Sie für das im `-account`

Parameter angegebene Konto erlauben oder verweigern möchten. Es gibt drei sich gegenseitig ausschließende Methoden zur Angabe von Rechten:

- Rechte
- Erweiterte Rechte
- Rohrechte (erweiterte Berechtigung)

> Wenn Sie keine Rechte für den DACL-Eintrag angeben, werden die Rechte standardmäßig auf `Full Control` gesetzt.

DACL-Einträge lassen sich optional anpassen, indem festgelegt wird, wie die Vererbung angewendet wird.

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einen DACL-Eintrag zu einem Sicherheitsdeskriptor hinzufügen: `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. Es sollte überprüft werden, 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
   ```

Weitere Informationen zu `vserver security file-directory ntfs dacl` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SMB Sicherheitsrichtlinien erstellen

Das Erstellen einer Dateisicherheitsrichtlinie für SVMs ist der dritte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten auf eine Datei oder einen Ordner. Eine Richtlinie dient als Container für verschiedene Aufgaben, wobei jede Aufgabe einen einzelnen Eintrag darstellt, der auf Dateien oder Ordner angewendet

werden kann. Aufgaben können der Sicherheitsrichtlinie später hinzugefügt werden.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollte die Sicherheitsrichtlinie mit jedem SVM (das NTFS-Sicherheitsstil-Volumes oder gemischte Sicherheitsstil-Volumes enthält) verknüpft werden.

Schritte

1. Eine 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. Die Sicherheitsrichtlinie wird überprüft: `vserver security file-directory policy show`

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

Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe wird diese einer Sicherheitsrichtlinie zugeordnet. Einer Sicherheitsrichtlinie können ein oder mehrere Aufgabeneinträge hinzugefügt werden.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf eine einzelne Operation, die von einer Sicherheitsrichtlinie an Dateien oder Ordnern mit NTFS- oder gemischter Sicherheit (oder an einem Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Dient zur Festlegung von Aufgaben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. Über Datei- und Verzeichnisaufgaben angewendete ACLs können mit SMB-Clients oder der ONTAP CLI verwaltet werden.

- Storage-Level Access Guard Aufgaben

  Dient zur Angabe von Aufgaben, die Storage-Level Access Guard-Sicherheitsdeskriptoren auf ein bestimmtes Volume anwenden. ACLs, die durch Storage-Level Access Guard-Aufgaben angewendet werden, können nur über die ONTAP CLI verwaltet werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder einer

Gruppe von Dateien (oder Ordnern). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Innerhalb einer Richtlinie kann es pro Pfad nur eine Aufgabe geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10.000 Aufgabeneinträge vorhanden sein.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Auch wenn eine Richtlinie mehr als eine Aufgabe enthalten kann, kann eine Richtlinie nicht so konfiguriert werden, dass sie sowohl Aufgaben für Dateiverzeichnisse als auch Storage-Level Access Guard-Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

- Storage-Level Access Guard wird verwendet, um Berechtigungen einzuschränken.

  Es gibt niemals zusätzliche Zugriffsrechte.

Beim Hinzufügen von Aufgaben zu Sicherheitsrichtlinien müssen die folgenden vier erforderlichen Parameter angegeben werden:

- SVM-Name
- Richtlinienname
- Pfad
- Sicherheitsdeskriptor, der dem Pfad zugeordnet wird

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition
- Zugriffskontrolltyp

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einer Sicherheitsrichtlinie wird eine Aufgabe mit zugehörigem Sicherheitsdeskriptor hinzugefügt: `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 den `-access-control` Parameter. Die Angabe des Zugriffskontrolltyps bei der Konfiguration von Datei- und Verzeichniszugriffsaufgaben 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. Die Konfiguration der Richtlinienaufgabe überprüfen: `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
```

Weitere Informationen zu `vserver security file-directory policy task` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SMB-Sicherheitsrichtlinien anwenden

Das Anwenden einer Dateisicherheitsrichtlinie auf SVMs ist der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner.

Über diese Aufgabe

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

> Beim Anwenden einer Überwachungsrichtlinie und zugehöriger SACLs werden alle vorhandenen DACLs überschrieben. Beim Anwenden einer Sicherheitsrichtlinie und der zugehörigen DACLs werden alle vorhandenen DACLs überschrieben. Vor dem Erstellen und Anwenden neuer Sicherheitsrichtlinien empfiehlt sich eine Überprüfung der bestehenden Richtlinien.

Schritt

1. Eine Sicherheitsrichtlinie anwenden: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

   Der Auftrag zur Anwendung der Richtlinie wird eingeplant 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
   ```

ONTAP SMB-Sicherheitsrichtlinienaufträge überwachen

Beim Anwenden der Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) kann der Fortschritt der Aufgabe überwacht werden, indem der Sicherheitsrichtlinienauftrag

überwacht wird. Dies ist hilfreich, wenn festgestellt werden soll, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn ein lang andauernder Auftrag vorliegt, bei dem eine Sicherheitsrichtlinie auf eine große Anzahl von Dateien und Ordnern angewendet wird.

Über diese Aufgabe

Um detaillierte Informationen zu einem Sicherheitsrichtlinienauftrag anzuzeigen, sollte der `-instance` Parameter verwendet werden.

Schritt

1. Der Auftrag zur Sicherheitsrichtlinie wird überwacht: `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
   ```

Die Sicherheit von ONTAP SMB-Dateien überprüfen

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, die die Daten enthält, sowie den Pfad zu den Dateien und Ordnern angeben, deren Sicherheitseinstellungen überprüft werden sollen. Der optionale `-expand-mask`Parameter kann verwendet werden, um detaillierte Informationen zu den Sicherheitseinstellungen anzuzeigen.

