Dateizugriff mit SMB einrichten

ONTAP 9

NetApp
October 29, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/security-styles-their-effects-concept.html on October 29, 2026. Always check docs.netapp.com for the latest.

Inhalt

Dateizugriff mit SMB einrichten . . . 1
Sicherheitsstile konfigurieren . . . 1
Informationen zu ONTAP SMB-Sicherheitsstilen und deren Auswirkungen . . . 1
SMB-Sicherheitsstile auf ONTAP SVM Root-Volumes konfigurieren . . . 3
SMB-Sicherheitsstile auf ONTAP FlexVol Volumes konfigurieren . . . 3
SMB-Sicherheitsstile auf ONTAP Qtrees konfigurieren . . . 4
Daten-Volumes in NAS-Namespaces erstellen und verwalten . . . 4
Informationen zum Erstellen und Verwalten von ONTAP SMB-Datenvolumes in NAS-Namespaces . . . 4
ONTAP SMB-Datenvolumes mit angegebenen Verbindungspunkten erstellen . . . 4
ONTAP SMB-Datenvolumes ohne Angabe von Verbindungspunkten erstellen . . . 5
Vorhandene ONTAP SMB-Volumes im NAS-Namespace einbinden oder aushängen . . . 6
Informationen zu ONTAP SMB-Volume-Mounts und Verbindungspunkten anzeigen . . . 8
Namenszuordnungen konfigurieren . . . 9
Informationen zur Konfiguration der ONTAP SMB-Namenszuordnungen . . . 9
Informationen zur ONTAP SMB Namenszuordnung . . . 10
Informationen zu ONTAP SMB Multidomain-Suchen für die Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen . . . 11
Informationen zu den Konvertierungsregeln für die ONTAP SMB-Namenszuordnung . . . 13
ONTAP SMB-Namenszuordnung erstellen . . . 13
Den standardmäßigen ONTAP SMB-Benutzer konfigurieren . . . 14
ONTAP Befehle zur Verwaltung von SMB-Namenszuordnungen . . . 15
Konfiguration von Namenszuordnungssuchen über mehrere Domänen hinweg . . . 15
Aktivieren oder Deaktivieren von ONTAP SMB Multidomain-Namenszuordnungssuchen . . . 15
Vertrauenswürdige ONTAP SMB-Domänen zurücksetzen und neu erkennen . . . 16
Informationen zu erkannten vertrauenswürdigen ONTAP SMB-Domänen . . . 16
Vertrauenswürdige ONTAP SMB-Domänen in bevorzugten Listen hinzufügen, entfernen oder ersetzen . . . 18
Informationen zur bevorzugten vertrauenswürdigen ONTAP SMB-Domänenliste anzeigen . . . 19
SMB-Freigaben erstellen und konfigurieren . . . 20
Informationen zum Erstellen und Konfigurieren von ONTAP SMB-Freigaben . . . 20
Informationen zu den standardmäßigen administrativen ONTAP SMB-Freigaben . . . 20
Informationen zu den Anforderungen an die Benennung von ONTAP SMB-Freigaben . . . 21
Informationen zu den Anforderungen an die Groß-/Kleinschreibung von ONTAP SMB-Verzeichnissen beim Erstellen von Freigaben in einer Multiprotokollumgebung . . . 22
Freigabeeigenschaften zu bestehenden ONTAP SMB-Freigaben hinzufügen oder entfernen . . . 23
ONTAP SMB-Benutzerzugriff mit der Einstellung „force-group share“ optimieren . . . 26
ONTAP SMB-Freigaben mit der Einstellung „force-group share“ erstellen . . . 27
Informationen zu ONTAP SMB-Freigaben mit der MMC anzeigen . . . 27
ONTAP Befehle zur Verwaltung von SMB-Freigaben . . . 29
Sicherer Dateizugriff mithilfe von SMB-Freigabe-ACLs . . . 29
Informationen zur Verwaltung von ONTAP SMB-ACLs auf Freigabeebene . . . 29
Erstellen von ONTAP SMB-Freigabe-Zugriffssteuerungslisten . . . 30
ONTAP Befehle zur Verwaltung von SMB-Freigabezugriffskontrolllisten . . . 32

Dateizugriff mithilfe von Dateiberechtigungen absichern . . . 32
Erweiterte NTFS-Dateiberechtigungen mithilfe der Registerkarte „Windows-Sicherheit“ für ONTAP SMB SVMs konfigurieren . . . 32
ONTAP Befehle für SMB NTFS-Dateiberechtigungen . . . 35
UNIX-Dateiberechtigungen bieten Zugriffskontrolle beim Zugriff auf Dateien über ONTAP SMB-Server. 36
Sicherer Dateizugriff durch Dynamic Access Control (DAC) . . . 37
Informationen zur DAC-Dateizugriffsicherheit für ONTAP SMB-Server . . . 37
Unterstützte DAC-Funktionalität für ONTAP SMB Server . . . 38
Informationen zur Verwendung von DAC und zentralen Zugriffsrichtlinien mit ONTAP SMB-Servern . . . 39
DAC für ONTAP SMB-Server aktivieren oder deaktivieren . . . 40
Verwaltung von ACLs mit DAC-ACEs, wenn DAC auf ONTAP SMB-Servern deaktiviert ist . . . 41
Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf ONTAP SMB Servern zu schützen . . . 41
Informationen zur DAC-Sicherheit für ONTAP SMB-Server . . . 44
Überlegungen zum Zurücksetzen von DAC auf ONTAP SMB-Servern . . . 46
SMB-Zugriff mithilfe von Exportrichtlinien absichern . . . 47
Informationen zur Verwendung von Exportrichtlinien mit ONTAP SMB-Zugriff . . . 47
Informationen zu ONTAP SMB Exportregeln . . . 48
Beispiele für ONTAP Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen . . . 49
ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren . . . 51
Die SMB-Exportregel des ONTAP SVM-Root-Volumes öffnen . . . 52
Sicherer Dateizugriff mit Storage Level Access Guard . . . 53
Informationen zum sicheren ONTAP SMB Dateizugriff mit Storage-Level Access Guard . . . 53
Anwendungsfälle für den Einsatz von Storage-Level Access Guard . . . 55
Konfigurationsworkflow für Storage-Level Access Guard auf ONTAP SMB Servern . . . 55
Storage-Level Access Guard auf ONTAP SMB-Servern konfigurieren . . . 57
Effektive SLAG-Matrix auf ONTAP SMB Servern . . . 62
Informationen zu Storage-Level Access Guard auf ONTAP SMB-Servern . . . 63
Storage-Level Access Guard auf ONTAP SMB-Servern entfernen . . . 65

Dateizugriff mit SMB einrichten

Sicherheitsstile konfigurieren

Informationen zu ONTAP SMB-Sicherheitsstilen und deren Auswirkungen

Es gibt vier verschiedene Sicherheitsstile: UNIX, NTFS, gemischt und einheitlich. Jeder Sicherheitsstil wirkt sich unterschiedlich darauf aus, wie Berechtigungen für Daten gehandhabt werden. Das Verständnis der unterschiedlichen Auswirkungen ist erforderlich, um den passenden Sicherheitsstil für die jeweiligen Zwecke auszuwählen.