Schritt

1. Datei- und Ordnersicherheitseinstellungen 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
```

Überwachungsrichtlinien für NTFS-Dateien und -Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden

ONTAP Befehle zum Konfigurieren und Anwenden von SMB-Überwachungsrichtlinien auf NTFS-Dateien und Ordner

Es sind mehrere Schritte erforderlich, um Überwachungsrichtlinien auf NTFS-Dateien und -Ordner mit der ONTAP CLI anzuwenden. Zuerst wird ein NTFS-Sicherheitsdeskriptor erstellt und SACLs zu diesem Sicherheitsdeskriptor hinzugefügt. Anschließend wird eine Sicherheitsrichtlinie erstellt und Richtlinienaufgaben hinzugefügt. Danach wird die Sicherheitsrichtlinie auf eine Storage Virtual Machine (SVM) angewendet.

Über diese Aufgabe

Nach der Anwendung der Sicherheitsrichtlinie können Sie den Sicherheitsrichtlinienauftrag überwachen und anschließend die Einstellungen für die angewendete Audit-Richtlinie überprüfen.

> Beim Anwenden einer Überwachungsrichtlinie und zugehöriger SACLs werden alle vorhandenen DACLs überschrieben. Vor dem Erstellen und Anwenden neuer Sicherheitsrichtlinien empfiehlt sich eine Überprüfung der bestehenden Richtlinien.

Verwandte Informationen

- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard
- Informationen zu den Grenzen bei der Verwendung von Befehlen zum Festlegen der SMB-Datei- und

Ordnersicherheit

- Sicherheitsdeskriptoren werden verwendet, um die Sicherheit von Dateien und Ordnern festzulegen.
- "SMB und NFS Auditierung und Sicherheitsverfolgung"
- NTFS-Sicherheitsdeskriptoren auf Servern erstellen

Erstellen von NTFS-Sicherheitsdeskriptoren auf ONTAP SMB Servern

Das Erstellen einer NTFS-Sicherheitsdeskriptor-Überwachungsrichtlinie ist der erste Schritt beim Konfigurieren und Anwenden von NTFS-Zugriffssteuerungslisten (ACLs) auf Dateien und Ordner in SVMs. Der Sicherheitsdeskriptor wird dem Datei- oder Ordnerpfad in einer Richtlinienaufgabe zugeordnet.

Über diese Aufgabe

Sie können NTFS-Sicherheitsdeskriptoren für Dateien und Ordner erstellen, die sich in NTFS-Sicherheitsstil-Volumes befinden, oder für Dateien und Ordner, die sich auf Volumes mit gemischtem Sicherheitsstil befinden.

Standardmäßig werden beim Erstellen eines Sicherheitsdeskriptors vier Einträge in der diskretionären Zugriffssteuerungsliste (DACL-ACEs) zu diesem Sicherheitsdeskriptor hinzugefügt. Die vier Standard-ACEs sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Wo die Berechtigungen angewendet werden
BUILTIN\Administratoren	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
BUILTIN\Users	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
ERSTELLER-BESITZER	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Eigentümer des Sicherheitsdeskriptors
- Primärgruppe des Eigentümers
- Rohsteuer-Flags

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Wenn Sie die erweiterten Parameter verwenden möchten, die Berechtigungsstufe auf „Erweitert“ setzen: `set -privilege advanced`
2. Ein Sicherheitsdeskriptor wird erstellt: `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. Es sollte überprüft werden, ob 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, zur Administrator-Berechtigungsebene zurückkehren: `set -privilege admin`

NTFS-SACL-Zugriffssteuerungseinträge zu den NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern hinzufügen

Das Hinzufügen von SACL (system access control list) Zugriffssteuerungsliste-Zugriffskontrolleinträgen (ACEs) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt beim Erstellen von NTFS-Überwachungsrichtlinien für Dateien oder Ordner in SVMs. Jeder Eintrag identifiziert den Benutzer oder die Gruppe, die überwacht werden soll. Der SACL-Eintrag definiert, ob erfolgreiche oder fehlgeschlagene Zugriffsversuche protokolliert werden sollen.

Über diese Aufgabe

Der SACL des Sicherheitsdeskriptors kann um eine oder mehrere ACEs ergänzt werden.

Enthält der Sicherheitsdeskriptor eine SACL mit bereits vorhandenen ACEs, wird die neue ACE der SACL hinzugefügt. Enthält der Sicherheitsdeskriptor keine SACL, wird die SACL erstellt und die neue ACE hinzugefügt.

Sie können SACL-Einträge konfigurieren, indem Sie festlegen, welche Rechte für erfolgreiche oder fehlgeschlagene Ereignisse für das im `-account` Parameter angegebene Konto geprüft werden sollen. Es gibt drei sich gegenseitig ausschließende Methoden zur Angabe von Rechten:

- Rechte
- Erweiterte Rechte
- Rohrechte (erweiterte Berechtigung)

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

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

Schritte

1. Einen SACL-Eintrag zu einem Sicherheitsdeskriptor hinzufügen: `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. Es sollte überprüft werden, ob der SACL-Eintrag 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
   ```

ONTAP SMB Sicherheitsrichtlinien erstellen

Das Erstellen einer Überwachungsrichtlinie für Storage Virtual Machines (SVMs) ist der dritte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten (ACLs) auf eine Datei oder einen Ordner. Eine Richtlinie dient als Container für verschiedene Aufgaben, wobei jede Aufgabe einen einzelnen Eintrag darstellt, der auf Dateien oder Ordner angewendet werden kann. Aufgaben können der Sicherheitsrichtlinie später hinzugefügt werden.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollte die Sicherheitsrichtlinie mit jeder Storage Virtual Machine (SVM) (die NTFS-Sicherheitsstil-Volumes oder gemischte Sicherheitsstil-Volumes enthält) verknüpft werden.

Schritte

1. Eine 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. Die Sicherheitsrichtlinie wird überprüft: `vserver security file-directory policy show`

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

Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe wird diese einer Sicherheitsrichtlinie zugeordnet. Einer Sicherheitsrichtlinie können ein oder mehrere Aufgabeneinträge hinzugefügt werden.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf eine einzelne Operation, die von einer Sicherheitsrichtlinie an Dateien oder Ordnern mit NTFS- oder gemischter Sicherheit (oder an einem Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Dient zur Festlegung von Aufgaben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. Über Datei- und Verzeichnisaufgaben angewendete ACLs können mit SMB-Clients oder der ONTAP CLI verwaltet werden.

- Storage-Level Access Guard Aufgaben

  Dient zur Angabe von Aufgaben, die Storage-Level Access Guard-Sicherheitsdeskriptoren auf ein bestimmtes Volume anwenden. ACLs, die durch Storage-Level Access Guard-Aufgaben angewendet werden, können nur über die ONTAP CLI verwaltet werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder einer Gruppe von Dateien (oder Ordnern). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Innerhalb einer Richtlinie kann es pro Pfad nur eine Aufgabe geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10.000 Aufgabeneinträge vorhanden sein.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Auch wenn eine Richtlinie mehr als eine Aufgabe enthalten kann, kann eine Richtlinie nicht so konfiguriert werden, dass sie sowohl Aufgaben für Dateiverzeichnisse als auch Storage-Level Access Guard-Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

- Storage-Level Access Guard wird verwendet, um Berechtigungen einzuschränken.

  Es gibt niemals zusätzliche Zugriffsrechte.

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition
- Zugriffskontrolltyp

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einer Sicherheitsrichtlinie wird eine Aufgabe mit zugehörigem Sicherheitsdeskriptor hinzugefügt: `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 den `-access-control` Parameter. Die Angabe des Zugriffskontrolltyps bei der Konfiguration von Datei- und Verzeichniszugriffsaufgaben 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. Die Konfiguration der Richtlinienaufgabe überprüfen: `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
   ```

Weitere Informationen zu `vserver security file-directory policy task` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SMB-Sicherheitsrichtlinien anwenden

Das Anwenden einer Überwachungsrichtlinie auf SVMs ist der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner.

Über diese Aufgabe

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

> Beim Anwenden einer Überwachungsrichtlinie und zugehöriger SACLs werden alle vorhandenen DACLs überschrieben. Beim Anwenden einer Sicherheitsrichtlinie und der zugehörigen DACLs werden alle vorhandenen DACLs überschrieben. Vor dem Erstellen und Anwenden neuer Sicherheitsrichtlinien empfiehlt sich eine Überprüfung der bestehenden Richtlinien.

Schritt

1. Eine Sicherheitsrichtlinie anwenden: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

   Der Auftrag zur Anwendung der Richtlinie wird eingeplant 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
   ```

ONTAP SMB-Sicherheitsrichtlinienaufträge überwachen

Beim Anwenden der Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) kann der Fortschritt der Aufgabe überwacht werden, indem der Sicherheitsrichtlinienauftrag überwacht wird. Dies ist hilfreich, wenn festgestellt werden soll, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn ein lang andauernder Auftrag vorliegt, bei dem eine Sicherheitsrichtlinie auf eine große Anzahl von Dateien und Ordnern angewendet wird.

Über diese Aufgabe

Um detaillierte Informationen zu einem Sicherheitsrichtlinienauftrag anzuzeigen, sollte der `-instance` Parameter verwendet werden.

Schritt

1. Der Auftrag zur Sicherheitsrichtlinie wird überwacht: `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
   ```

ONTAP SMB Auditrichtlinien überprüfen

Die Überwachungsrichtlinie kann überprüft werden, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die die Sicherheitsrichtlinie angewendet wurde, die gewünschten Überwachungssicherheitseinstellungen aufweisen.

Über diese Aufgabe

Sie verwenden den `vserver security file-directory show` Befehl, um Informationen zur Überwachungsrichtlinie anzuzeigen. Es muss der Name der SVM, die die Daten enthält, sowie der Pfad zu den Daten angegeben werden, deren Datei- oder Ordner-Überwachungsrichtlinieninformationen angezeigt werden sollen.

Schritt

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

Beispiel

Der folgende Befehl zeigt die auf den Pfad “/corp” in SVM vs1 angewendeten Überwachungsrichtlinieninformationen an. Auf den Pfad sind sowohl ein SUCCESS- als auch ein SUCCESS/FAIL-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
```

Informationen zur Verwaltung von ONTAP SMB-Sicherheitsrichtlinienjobs

Wenn ein Sicherheitsrichtlinienauftrag existiert, kann unter bestimmten Umständen diese Sicherheitsrichtlinie oder die der Richtlinie zugewiesenen Aufgaben nicht geändert werden. Es ist wichtig zu verstehen, unter welchen Bedingungen Sicherheitsrichtlinien geändert werden können oder nicht, damit etwaige Änderungsversuche erfolgreich sind. Zu den Änderungen an der Richtlinie zählen 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 dieser Richtlinie zugewiesene Aufgabe nicht ändern, wenn ein Auftrag für diese Richtlinie existiert und sich dieser Auftrag in einem der folgenden Zustände befindet:

- Der Auftrag wird ausgeführt oder ist in Bearbeitung.
- Der Auftrag ist pausiert.
- Der Auftrag wird fortgesetzt und befindet sich im Status „Wird ausgeführt“.
- Wenn der Job auf das Failover zu einem anderen Knoten wartet.