Es ist wichtig zu verstehen, dass Sicherheitsstile nicht festlegen, welche Clienttypen auf Daten zugreifen dürfen oder nicht. Sicherheitsstile bestimmen lediglich die Art der Berechtigungen, die ONTAP zur Steuerung des Datenzugriffs verwendet, und welcher Clienttyp diese Berechtigungen ändern darf.

Wenn beispielsweise ein Volume den UNIX-Sicherheitsstil verwendet, können SMB-Clients weiterhin auf Daten zugreifen (sofern sie ordnungsgemäß authentifizieren und autorisieren), da ONTAP multiprotokollfähig ist. ONTAP verwendet jedoch UNIX-Berechtigungen, die nur UNIX-Clients mit nativen Tools ändern können.

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Resultierender effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
Unix	NFS	• NFSv3 Modusbits • NFSv4.x-ACLs	Unix	NFS und SMB
NTFS	SMB	NTFS-ACLs	NTFS	NFS und SMB
Gemischt	NFS oder SMB	• NFSv3 Modusbits • NFSv4.x-ACLs • NTFS-ACLs	• UNIX (für NFSv3-Modusbits und NFSv4.x-ACLs) • NTFS (für NTFS-ACLs)	NFS und SMB
Unified (Nur für unbegrenzte Volumes, in ONTAP 9.4 und früheren Versionen.)	NFS oder SMB	• NFSv3 Modusbits • NFSv4.1-ACLs • NTFS-ACLs	• UNIX (für NFSv3-Modusbits und NFSv4.1-ACLs) • NTFS (für NTFS-ACLs)	NFS und SMB

FlexVol Volumes unterstützen UNIX, NTFS und gemischte Sicherheitsstile. Wenn der Sicherheitsstil gemischt oder einheitlich ist, hängen die effektiven Berechtigungen vom Clienttyp ab, der die Berechtigungen zuletzt geändert hat, da Benutzer den Sicherheitsstil individuell festlegen. Wenn der letzte Client, der die Berechtigungen geändert hat, ein NFSv3-Client war, sind die Berechtigungen UNIX NFSv3-Modusbits. Wenn der letzte Client ein NFSv4-Client war, sind die Berechtigungen NFSv4-ACLs. Wenn der letzte Client ein SMB-Client war, sind die Berechtigungen Windows NTFS-ACLs.

Der einheitliche Sicherheitsstil ist nur mit unbegrenzten Volumes verfügbar, die in ONTAP 9.5 und späteren Versionen nicht mehr unterstützt werden. Weitere Informationen finden sich unter FlexGroup

Volumenmanagement-Übersicht.

Der `show-effective-permissions` Parameter mit dem `vserver security file-directory` Befehl ermöglicht die Anzeige der effektiven Berechtigungen, die einem Windows- oder UNIX-Benutzer für den angegebenen Datei- oder Ordnerpfad gewährt wurden. Zusätzlich ermöglicht der optionale Parameter `-share-name` die Anzeige der effektiven Freigabeberechtigung. Weitere Informationen zu `vserver security file-directory show-effective-permissions` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP legt zunächst einige Standard-Dateiberechtigungen fest. Standardmäßig ist der effektive Sicherheitsstil für alle Daten in UNIX-, gemischten und einheitlichen Security-Style-Volumes UNIX, und der effektive Berechtigungstyp ist UNIX-Modusbits (0755, sofern nicht anders angegeben), bis ein Client die Berechtigungen gemäß dem Standard-Sicherheitsstil konfiguriert. Standardmäßig ist der effektive Sicherheitsstil für alle Daten in NTFS-Security-Style-Volumes NTFS, und es besteht eine ACL, die allen Benutzern vollständige Kontrolle erlaubt.

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Sicherheitsstile können auf FlexVol-Volumes (sowohl Root- als auch Datenvolumes) und qtrees festgelegt werden. Sicherheitsstile können manuell bei der Erstellung festgelegt, automatisch übernommen oder zu einem späteren Zeitpunkt geändert werden. == Entscheiden Sie, welche SMB-Sicherheitsstile auf ONTAP SVMs verwendet werden sollen

Zur Unterstützung bei der Entscheidung, welchen Sicherheitsstil Sie für ein Volume verwenden, sind zwei Faktoren zu berücksichtigen. Der wichtigste Faktor ist die Art des Administrators, der das Dateisystem verwaltet. Der zweite Faktor ist die Art des Benutzers oder Dienstes, der auf die Daten auf dem Volume zugreift.

Bei der Konfiguration des Sicherheitsstils eines Volumes sollten die Anforderungen Ihrer Umgebung berücksichtigt werden, um den optimalen Sicherheitsstil auszuwählen und Probleme bei der Berechtigungsverwaltung zu vermeiden. Die folgenden Überlegungen können bei der Entscheidung helfen:

Sicherheitsstil	Wählen Sie aus, ob…
UNIX	• Das Dateisystem wird von einem UNIX-Administrator verwaltet. • Die Mehrheit der Nutzer sind NFS-Clients. • Eine Anwendung, die auf die Daten zugreift, verwendet einen UNIX-Benutzer als Dienstkonto.
NTFS	• Das Dateisystem wird von einem Windows-Administrator verwaltet. • Die Mehrheit der Nutzer sind SMB-Clients. • Eine Anwendung, die auf die Daten zugreift, verwendet einen Windows-Benutzer als Dienstkonto.
Gemischt	Das Dateisystem wird sowohl von UNIX- als auch von Windows-Administratoren verwaltet, und die Benutzer bestehen sowohl aus NFS- als auch aus SMB-Clients.

Informationen zur Vererbung des Sicherheitsstils bei ONTAP SMB

Wenn Sie beim Erstellen eines neuen FlexVol volume oder eines qtree keinen Sicherheitsstil angeben, wird der Sicherheitsstil auf unterschiedliche Weise übernommen.