Unter den folgenden Umständen ist es möglich, eine Sicherheitsrichtlinie oder eine dieser Richtlinie zugewiesene Aufgabe erfolgreich zu ändern, sofern ein Auftrag für eine Sicherheitsrichtlinie existiert:

- Der Policy Job wurde gestoppt.
- Der Policy-Job wurde erfolgreich abgeschlossen.

ONTAP Befehle zur Verwaltung von NTFS- und SMB-Sicherheitsrichtlinien und Zugriffskontrolleinträgen

Mit ONTAP-Befehlen können Sie NTFS-Sicherheitsdeskriptoren und Zugriffssteuerungseinträge (ACEs) in DACLs und SACLs erstellen, ändern, löschen und Informationen dazu anzeigen. Sie können auch ONTAP-Befehle verwenden, um SMB-Sicherheitsrichtlinien, Richtlinienaufgaben und Richtlinienaufträge zu verwalten.

ONTAP Befehle zur Verwaltung von NTFS-Sicherheitsdeskriptoren auf SMB-Servern

Für die Verwaltung von Sicherheitsdeskriptoren stehen spezielle ONTAP Befehle zur Verfügung. Sie können Sicherheitsdeskriptoren erstellen, ändern, löschen und Informationen darüber anzeigen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
NTFS-Sicherheitsdeskriptoren erstellen	`vserver security file-directory ntfs create`
Vorhandene NTFS-Sicherheitsdeskriptoren ändern	`vserver security file-directory ntfs modify`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen zu vorhandenen NTFS-Sicherheitsdeskriptoren anzeigen	`vserver security file-directory ntfs show`
NTFS-Sicherheitsdeskriptoren löschen	`vserver security file-directory ntfs delete`

Weitere Informationen zu `vserver security file-directory ntfs` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NTFS DACL-Zugriffskontrolleinträgen auf SMB-Servern

Für die Verwaltung von DACL-Zugriffskontrolleinträgen (ACEs) stehen spezielle ONTAP Befehle zur Verfügung. Es ist möglich, ACEs jederzeit zu NTFS DACLs hinzuzufügen. Auch die Verwaltung bestehender NTFS DACLs durch Ändern, Löschen und Anzeigen von Informationen zu ACEs in DACLs ist möglich.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
ACEs erstellen und zu NTFS-DACLs hinzufügen	`vserver security file-directory ntfs dacl add`
Vorhandene ACEs in NTFS-DACLs ändern	`vserver security file-directory ntfs dacl modify`
Informationen zu vorhandenen ACEs in NTFS-DACLs	`vserver security file-directory ntfs dacl show`
Vorhandene ACEs aus NTFS-DACLs entfernen	`vserver security file-directory ntfs dacl remove`

Weitere Informationen zu `vserver security file-directory ntfs dacl` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NTFS SACL-Zugriffskontrolleinträgen auf SMB-Servern

Für die Verwaltung von SACL-Zugriffskontrolleinträgen (ACEs) stehen spezielle ONTAP Befehle zur Verfügung. ACEs können jederzeit zu NTFS SACLs hinzugefügt werden. Auch die Verwaltung bestehender NTFS SACLs durch Ändern, Löschen und Anzeigen von Informationen zu ACEs in SACLs ist möglich.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
ACEs erstellen und zu den NTFS-SACLs hinzufügen	`vserver security file-directory ntfs sacl add`
Vorhandene ACEs in NTFS-SACLs ändern	`vserver security file-directory ntfs sacl modify`
Informationen zu vorhandenen ACEs in NTFS-SACLs anzeigen	`vserver security file-directory ntfs sacl show`
Vorhandene ACEs aus den NTFS-SACLs entfernen	`vserver security file-directory ntfs sacl remove`

Weitere Informationen zu `vserver security file-directory ntfs sacl` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von SMB-Sicherheitsrichtlinien

Für die Verwaltung von Sicherheitsrichtlinien stehen spezielle ONTAP Befehle zur Verfügung. Es können Informationen zu Richtlinien angezeigt und Richtlinien gelöscht werden. Eine Sicherheitsrichtlinie kann nicht geändert werden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinien erstellen	`vserver security file-directory policy create`
Informationen zu Sicherheitsrichtlinien	`vserver security file-directory policy show`
Sicherheitsrichtlinien löschen	`vserver security file-directory policy delete`

Weitere Informationen zu `vserver security file-directory policy` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von SMB-Sicherheitsrichtlinienaufgaben

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

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinienaufgaben hinzufügen	`vserver security file-directory policy task add`
Aufgaben zur Änderung der Sicherheitsrichtlinie	`vserver security file-directory policy task modify`
Informationen zu Aufgaben der Sicherheitsrichtlinie	`vserver security file-directory policy task show`
Sicherheitsrichtlinien-Aufgaben entfernen	`vserver security file-directory policy task remove`

Weitere Informationen zu `vserver security file-directory policy task` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von SMB Security Policy Jobs

Es gibt ONTAP Befehle zum Anhalten, Fortsetzen, Stoppen und Anzeigen von Informationen über Sicherheitsrichtlinienaufträge.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinien-Jobs pausieren	`vserver security file-directory job pause -vserver vserver_name -id integer`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinien-Jobs fortsetzen	`vserver security file-directory job resume -vserver vserver_name -id integer`
Informationen zu Sicherheitsrichtlinien-Jobs anzeigen	`vserver security file-directory job show -vserver vserver_name`Die Job-ID eines Jobs lässt sich mit diesem Befehl ermitteln.
Sicherheitsrichtlinien-Jobs stoppen	`vserver security file-directory job stop -vserver vserver_name -id integer`

Weitere Informationen zu `vserver security file-directory job` finden sich in der "ONTAP-Befehlsreferenz".