Sicherheitsstile werden folgendermaßen vererbt:

- Ein FlexVol volume übernimmt den Sicherheitsstil des Root-Volumes der SVM, in der es enthalten ist.
- Ein Qtree erbt den Sicherheitsstil des ihn enthaltenden FlexVol volume.
- Eine Datei oder ein Verzeichnis erbt den Sicherheitsstil des übergeordneten FlexVol volume oder qtree.

SMB-Sicherheitsstile auf ONTAP SVM Root-Volumes konfigurieren

Der Sicherheitsstil des Root-Volumes der Storage Virtual Machine (SVM) wird konfiguriert, um die Art der Berechtigungen für Daten auf dem Root-Volume der SVM festzulegen.

Schritte

1. Der `vserver create`Befehl mit dem `-rootvolume-security-style`Parameter dient zur Definition des Sicherheitsstils.

   Die möglichen Optionen für den Sicherheitsstil des Root-Volumes sind `unix`, `ntfs` oder `mixed`.

2. Anzeige und Überprüfung der Konfiguration, einschließlich des Sicherheitsstils des Root-Volumes der erstellten SVM: `vserver show -vserver` *`vserver_name`*

SMB-Sicherheitsstile auf ONTAP FlexVol Volumes konfigurieren

Der Sicherheitsstil des FlexVol volume wird konfiguriert, um die Art der Berechtigungen festzulegen, die für Daten auf FlexVol volumes der Storage Virtual Machine (SVM) verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn das FlexVol Volume…	Verwenden Sie den Befehl…
Existiert noch nicht	`volume create` und den `-security-style` Parameter zur Angabe des Sicherheitsstils einschließen.
Existiert bereits	`volume modify` und den `-security-style` Parameter zur Angabe des Sicherheitsstils einschließen.

   Die möglichen Optionen für den FlexVol volume-Sicherheitsstil sind `unix`, `ntfs`, oder `mixed`.

   Wenn beim Erstellen eines FlexVol volume kein Sicherheitsstil angegeben wird, übernimmt das Volume den Sicherheitsstil des Stammvolumes.

   Weitere Informationen zu den `volume create` oder `volume modify` Befehlen finden sich unter "Logische Speicherverwaltung".

2. Um die Konfiguration einschließlich des Sicherheitsstils des von Ihnen erstellten FlexVol Volumes anzuzeigen, ist folgender Befehl einzugeben:

```
volume show -volume volume_name -instance
```

SMB-Sicherheitsstile auf ONTAP Qtrees konfigurieren

Der Sicherheitsstil des Qtree-Volumes wird konfiguriert, um die Art der Berechtigungen festzulegen, die für Daten auf Qtrees verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn der Qtree…	Verwenden Sie den Befehl…
Existiert noch nicht	`volume qtree create` und den `-security -style` Parameter zur Angabe des Sicherheitsstils einschließen.
Existiert bereits	`volume qtree modify` und den `-security -style` Parameter zur Angabe des Sicherheitsstils einschließen.

   Die möglichen Optionen für den Qtree-Sicherheitsstil sind `unix`, `ntfs` oder `mixed`.

   Wenn beim Erstellen eines Qtree kein Sicherheitsstil angegeben wird, ist der Standard-Sicherheitsstil `mixed`.

   Weitere Informationen zu den `volume qtree create` oder `volume qtree modify` Befehlen finden sich unter "Logische Speicherverwaltung".

2. Um die Konfiguration, einschließlich des Sicherheitsstils des von Ihnen erstellten Qtrees, anzuzeigen, ist folgender Befehl einzugeben: `volume qtree show -qtree qtree_name -instance`

Daten-Volumes in NAS-Namespaces erstellen und verwalten

Informationen zum Erstellen und Verwalten von ONTAP SMB-Datenvolumes in NAS-Namespaces

Um den Dateizugriff in einer NAS-Umgebung zu verwalten, müssen Sie Datenvolumes und Verbindungspunkte auf Ihrer Storage Virtual Machine (SVM) verwalten. Dies umfasst die Planung Ihrer Namespace-Architektur, das Erstellen von Volumes mit oder ohne Verbindungspunkte, das Einbinden oder Aushängen von Volumes sowie das Anzeigen von Informationen über Datenvolumes und NFS-Server- oder CIFS-Server-Namespaces.

ONTAP SMB-Datenvolumes mit angegebenen Verbindungspunkten erstellen

Beim Erstellen eines Datenvolumes kann der Verbindungspunkt festgelegt werden. Das resultierende Volume wird automatisch am Verbindungspunkt eingebunden und steht sofort zur Konfiguration für den NAS-Zugriff bereit.

Bevor Sie beginnen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits existieren.

Folgende Zeichen dürfen im Verbindungspfad nicht verwendet werden: * # " > < | ? \

Darüber hinaus darf die Verbindungspfadlänge nicht mehr als 255 Zeichen betragen.

Schritte

1. Das Volume mit einer Verbindung erstellen: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

   Der Verbindungspfad muss mit dem Stammverzeichnis (/) beginnen und kann sowohl Verzeichnisse als auch verknüpfte Volumes enthalten. Der Verbindungspfad muss nicht den Namen des Volumes enthalten. Verbindungspfade sind unabhängig vom Volume-Namen.

   Die Angabe eines Sicherheitsstils für das Volume ist optional. Wenn kein Sicherheitsstil angegeben wird, erstellt ONTAP das Volume mit demselben Sicherheitsstil, der auf das Root-Volume der Storage Virtual Machine (SVM) angewendet wird. Der Sicherheitsstil des Root-Volumes entspricht jedoch möglicherweise nicht dem Sicherheitsstil, der für das zu erstellende Datenvolume gewünscht ist. Es empfiehlt sich, den Sicherheitsstil beim Erstellen des Volumes anzugeben, um schwer zu behebende Probleme beim Dateizugriff zu minimieren.

   Der Verbindungspfad ist nicht Groß-/Kleinschreibung-abhängig; `/ENG` ist identisch mit `/eng`. Wird eine CIFS-Freigabe erstellt, behandelt Windows den Verbindungspfad so, als ob er Groß-/Kleinschreibung-abhängig ist. Beispielsweise muss, wenn die Verbindung `/ENG` ist, der Pfad einer CIFS-Freigabe mit `/ENG` beginnen und nicht mit `/eng`.

   Es gibt zahlreiche optionale Parameter, mit denen Sie ein Datenvolumen anpassen können. Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

2. Überprüfen, ob das Volume mit dem gewünschten Verbindungspunkt erstellt wurde: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Beispiel

Das folgende Beispiel erstellt ein Volume namens “home4” auf SVM vs1, das einen Verbindungspfad hat `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

ONTAP SMB-Datenvolumes ohne Angabe von Verbindungspunkten erstellen

Sie können ein Datenvolume erstellen, ohne einen Verbindungspunkt anzugeben. Das resultierende Volume wird nicht automatisch eingebunden und steht nicht zur

Konfiguration für NAS-Zugriff zur Verfügung. Das Volume muss eingebunden werden, bevor SMB-Freigaben oder NFS-Exporte für dieses Volume konfiguriert werden können.

Bevor Sie beginnen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits existieren.

Schritte

1. Das Volume ohne Verbindungspunkt kann mit folgendem Befehl erstellt werden: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   Die Angabe eines Sicherheitsstils für das Volume ist optional. Wenn kein Sicherheitsstil angegeben wird, erstellt ONTAP das Volume mit demselben Sicherheitsstil, der auf das Root-Volume der Storage Virtual Machine (SVM) angewendet wird. Der Sicherheitsstil des Root-Volumes entspricht jedoch möglicherweise nicht dem gewünschten Sicherheitsstil für das Datenvolume. Es empfiehlt sich, den Sicherheitsstil beim Erstellen des Volumes anzugeben, um schwer zu behebende Probleme beim Dateizugriff zu minimieren.

   Es gibt zahlreiche optionale Parameter, mit denen Sie ein Datenvolumen anpassen können. Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

2. Es wird überprüft, ob das Volume ohne Verbindungspunkt erstellt wurde: `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

Das folgende Beispiel erstellt ein Volume mit dem Namen “sales”, das sich auf SVM vs1 befindet und nicht an einem Verbindungspunkt eingebunden ist:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Vorhandene ONTAP SMB-Volumes im NAS-Namespace einbinden oder aushängen

Ein Volume muss im NAS-Namespace eingebunden sein, bevor Sie den NAS-Client-Zugriff auf die in den Storage Virtual Machine (SVM)-Volumes enthaltenen Daten konfigurieren können. Ein Volume kann an einem Verbindungspunkt eingebunden werden, wenn es derzeit nicht eingebunden ist. Volumes können auch ausgehängt werden.

Über diese Aufgabe

Wenn ein Volume ausgehängt und offline genommen wird, sind alle Daten innerhalb der Verbindung, einschließlich der Daten in Volumes mit Verbindungen innerhalb des Namespace des ausgehängten Volumes, für NAS-Clients nicht zugänglich.

> Um den Dateizugriff eines NAS-Clients auf ein Volume zu beenden, reicht es nicht aus, das Volume einfach auszuhängen. Das Volume muss offline genommen werden oder es sind andere Maßnahmen erforderlich, um sicherzustellen, dass Client-seitig Dateihandle-Caches ungültig werden. Weitere Informationen enthält der folgende Knowledge Base Artikel: "NFSv3-Clients haben weiterhin Zugriff auf ein Volume, nachdem sie aus dem Namespace in ONTAP entfernt wurden"

Wenn ein Volume ausgehängt und offline genommen wird, gehen die darin enthaltenen Daten nicht verloren. Zudem bleiben bestehende Volume-Exportrichtlinien und SMB-Shares, die auf dem Volume oder in Verzeichnissen und Verbindungspunkten innerhalb des ausgehängten Volumes erstellt wurden, erhalten. Wird das ausgehängte Volume wieder eingebunden, können NAS-Clients mit den bestehenden Exportrichtlinien und SMB-Shares auf die darin enthaltenen Daten zugreifen.

Schritte

1. Die gewünschte Aktion ausführen:

Wenn Sie möchten…	Die Befehle werden eingegeben…
Ein Volume einbinden	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Aushängen eines Volumes	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Es sollte sichergestellt werden, dass sich das Volume im gewünschten Mount-Status befindet:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Beispiele

Das folgende Beispiel bindet ein Volume namens “sales”, das sich auf SVM “vs1” befindet, an den Verbindungspunkt “/sales” ein:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
```