Den Metadatencache für SMB-Freigaben konfigurieren

Metadaten-Caching ermöglicht das Zwischenspeichern von Dateiattributen auf SMB 1.0 Clients, um einen schnelleren Zugriff auf Datei- und Ordnerattribute zu bieten. Das Attribut-Caching kann für jede Freigabe einzeln aktiviert oder deaktiviert werden. Die Gültigkeitsdauer (Time-to-Live) der zwischengespeicherten Einträge kann ebenfalls konfiguriert werden, wenn Metadaten-Caching aktiviert ist. Eine Konfiguration des Metadaten-Cachings ist nicht erforderlich, wenn Clients über SMB 2.x oder SMB 3.0 auf Freigaben zugreifen.

Wenn diese Funktion aktiviert ist, speichert der SMB-Metadatencache Pfad- und Dateiattributdaten für eine begrenzte Zeit. Dies kann die SMB-Leistung für SMB 1.0 Clients mit gängigen Arbeitslasten verbessern.

Bei bestimmten Aufgaben erzeugt SMB ein erhebliches Datenaufkommen, das mehrere identische Abfragen für Pfad- und Dateimetadaten enthalten kann. Die Anzahl redundanter Abfragen lässt sich reduzieren und die Leistung für SMB 1.0 Clients verbessern, wenn SMB-Metadaten-Caching verwendet wird, um die Informationen stattdessen aus dem Cache abzurufen.

> Es ist zwar unwahrscheinlich, aber möglich, dass der Metadaten-Cache veraltete Informationen an SMB 1.0-Clients ausliefert. Falls dieses Risiko in Ihrer Umgebung nicht akzeptabel ist, sollte diese Funktion nicht aktiviert werden.

Der ONTAP SMB-Metadaten-Cache kann aktiviert werden.

Die SMB-Leistung für SMB 1.0-Clients lässt sich durch Aktivierung des SMB-Metadaten-Caches verbessern. Standardmäßig ist die SMB-Metadaten-Zwischenspeicherung deaktiviert.

Schritt

1. Aktivieren Sie das SMB-Metadaten-Caching für eine neue oder bestehende Freigabe:
   - Aktivieren Sie das SMB-Metadaten-Caching beim Erstellen einer neuen Freigabe:

```
vserver cifs share create -vserver <SVM_name> -share-name
<share_name> -path <path> -share-properties attributecache
```

- Aktivieren Sie das SMB-Metadaten-Caching für eine vorhandene Freigabe:

```
vserver cifs share properties add -vserver <SVM_name> -share-name
<share_name> -share-properties attributecache
```

Die Lebensdauer von ONTAP SMB Metadaten-Cache-Einträgen konfigurieren

Sie können die Lebensdauer von SMB-Metadaten-Cache-Einträgen konfigurieren, um die Leistung 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 die SMB-Metadaten-Cache-Funktion nicht aktiviert ist, wird die SMB-Cache-TTL-Einstellung nicht verwendet.

Schritt

1. Konfigurieren Sie die Lebensdauer von SMB-Metadaten-Cache-Einträgen auf einer neuen oder vorhandenen Freigabe:
   - Konfigurieren Sie die Lebensdauer von SMB-Metadaten-Cache-Einträgen beim Erstellen einer neuen Freigabe:

```
vserver cifs share create -vserver <SVM_name> -share-name
<share_name> -path <path> -attribute-cache-ttl
[integerh][integerm][integers]
```

   - Konfigurieren der Lebensdauer von SMB-Metadaten-Cache-Einträgen auf einer vorhandenen Freigabe:

```
vserver cifs share modify -vserver <SVM_name> -share-name
<share_name> -attribute-cache-ttl [integerh][integerm][integers]
```

Beim Erstellen oder Ändern von Freigaben können Sie zusätzliche Konfigurationsoptionen und Eigenschaften festlegen. Weitere Informationen zu `vserver cifs share` finden sich in der "ONTAP-Befehlsreferenz".

Dateisperren verwalten

Informationen zur ONTAP SMB-Dateisperrung zwischen Protokollen

Die Dateisperrung ist eine Methode, mit der Clientanwendungen 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.

Handelt es sich beim Client um einen NFS-Client, sind Sperren empfehlend; handelt es sich beim Client um einen SMB-Client, sind Sperren obligatorisch.

Aufgrund von Unterschieden zwischen den Dateisperren von NFS und SMB kann es vorkommen, dass ein NFS-Client nicht auf eine Datei zugreifen kann, die zuvor von einer SMB-Anwendung geöffnet wurde.

Folgendes geschieht, wenn ein NFS-Client versucht, auf eine von einer SMB-Anwendung gesperrte Datei zuzugreifen:

- In gemischten oder NTFS-Volumes können Dateimanipulationsvorgänge wie `rm`, `rmdir` und `mv` dazu führen, dass die NFS-Anwendung fehlschlägt.
- NFS-Lese- und Schreibvorgänge werden durch die SMB-Öffnungsmodi deny-read und deny-write jeweils für lesen bzw. schreiben verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei mit einer exklusiven SMB-Bytesperre gesperrt ist.
- Link aufheben
  - Für NTFS-Dateisysteme werden SMB- und CIFS-Löschvorgänge unterstützt.

    Die Datei wird nach dem letzten Schließen gelöscht.
  - NFS unlink-Operationen werden nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind und die Operation „Letztes Löschen beim Schließen“ für NFS nicht unterstützt wird.
  - Für UNIX-Dateisysteme wird die Operation "unlink" unterstützt.