```
vs1       sales      online    /sales          true
```

Das folgende Beispiel hängt ein Volume namens “data” auf SVM “vs1” aus und nimmt es offline:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Informationen zu ONTAP SMB-Volume-Mounts und Verbindungspunkten anzeigen

Sie können Informationen zu eingebundenen Volumes für Storage Virtual Machines (SVMs) und den Verbindungspunkten, an die die Volumes eingebunden sind, anzeigen. Es lässt sich auch feststellen, welche Volumes nicht an einen Verbindungspunkt eingebunden sind. Diese Informationen ermöglichen ein besseres Verständnis und eine effektivere Verwaltung Ihres SVM-Namespaces.

Schritte

1. Die gewünschte Aktion ausführen:

Wenn Sie anzeigen möchten…	Geben Sie den Befehl ein…
Zusammenfassende Informationen zu eingebundenen und nicht eingebundenen Volumes auf dem SVM	`volume show -vserver vserver_name -junction`
Detaillierte Informationen zu eingebundenen und nicht eingebundenen Volumes auf dem SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Spezifische Informationen zu eingebundenen und nicht eingebundenen Volumes auf dem SVM	a. Bei Bedarf lassen sich die gültigen Felder für den `-fields` Parameter mit folgendem Befehl anzeigen: `volume show -fields ?` b. Die gewünschten Informationen werden mit dem `-fields` Parameter angezeigt: volume show -vserver vserver_name -fields fieldname,…

Beispiele

Das folgende Beispiel zeigt eine Zusammenfassung der eingebundenen und nicht eingebundenen Volumes auf SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

Das folgende Beispiel zeigt Informationen zu bestimmten Feldern für Volumes auf SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Namenszuordnungen konfigurieren

Informationen zur Konfiguration der ONTAP SMB-Namenszuordnungen

ONTAP verwendet Namenszuordnung, um CIFS-Identitäten UNIX-Identitäten, Kerberos-Identitäten UNIX-Identitäten und UNIX-Identitäten CIFS-Identitäten zuzuordnen. Diese Informationen werden benötigt, um Benutzeranmeldeinformationen zu erhalten und den korrekten Dateizugriff bereitzustellen, unabhängig davon, ob die Verbindung von einem

NFS-Client oder einem CIFS-Client erfolgt.

Es gibt zwei Ausnahmen, bei denen Sie keine Namenszuordnung verwenden müssen:

- Sie konfigurieren eine reine UNIX-Umgebung und planen nicht, CIFS-Zugriff oder den NTFS-Sicherheitsstil auf Volumes zu verwenden.
- Stattdessen wird der Standardbenutzer konfiguriert.

  In diesem Szenario ist keine Namenszuordnung erforderlich, da statt der Zuordnung jeder einzelnen Client-Anmeldeinformation alle Client-Anmeldeinformationen demselben Standardbenutzer zugeordnet werden.

Beachten Sie, dass die Namenszuordnung nur für Benutzer und nicht für Gruppen verwendet werden kann.

Sie können jedoch eine Gruppe einzelner Benutzer einem bestimmten Benutzer zuordnen. Beispielsweise können alle AD-Benutzer, deren Name mit dem Wort SALES beginnt oder endet, einem bestimmten UNIX-Benutzer und der Benutzer-UID dieses Benutzers zugeordnet werden.

Informationen zur ONTAP SMB Namenszuordnung

Wenn ONTAP Anmeldeinformationen für einen Benutzer zuordnen muss, prüft es zunächst die lokale Name-Mapping-Datenbank und den LDAP-Server auf eine vorhandene Zuordnung. Ob einer oder beide geprüft werden und in welcher Reihenfolge, wird durch die Namensdienstkonfiguration der SVM bestimmt.

- Zuordnung von Windows zu UNIX

  Wird keine Zuordnung gefunden, prüft ONTAP, ob der in Kleinbuchstaben geschriebene Windows-Benutzername ein gültiger Benutzername in der UNIX-Domäne ist. Falls dies nicht funktioniert, wird der standardmäßige UNIX-Benutzer verwendet, sofern dieser konfiguriert ist. Ist der Standard-UNIX-Benutzer nicht konfiguriert und ONTAP kann auch auf diesem Weg keine Zuordnung herstellen, schlägt die Zuordnung fehl und ein Fehler wird zurückgegeben.

- Für die UNIX-zu-Windows-Zuordnung

  Wird keine Zuordnung gefunden, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der Standard-SMB-Benutzer verwendet, sofern dieser konfiguriert ist. Ist der Standard-CIFS-Benutzer nicht konfiguriert und ONTAP kann auch auf diesem Weg keine Zuordnung herstellen, schlägt die Zuordnung fehl und ein Fehler wird zurückgegeben.

Maschinenkonten werden standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung der Maschinenkonten fehl.

- Ab ONTAP 9.5 ist es möglich, Maschinenkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuzuordnen.
- In ONTAP 9.4 und früher ist es nicht möglich, Maschinenkonten anderen Benutzern zuzuordnen.

  Selbst wenn Namenszuordnungen für Maschinenkonten definiert sind, werden die Zuordnungen ignoriert.

Informationen zu ONTAP SMB Multidomain-Suchen für die Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen

ONTAP unterstützt die Suche in mehreren Domänen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle ermittelten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersetzungsmuster durchsucht, bis ein passendes Ergebnis gefunden wird. Alternativ ist es möglich, eine Liste bevorzugter vertrauenswürdiger Domänen zu konfigurieren, die anstelle der ermittelten vertrauenswürdigen Domänenliste verwendet und der Reihe nach durchsucht wird, bis ein passendes Ergebnis gefunden wird.

Wie Domänenvertrauensstellungen die Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen beeinflussen

Um die Funktionsweise der domänenübergreifenden Benutzernamenszuordnung zu verstehen, ist es erforderlich, die Funktionsweise von Domänenvertrauensstellungen in Verbindung mit ONTAP zu verstehen. Active Directory-Vertrauensstellungen mit der Home-Domäne des CIFS-Servers können entweder eine bidirektionale Vertrauensstellung oder eine von zwei Arten unidirektionaler Vertrauensstellungen sein, entweder eine eingehende oder eine ausgehende Vertrauensstellung. Die Home-Domäne ist die Domäne, zu der der CIFS-Server auf der SVM gehört.

- *Bidirektionales Vertrauen*

  Bei bidirektionalen Vertrauensstellungen vertrauen sich beide Domänen. Wenn die Heimatdomäne des CIFS-Servers eine bidirektionale Vertrauensstellung mit einer anderen Domäne hat, kann die Heimatdomäne einen Benutzer der vertrauenswürdigen Domäne authentifizieren und autorisieren und umgekehrt.

  Die Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen kann nur in Domänen mit bidirektionalen Vertrauensstellungen zwischen der Heimatdomäne und der anderen Domäne durchgeführt werden.

- *Ausgehendes Vertrauen*

  Bei einer ausgehenden Vertrauensstellung vertraut die Heimatdomäne der anderen Domäne. In diesem Fall kann die Heimatdomäne einen Benutzer der ausgehend vertrauenswürdigen Domäne authentifizieren und autorisieren.

  Bei der Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen wird eine Domäne mit einer ausgehenden Vertrauensstellung zur Home-Domäne *nicht* durchsucht.

- *Eingehendes Vertrauen*

  Bei einer eingehenden Vertrauensstellung vertraut die andere Domäne der Heimatdomäne des CIFS-Servers. In diesem Fall kann die Heimatdomäne einen Benutzer der eingehenden vertrauenswürdigen Domäne weder authentifizieren noch autorisieren.

  Bei der Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen wird eine Domäne mit einer eingehenden Vertrauensstellung zur Heimatdomäne *nicht* durchsucht.

Wie Platzhalter (*) zur Konfiguration von multidomain Suchen für die Namenszuordnung verwendet werden

Die Suche nach domänenübergreifenden Namenszuordnungen wird durch die Verwendung von Platzhaltern im Domänenteil des Windows-Benutzernamens erleichtert. Die folgende Tabelle veranschaulicht, wie Platzhalter im Domänenteil eines Namenszuordnungseintrags verwendet werden können, um domänenübergreifende Suchen zu ermöglichen:

Muster	Ersatz	Ergebnis
root	*\\Administrator	Der UNIX-Benutzer “root” ist dem Benutzer “administrator” zugeordnet. Alle vertrauenswürdigen Domänen werden der Reihe nach durchsucht, bis der erste passende Benutzer mit dem Namen “administrator” gefunden wird.
*	**	Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden der Reihe nach durchsucht, bis der erste passende Benutzer mit diesem Namen gefunden wird. Das Muster ** ist nur für die Namenszuordnung von UNIX nach Windows gültig, nicht umgekehrt.

Wie Suchvorgänge nach Namen mit mehreren Domänen durchgeführt werden

Es stehen zwei Methoden zur Verfügung, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für multidomain Name Searches verwendet wird:

- Die von ONTAP automatisch erstellte Liste der bidirektionalen Vertrauensstellungen kann verwendet werden
- Die bevorzugte Liste vertrauenswürdiger Domänen verwenden, die Sie zusammengestellt haben

Wenn ein UNIX-Benutzer einem Windows-Benutzer zugeordnet wird, wobei für den Domänenteil des Benutzernamens ein Platzhalter verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt gesucht:

- Wenn eine bevorzugte Liste vertrauenswürdiger Domänen konfiguriert ist, wird der zugeordnete Windows-Benutzer nur in dieser Suchliste in der angegebenen Reihenfolge gesucht.
- Wenn keine bevorzugte Liste vertrauenswürdiger Domänen konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Heimatdomäne gesucht.
- Wenn für die Heimatdomäne keine bidirektional vertrauenswürdigen Domänen vorhanden sind, wird der Benutzer in der Heimatdomäne gesucht.

Ab ONTAP 9.13.1 führt ONTAP bei der Suche nach vertrauenswürdigen Domänen während Namenszuordnungsvorgängen für mehrere Domänen eine Standortermittlung für diese vertrauenswürdigen Domänen durch und verwendet den ermittelten Standort für Domänencontroller-Abfragen. Dadurch wird sichergestellt, dass DNS-SRV-Abfragen die korrekten Standortinformationen für Domänencontroller vertrauenswürdiger Domänen verwenden. Wenn die Standortermittlung für vertrauenswürdige Domänen fehlschlägt, verwendet ONTAP den Standardstandort des SMB-Servers.

Wenn ein UNIX-Benutzer einem Windows-Benutzer zugeordnet ist, dessen Benutzername keinen Domänenteil enthält, wird der Windows-Benutzer in der Heimatdomäne gesucht.

Informationen zu den Konvertierungsregeln für die ONTAP SMB-Namenszuordnung

Ein ONTAP-System verwaltet für jede SVM einen Satz von Konvertierungsregeln. Jede Regel besteht aus zwei Teilen: einem Muster und einer Ersetzung. Die Konvertierung beginnt am Anfang der entsprechenden Liste und führt eine Ersetzung basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein regulärer Ausdruck im UNIX-Stil. Die Ersetzung ist eine Zeichenkette mit Escape-Sequenzen, die Teilausdrücke des Musters darstellen, analog zum UNIX `sed` Programm.

ONTAP SMB-Namenszuordnung erstellen

Sie können den `vserver name-mapping create` Befehl verwenden, um eine Namenszuordnung zu erstellen. Namenszuordnungen werden verwendet, damit Windows-Benutzer auf UNIX Security Style Volumes zugreifen können und umgekehrt.

Über diese Aufgabe

ONTAP unterstützt für jede SVM bis zu 12.500 Namenszuordnungen pro Richtung.

Schritt

1. Namenszuordnung erstellen: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > Die `-pattern` und `-replacement`-Anweisungen können als reguläre Ausdrücke formuliert werden. Die `-replacement`-Anweisung kann auch verwendet werden, um dem Benutzer eine Zuordnung explizit zu verweigern, indem die Null-Ersetzungszeichenkette `" "` (das Leerzeichen) verwendet wird. Weitere Informationen zu `vserver name-mapping create` finden sich in der "ONTAP-Befehlsreferenz".

   Wenn Windows-zu-UNIX-Zuordnungen erstellt werden, müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, ausloggen und sich erneut anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Der folgende Befehl erstellt eine Namenszuordnung auf der SVM mit dem Namen vs1. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätsliste. Die Zuordnung ordnet den UNIX-Benutzer johnd dem Windows-Benutzer ENG\JohnDoe zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

Der folgende Befehl erstellt eine weitere Namenszuordnung auf der SVM mit dem Namen vs1. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätsliste. Hier beinhalten Muster und Ersetzung reguläre Ausdrücke. Die Zuordnung ordnet jeden CIFS-Benutzer in der Domäne ENG Benutzern in der mit der SVM verknüpften LDAP-Domäne zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

Der folgende Befehl erstellt eine weitere Namenszuordnung auf der SVM mit dem Namen vs1. Das Muster enthält hierbei das Zeichen “$” im Windows-Benutzernamen, das maskiert werden muss. Die Zuordnung ordnet den Windows-Benutzer ENG\john$ops dem UNIX-Benutzer john_ops zu.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Den standardmäßigen ONTAP SMB-Benutzer konfigurieren

Sie können einen Standardbenutzer konfigurieren, der verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie keine einzelnen Benutzer zwischen UNIX und Windows zuordnen möchten. Alternativ sollte kein Standardbenutzer konfiguriert werden, wenn die Authentifizierung nicht zugeordneter Benutzer fehlschlagen soll.

Über diese Aufgabe

Für die CIFS Authentifizierung kann anstelle der Zuordnung jedes Windows-Benutzers zu einem einzelnen UNIX-Benutzer ein Standard-UNIX-Benutzer angegeben werden.

Für die NFS Authentifizierung kann anstelle der Zuordnung jedes UNIX-Benutzers zu einem einzelnen Windows-Benutzer ein Standard-Windows-Benutzer angegeben werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Den Standard-UNIX-Benutzer konfigurieren	`vserver cifs options modify -default -unix-user` *`user_name`*
Den Standard-Windows-Benutzer konfigurieren	`vserver nfs modify -default-win-user` *`user_name`*

ONTAP Befehle zur Verwaltung von SMB-Namenszuordnungen

Für die Verwaltung von Namenszuordnungen gibt es spezielle ONTAP Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine Namenszuordnung erstellen	`vserver name-mapping create`
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Anzeigenamenzuordnungen anzeigen	`vserver name-mapping show`
Die Position zweier Namenszuordnungen wird getauscht. HINWEIS: Ein Tausch ist nicht zulässig, wenn die Namenszuordnung mit einem ip-qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Eine Namenszuordnung ändern	`vserver name-mapping modify`
Eine Namenszuordnung löschen	`vserver name-mapping delete`
Die korrekte Namenszuordnung validieren	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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

Konfiguration von Namenszuordnungssuchen über mehrere Domänen hinweg

Aktivieren oder Deaktivieren von ONTAP SMB Multidomain-Namenszuordnungssuchen

Bei der Suche nach domänenübergreifenden Namenszuordnungen kann im Domänenteil eines Windows-Namens beim Konfigurieren der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen ein Platzhalterzeichen (**) verwendet werden. Durch die Verwendung eines Platzhalterzeichens (**) im Domänenteil des Namens kann ONTAP alle Domänen durchsuchen, die eine bidirektionale Vertrauensstellung mit der Domäne haben, die das Computerkonto des CIFS-Servers enthält.

Über diese Aufgabe

Als Alternative zur Suche in allen bidirektional vertrauenswürdigen Domänen kann eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert werden. Wenn eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert ist, verwendet ONTAP diese Liste anstelle der ermittelten bidirektional vertrauenswürdigen Domänen, um multidomain Namenszuordnungs-Suchen durchzuführen.

- Die Suche nach domänenübergreifenden Namenszuordnungen ist standardmäßig aktiviert.
- Diese Option ist auf der Stufe „Erweitertes Berechtigungsniveau“ verfügbar.

Schritte

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

Wenn Sie möchten, dass die Suche nach Multidomain-Namenszuordnungen durchgeführt wird…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled false`

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

Verwandte Informationen

Verfügbare Serveroptionen

Vertrauenswürdige ONTAP SMB-Domänen zurücksetzen und neu erkennen

Sie können die erneute Erkennung aller vertrauenswürdigen Domänen erzwingen. Dies kann nützlich sein, wenn die Server der vertrauenswürdigen Domänen nicht angemessen reagieren oder sich die Vertrauensstellungen geändert haben. Es werden nur Domänen erkannt, die über eine bidirektionale Vertrauensstellung zur Heimatdomäne verfügen, also der Domäne, die das Computerkonto des CIFS-Servers enthält.

Ab ONTAP 9.13.1 führt ONTAP bei der erneuten Erkennung vertrauenswürdiger Domänen auch eine Standortermittlung für diese vertrauenswürdigen Domänen durch. ONTAP verwendet die ermittelten Standortinformationen für Domänencontroller-Abfragen vertrauenswürdiger Domänen. Dies trägt dazu bei, dass DNS-SRV-Abfragen die korrekten Standortinformationen für Domänencontroller vertrauenswürdiger Domänen verwenden. Wenn die Standortermittlung für eine vertrauenswürdige Domäne fehlschlägt, verwendet ONTAP den Standardstandort des SMB-Servers.

Schritt

1. Vertrauenswürdige Domänen werden mithilfe des `vserver cifs domain trusts rediscover` Befehls zurückgesetzt und neu erkannt.

   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

Verwandte Informationen

Informationen zu erkannten vertrauenswürdigen Domänen anzeigen

Informationen zu erkannten vertrauenswürdigen ONTAP SMB-Domänen

Sie können Informationen zu den ermittelten vertrauenswürdigen Domänen für die Heimatdomäne des CIFS-Servers anzeigen, also die Domäne, die das Computerkonto des CIFS-Servers enthält. Dies kann hilfreich sein, wenn Sie wissen möchten, welche

vertrauenswürdigen Domänen ermittelt wurden und wie sie in der Liste der ermittelten vertrauenswürdigen Domänen angeordnet sind.

Über diese Aufgabe

Es werden nur Domänen mit bidirektionalen Vertrauensstellungen zur Heimatdomäne ermittelt. Da der Domänencontroller (DC) der Heimatdomäne die Liste der vertrauenswürdigen Domänen in einer vom DC festgelegten Reihenfolge zurückgibt, lässt sich die Reihenfolge der Domänen in der Liste nicht vorhersagen. Durch die Anzeige der Liste der vertrauenswürdigen Domänen lässt sich die Suchreihenfolge für Namenszuordnungen in mehreren Domänen ermitteln.

Ab ONTAP 9.13.1 führt ONTAP auch eine Standortermittlung für vertrauenswürdige Domänen durch und verwendet den ermittelten Standort, um Domänencontroller für diese Domänen zu finden. Dies trägt dazu bei, dass DNS-SRV-Abfragen die korrekten Standortinformationen für Domänencontroller vertrauenswürdiger Domänen verwenden. Wenn die Standortermittlung für eine vertrauenswürdige Domäne fehlschlägt, greift ONTAP auf den Standardstandort des SMB-Servers zurück.

Die angezeigten Informationen zur vertrauenswürdigen Domäne sind nach Knoten und Storage Virtual Machine (SVM) gruppiert.

Schritt

1. Informationen über erkannte vertrauenswürdige Domänen werden mit dem `vserver cifs domain trusts show` Befehl angezeigt.

   ```
   vserver cifs domain trusts show -vserver vs1
   ```

   ```
      Node: node1
   Vserver: vs1