    Es wird unterstützt, da NFS- und UNIX-Semantik erforderlich sind.
- Umbenennen
  - Für NTFS-Dateisysteme kann die Zieldatei umbenannt werden, wenn sie über SMB oder CIFS geöffnet wird.
  - NFS-Umbenennung wird nicht unterstützt.

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

In UNIX-Sicherheitsstil-Volumes ignorieren NFS-Unlink- und Rename-Operationen den SMB-Sperrstatus und ermöglichen den Zugriff auf die Datei. Alle anderen NFS-Operationen auf UNIX-Sicherheitsstil-Volumes berücksichtigen den SMB-Sperrstatus.

Informationen zu schreibgeschützten Bits in ONTAP SMB

Das Schreibschutzbit wird für jede Datei einzeln gesetzt, um anzuzeigen, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients unter Windows können ein schreibgeschütztes Bit pro Datei setzen. NFS-Clients setzen kein schreibgeschütztes Bit pro Datei, da NFS-Clients keine Protokolloperationen haben, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann das Schreibschutzbit einer Datei setzen, wenn diese von einem SMB-Client unter Windows erstellt wird. ONTAP kann das Schreibschutzbit auch setzen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Manche Software erfordert, dass das Schreibschutzbit aktiviert ist, wenn sie von NFS-Clients und SMB-Clients verwendet wird.

Damit ONTAP die korrekten Lese- und Schreibberechtigungen für eine zwischen NFS-Client und SMB-Client gemeinsam genutzte Datei beibehält, wird das Schreibschutzbit nach den folgenden Regeln behandelt:

- NFS behandelt jede Datei, bei der das Schreibschutzbit aktiviert ist, so, als ob keine Schreibberechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Schreibberechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert war, aktiviert ONTAP das Schreibschutzbit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungsbit aktiviert, deaktiviert ONTAP das Nur-Lesen-Bit für diese Datei.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein NFS-Client versucht, die 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, wobei die Schreibberechtigungsbits maskiert sind.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein SMB-Client das Schreibschutzbit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien, bei denen das Schreibschutzbit aktiviert ist, sind nur für root beschreibbar.

Das Schreibschutzbit interagiert mit den ACL- und Unix-Modusbits auf folgende Weise:

Wenn das Schreibschutzbit einer Datei gesetzt ist:

- An der ACL für diese Datei werden keine Änderungen vorgenommen. NFS-Clients sehen dieselbe ACL wie vor dem Setzen des Schreibschutzbits.
- Sämtliche Unix-Modusbits, die Schreibzugriff auf die Datei ermöglichen, werden ignoriert.
- Sowohl NFS- als auch SMB-Clients können die Datei lesen, aber sie können sie nicht verändern.
- ACLs und UNIX-Modusbits werden zugunsten des Schreibschutzbits ignoriert. Das bedeutet, dass selbst wenn die ACL Schreibzugriff erlaubt, das Schreibschutzbit Änderungen verhindert.

Wenn das Schreibschutzbit einer Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff anhand der ACL und der UNIX-Modusbits.
  - Wenn entweder die ACL oder die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei nicht ändern.
  - Wenn weder die ACL noch die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.

Änderungen an Dateiberechtigungen werden auf SMB-Clients sofort wirksam, auf NFS-Clients hingegen möglicherweise nicht sofort, wenn der NFS-Client das Attribut-Caching aktiviert.

Wie ONTAP sich von Windows bei der Handhabung von Sperren auf freigegebenen Pfadkomponenten unterscheidet

Im Gegensatz zu Windows sperrt ONTAP nicht die einzelnen Komponenten des Pfades zu einer geöffneten Datei, solange die Datei geöffnet ist. Dieses Verhalten betrifft auch SMB-Freigabepfade.

Da ONTAP die einzelnen Pfadkomponenten nicht sperrt, ist es möglich, eine Pfadkomponente oberhalb der geöffneten Datei oder Freigabe umzubenennen, was bei bestimmten Anwendungen zu Problemen führen oder den Freigabepfad in der SMB-Konfiguration ungültig machen kann. Dies kann dazu führen, dass die Freigabe nicht zugänglich ist.

Um Probleme zu vermeiden, die durch das Umbenennen von Pfadkomponenten entstehen, lassen sich

Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Informationen zu ONTAP SMB-Sperren anzeigen

Informationen über die aktuellen Dateisperren können angezeigt werden, einschließlich der Art der gehaltenen Sperren und des Sperrstatus, Details zu Bytebereichssperren, Sharelock-Modi, Delegation Locks und Opportunistic Locks sowie darüber, ob Sperren mit dauerhaften oder persistenten Handles geöffnet sind.

Über diese Aufgabe

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

Standardmäßig zeigt der Befehl Informationen zu allen Sperren an. Mit Befehlsparametern lässt sich die Anzeige von Informationen zu Sperren für eine bestimmte Storage Virtual Machine (SVM) steuern oder die Ausgabe des Befehls nach anderen Kriterien filtern.

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

- Byte-Range-Sperren, die nur einen Teil einer Datei sperren.
- Freigabesperren, die geöffnete Dateien sperren.
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Client-seitige Caching über NFSv4.x steuern.

Durch die Angabe optionaler Parameter lassen sich wichtige Informationen zu jedem Sperrtyp ermitteln. Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Informationen zu Sperren werden mit dem `vserver locks show` Befehl angezeigt.

Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen zu einer NFSv4-Sperre für eine Datei mit dem Pfad `/vol1/file1`. Der Zugriffsmodus von Sharelock ist write-deny_none, und die Sperre wurde mit 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 Sharelock-Informationen zur SMB-Sperre einer Datei mit

dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird für die Datei mit dem Sharelock-Zugriffsmodus write-deny_none an einen Client mit der IP-Adresse 10.3.1.3 gewährt. Ein Lease-Oplock wird mit dem Oplock-Level Batch 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
```

ONTAP SMB-Sperren aufheben

Wenn Dateisperren den Zugriff von Clients auf Dateien verhindern, können Informationen über die aktuell bestehenden Sperren angezeigt und anschließend bestimmte Sperren aufgehoben werden. Beispiele für Szenarien, in denen das Aufheben von Sperren erforderlich sein kann, sind das Debuggen von Anwendungen.

Über diese Aufgabe

Der `vserver locks break`Befehl ist nur auf der erweiterten Berechtigungsstufe und höher verfügbar. Weitere Informationen zu `vserver locks break` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Um die Informationen zu finden, die Sie zum Aufheben einer Sperre benötigen, verwenden Sie den `vserver locks show` Befehl.

   Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
3. Führen Sie eine der folgenden Aktionen aus:

Wenn ein Schloss durch Angabe von… aufgehoben werden soll	Geben Sie den Befehl ein…
Der SVM Name, der Volumenname, 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 Administratorrechteebene: `set -privilege admin`

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

SMB-Aktivitäten überwachen

ONTAP SMB-Sitzungsinformationen anzeigen

Sie können Informationen zu bestehenden SMB-Sitzungen anzeigen, darunter die SMB-Verbindungs- und Sitzungs-ID sowie die IP-Adresse der Workstation, die die Sitzung nutzt. Sie können Informationen zur Protokollversion der Sitzung und zum kontinuierlich verfügbaren Schutzniveau anzeigen, was dabei hilft zu erkennen, ob die Sitzung unterbrechungsfreie Vorgänge unterstützt.

Über diese Aufgabe

Sie können Informationen zu allen Sitzungen Ihrer SVM in zusammengefasster Form anzeigen. In vielen Fällen ist die Ausgabemenge jedoch sehr groß. Welche Informationen in der Ausgabe angezeigt werden, lässt sich durch optionale Parameter anpassen:

- Der optionale `-fields`Parameter ermöglicht die Anzeige von Ausgaben zu den ausgewählten Feldern.

  Sie können `-fields ?` eingeben, um festzustellen, welche Felder Sie verwenden können.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über bestehende SMB-Sitzungen anzuzeigen.
- Sie können den `-fields` Parameter oder den `-instance` Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
Für alle Sitzungen auf der SVM in zusammengefasster Form	`vserver cifs session show -vserver vserver_name`
Bei einer bestimmten Verbindungs-ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
Von einer bestimmten Workstation IP-Adresse	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
An einer bestimmten LIF-IP-Adresse	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Auf einem bestimmten Knoten	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	Von einem bestimmten Windows-Benutzer
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Mit einem festgelegten Authentifizierungsmechanismus

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Mit einer bestimmten Protokollversion	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== Der permanent verfügbare Schutz und SMB Multichannel sind nur für SMB 3.0 und höhere Sitzungen verfügbar. Um deren Status für alle qualifizierenden Sitzungen anzuzeigen, sollte dieser Parameter mit dem Wert `SMB3` oder höher angegeben werden. ====
Mit einem festgelegten Niveau an kontinuierlich verfügbarem Schutz	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Wenn der Status „Dauerhaft verfügbar“ `Partial` ist, bedeutet dies, dass die Sitzung mindestens eine geöffnete, dauerhaft verfügbare Datei enthält, aber auch einige Dateien, die nicht mit dauerhaft verfügbarer Schutz geöffnet sind. Der `vserver cifs sessions file show` Befehl kann verwendet werden, um zu bestimmen, welche Dateien in der bestehenden Sitzung nicht mit dauerhaft verfügbarer Schutz geöffnet sind. ====
Mit einem festgelegten SMB-Signing-Sitzungsstatus	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Beispiele

Der folgende Befehl zeigt Sitzungsinformationen für die Sitzungen auf SVM vs1 an, die von einer Workstation mit der IP-Adresse 10.1.1.1 aufgebaut 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
```

Der folgende Befehl zeigt detaillierte Sitzungsinformationen für Sitzungen mit kontinuierlich verfügbarem Schutz auf SVM vs1 an. Die Verbindung wurde mit dem Domänenkonto 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
```

Der folgende Befehl zeigt Sitzungsinformationen zu einer Sitzung an, die SMB 3.0 und SMB Multichannel auf SVM vs1 verwendet. Im Beispiel hat sich der Benutzer von einem SMB 3.0-fähigen Client über die LIF-IP-Adresse mit dieser Freigabe verbunden; daher wurde als Authentifizierungsmechanismus standardmäßig NTLMv2 verwendet. Die Verbindung muss über Kerberos-Authentifizierung hergestellt werden, um einen dauerhaft verfügbaren Schutz zu gewährleisten.

```
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

Informationen zu geöffneten SMB-Dateien

Informationen zu geöffneten ONTAP SMB-Dateien

Es lassen sich Informationen zu geöffneten SMB-Dateien anzeigen, einschließlich der SMB-Verbindungs- und Sitzungs-ID, des Host-Volumes, des Freigabenamens und des Freigabepfads. Es lassen sich Informationen zum kontinuierlich verfügbaren Schutzniveau einer Datei anzeigen, was hilfreich ist, um festzustellen, ob sich eine geöffnete Datei in einem Zustand befindet, der unterbrechungsfreie Vorgänge unterstützt.

Über diese Aufgabe

Informationen über geöffnete Dateien in einer bestehenden SMB-Sitzung können angezeigt werden. Die angezeigten Informationen sind hilfreich, wenn SMB-Sitzungsinformationen für bestimmte Dateien innerhalb einer SMB-Sitzung ermittelt werden müssen.