   Home Domain             Trusted Domain
   ----------------------  ----------------------------------
   EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                           CIFS2.EXAMPLE.COM
                           EXAMPLE.COM

      Node: node2
   Vserver: vs1

   Home Domain             Trusted Domain
   ----------------------  ----------------------------------
   EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                           CIFS2.EXAMPLE.COM
                           EXAMPLE.COM
   ```

Verwandte Informationen

Vertrauenswürdige Domänen zurücksetzen und neu erkennen

Vertrauenswürdige ONTAP SMB-Domänen in bevorzugten Listen hinzufügen, entfernen oder ersetzen

Sie können vertrauenswürdige Domänen zur Liste der bevorzugten vertrauenswürdigen Domänen für den SMB-Server hinzufügen oder daraus entfernen oder die aktuelle Liste bearbeiten. Wenn eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert ist, wird diese Liste anstelle der ermittelten bidirektionalen vertrauenswürdigen Domänen bei multidomänenübergreifenden Namenszuordnungs-Suchen verwendet.

Über diese Aufgabe

- Wenn Sie einer bestehenden Liste vertrauenswürdige Domänen hinzufügen, wird die neue Liste mit der bestehenden Liste zusammengeführt, wobei die neuen Einträge am Ende eingefügt werden. Die vertrauenswürdigen Domänen werden in der Reihenfolge durchsucht, in der sie in der Liste der vertrauenswürdigen Domänen erscheinen.
- Wenn Sie vertrauenswürdige Domänen aus der bestehenden Liste entfernen und keine Liste angeben, wird die gesamte Liste der vertrauenswürdigen Domänen für die angegebene Storage Virtual Machine (SVM) entfernt.
- Wenn die bestehende Liste der vertrauenswürdigen Domänen geändert wird, überschreibt die neue Liste die bestehende Liste.

> Sie sollten in der Liste der bevorzugten vertrauenswürdigen Domänen nur bidirektional vertrauenswürdige Domänen eintragen. Obwohl Sie ausgehende oder eingehende Vertrauensstellungen in die bevorzugte Domänenliste eintragen können, werden diese bei der Durchführung von multidomain Namenszuordnungs-Suchen nicht verwendet. ONTAP überspringt den Eintrag für die unidirektionale Domäne und fährt mit der nächsten bidirektional vertrauenswürdigen Domäne in der Liste fort.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Folgendes mit der Liste der bevorzugten vertrauenswürdigen Domänen durchführen möchten…	Verwenden Sie den Befehl…
Vertrauenswürdige Domänen zur Liste hinzufügen	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Vertrauenswürdige Domänen aus der Liste entfernen	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Die bestehende Liste bearbeiten	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Beispiele

Der folgende Befehl fügt zwei vertrauenswürdige Domänen (cifs1.example.com und cifs2.example.com) zur Liste der bevorzugten vertrauenswürdigen Domänen hinzu, die von SVM vs1 verwendet wird:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
```

```
-trusted-domains cifs1.example.com, cifs2.example.com
```