Wenn Sie beispielsweise eine SMB-Sitzung haben, bei der einige der geöffneten Dateien mit kontinuierlich verfügbarem Schutz geöffnet sind und andere nicht (der Wert für das `-continuously-available` Feld in `vserver cifs session show` der Befehlsausgabe ist `Partial`), lässt sich mit diesem Befehl ermitteln, welche Dateien nicht kontinuierlich verfügbar sind.

Informationen zu allen geöffneten Dateien in etablierten SMB-Sitzungen auf Storage Virtual Machines (SVMs) können in zusammengefasster Form angezeigt werden, wenn der `vserver cifs session file show` Befehl ohne optionale Parameter verwendet wird.

In vielen Fällen ist die Ausgabemenge jedoch groß. Die angezeigten Informationen lassen sich durch Angabe optionaler Parameter anpassen. Dies kann hilfreich sein, wenn Informationen nur für eine kleine Teilmenge der geöffneten Dateien angezeigt werden sollen.

- Der optionale `-fields`Parameter ermöglicht die Anzeige der Ausgabe auf den von Ihnen ausgewählten Feldern.

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

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über geöffnete SMB-Dateien anzuzeigen.

  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 geöffnete SMB-Dateien anzeigen möchten…	**Führen Sie den folgenden Befehl aus…**
In zusammengefasster Form auf der SVM	`vserver cifs session file show -vserver vserver_name`
Auf einem bestimmten Knoten	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	Bei einer bestimmten Datei-ID
`vserver cifs session file show -vserver vserver_name -file-id integer`	Bei einer bestimmten SMB-Verbindungs-ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Bei einer bestimmten SMB-Sitzungs-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
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	Auf 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 dem festgelegten Niveau an kontinuierlich verfügbarem Schutz

Wenn Sie geöffnete SMB-Dateien anzeigen möchten…	Führen Sie den folgenden Befehl aus…
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Wenn der Status „Dauerhaft verfügbar“ `No` ist, bedeutet dies, dass diese geöffneten Dateien nicht in der Lage sind, sich nach einer Übernahme und Rückgabe unterbrechungsfrei zu erholen. Sie können sich auch nicht von einer allgemeinen Aggregat-Verschiebung zwischen Partnern in einer Hochverfügbarkeitsbeziehung erholen. ====
Mit dem angegebenen wiederverbundenen Zustand	`vserver cifs session file show -vserver vserver_name -reconnected {No

Es gibt zusätzliche optionale Parameter, mit denen Sie die Ausgaberesultate verfeinern können. Weitere Informationen zu `vserver cifs session file show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiele

Das folgende Beispiel zeigt Informationen über geöffnete Dateien auf SVM vs1:

```
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
```

Das folgende Beispiel zeigt detaillierte Informationen zu geöffneten SMB-Dateien mit der Datei-ID 82 auf SVM vs1:

```
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

Sitzungsinformationen anzeigen

Festgestellt werden kann, welche Statistiken, Objekte und Zähler auf ONTAP SMB-Servern verfügbar sind.

Bevor Sie Informationen über CIFS, SMB, Auditing und BranchCache Hash-Statistiken sowie zur Überwachung der Leistung erhalten können, muss bekannt sein, welche Objekte und Zähler verfügbar sind, aus denen Daten gewonnen werden können.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie feststellen möchten…	Eingeben…
Welche Objekte sind verfügbar	`statistics catalog object show`
Spezifische verfügbare Objekte	`statistics catalog object show -object object_name`
Welche Zähler stehen zur Verfügung?	`statistics catalog counter show -object object_name`

   Weitere Informationen zu `statistics catalog object show`, einschließlich der verfügbaren Objekte und Zähler, finden Sie in der "ONTAP-Befehlsreferenz".

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

Beispiele

Der folgende Befehl zeigt Beschreibungen ausgewählter Statistikobjekte im Zusammenhang mit dem CIFS- und SMB-Dateizugriff im Cluster auf der Ebene der erweiterten Berechtigungen an:

```
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
```

Der folgende Befehl zeigt Informationen zu einigen Zählern für das `cifs` Objekt auf der erweiterten Berechtigungsebene an:

Dieses Beispiel zeigt nicht alle verfügbaren Zähler für das `cifs` Objekt; die Ausgabe ist gekürzt.

```
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

- Statistiken anzeigen
- "Statistiken Katalog Zähler Objekt anzeigen"
- "Statistiken Start"

ONTAP SMB Statistiken anzeigen

Es lassen sich verschiedene Statistiken anzeigen, darunter Statistiken zu CIFS und SMB, Auditing und BranchCache-Hashes, um die Leistung zu überwachen und Probleme zu diagnostizieren.

Bevor Sie beginnen

Sie müssen Datenbeispiele mithilfe der `statistics start` und `statistics stop` Befehle gesammelt haben, bevor Sie Informationen über Objekte anzeigen können.

Weitere Informationen zu `statistics start` und `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Statistiken für…	Eingeben…
Alle Versionen von SMB	`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 Knotens	`statistics show -object nblade_cifs`
Multiprotokoll-Audit	`statistics show -object audit_ng`
BranchCache Hash-Dienst	`statistics show -object hashd`
dynamisches DNS	`statistics show -object ddns_update`

   Weitere Informationen zu `statistics show` finden sich in der "ONTAP-Befehlsreferenz".

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

Verwandte Informationen

- Welche Statistiken, Objekte und Zähler auf den Servern verfügbar sind, lässt sich feststellen.
- Überwachung von SMB-signierten Sitzungsstatistiken
- Anzeige der BranchCache Statistiken
- Statistiken dienen zur Überwachung der automatischen Knotenweiterleitungsaktivität.
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"
- "Einrichtung der Leistungsüberwachung"

Copyright-Informationen

Copyright © 2026 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.