Der folgende Befehl entfernt zwei vertrauenswürdige Domänen aus der von SVM vs1 verwendeten Liste:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Der folgende Befehl ändert die von SVM vs1 verwendete Liste vertrauenswürdiger Domänen. Die neue Liste ersetzt die ursprüngliche Liste:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Verwandte Informationen

Informationen zur Liste der bevorzugten vertrauenswürdigen Domänen

Informationen zur bevorzugten vertrauenswürdigen ONTAP SMB-Domänenliste anzeigen

Sie können Informationen darüber anzeigen, welche vertrauenswürdigen Domänen in der Liste der bevorzugten vertrauenswürdigen Domänen enthalten sind und in welcher Reihenfolge sie durchsucht werden, wenn multidomain Namenszuordnungs-Suchen aktiviert sind. Eine bevorzugte vertrauenswürdige Domänenliste kann als Alternative zur automatisch ermittelten Liste vertrauenswürdiger Domänen konfiguriert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen zu Folgendem angezeigt werden sollen…	Verwenden Sie den Befehl…
Alle bevorzugten vertrauenswürdigen Domänen im Cluster, gruppiert nach Storage Virtual Machine (SVM)	`vserver cifs domain name-mapping-search show`
Alle bevorzugten vertrauenswürdigen Domänen für eine bestimmte SVM	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

Der folgende Befehl zeigt Informationen zu allen bevorzugten vertrauenswürdigen Domänen im Cluster an:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ---------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Verwandte Informationen

SMB-Freigaben erstellen und konfigurieren

Informationen zum Erstellen und Konfigurieren von ONTAP SMB-Freigaben

Bevor Benutzer und Anwendungen über SMB auf Daten auf dem CIFS-Server zugreifen können, müssen SMB-Shares erstellt und konfiguriert werden, was einen benannten Zugriffspunkt in einem Volume darstellt. Shares können angepasst werden, indem Share-Parameter und Share-Eigenschaften angegeben werden. Eine vorhandene Share kann jederzeit geändert werden.

Wenn eine SMB-Freigabe erstellt wird, erstellt ONTAP standardmäßig eine ACL für die Freigabe mit Vollzugriffsberechtigungen für Everyone.

SMB-Freigaben sind an den CIFS-Server auf der Storage Virtual Machine (SVM) gebunden. SMB-Freigaben werden gelöscht, wenn entweder die SVM gelöscht wird oder der mit ihr verbundene CIFS-Server von der SVM gelöscht wird. Wird der CIFS-Server auf der SVM neu erstellt, müssen die SMB-Freigaben ebenfalls neu erstellt werden.

Verwandte Informationen

- Informationen zu lokalen Benutzern und Gruppen
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"
- Zeichenzuordnung für die Dateinamenübersetzung auf Volumes konfigurieren

Informationen zu den standardmäßigen administrativen ONTAP SMB-Freigaben

Wenn Sie einen CIFS-Server auf Ihrer Storage Virtual Machine (SVM) erstellen, werden automatisch standardmäßige administrative Freigaben angelegt. Es ist wichtig zu verstehen, was diese Standardfreigaben sind und wie sie verwendet werden.

ONTAP erstellt beim Erstellen des CIFS-Servers die folgenden standardmäßigen administrativen Freigaben:

> Ab ONTAP 9.8 wird die admin$ Freigabe nicht mehr standardmäßig erstellt.

- ipc$
- admin$ (nur ONTAP 9.7 und älter)
- c$

Da Freigaben, die mit dem $-Zeichen enden, versteckte Freigaben sind, sind die standardmäßigen administrativen Freigaben nicht über „Arbeitsplatz“ sichtbar, sie lassen sich jedoch über „Freigegebene Ordner“ anzeigen.

Wie die Standardfreigaben ipc$ und admin$ verwendet werden

Die Freigaben ipc$ und admin$ werden von ONTAP verwendet und können von Windows-Administratoren nicht genutzt werden, um auf Daten zuzugreifen, die sich auf der SVM befinden.

- ipc$ Freigabe

Die ipc$-Freigabe ist eine Ressource, die die für die Kommunikation zwischen Programmen unerlässlichen Named Pipes freigibt. Die ipc$-Freigabe wird während der Remote-Administration eines Computers und beim Anzeigen der freigegebenen Ressourcen eines Computers verwendet. Die Freigabeeinstellungen, Freigabeeigenschaften oder ACLs der ipc$-Freigabe können nicht geändert werden. Die ipc$-Freigabe kann auch nicht umbenannt oder gelöscht werden.

- admin$ Freigabe (nur ONTAP 9.7 und früher)

  Ab ONTAP 9.8 wird die admin$ Freigabe nicht mehr standardmäßig erstellt.

  Die administrative Freigabe admin$ wird während der Remote-Administration der SVM verwendet. Der Pfad dieser Ressource ist immer der Pfad zum SVM-Root. Die Freigabeeinstellungen, Freigabeeigenschaften oder ACLs für die administrative Freigabe admin$ können nicht geändert werden. Auch das Umbenennen oder Löschen der administrativen Freigabe admin$ ist nicht möglich.

Wie die Standardfreigabe c$ verwendet wird

Die c$ Freigabe ist eine administrative Freigabe, die der Cluster- oder SVM-Administrator verwenden kann, um auf das SVM Root-Volume zuzugreifen und es zu verwalten.

Die folgenden Merkmale kennzeichnen die c$ administrative Freigabe:

- Der Pfad für diese Freigabe ist immer der Pfad zum SVM-Root-Volume und kann nicht geändert werden.
- Die Standard-ACL für die c$ Freigabe ist Administrator / Vollzugriff.

  Dieser Benutzer ist der BUILTIN\administrator. Standardmäßig kann der BUILTIN\administrator auf die Freigabe zugreifen und Dateien und Ordner im zugeordneten Stammverzeichnis anzeigen, erstellen, ändern oder löschen. Beim Verwalten von Dateien und Ordnern in diesem Verzeichnis ist Vorsicht geboten.

- Sie können die ACL der c$ Freigabe ändern.
- Sie können die Einstellungen und Eigenschaften der C$-Freigabe ändern.
- Sie können die c$ Freigabe nicht löschen.
- Der SVM-Administrator kann vom zugeordneten c$ Share aus über die Namensraumübergänge auf den Rest des SVM-Namensraums zugreifen.
- Auf die c$ Freigabe kann über die Microsoft Management Console zugegriffen werden.

Verwandte Informationen

Erweiterte Dateiberechtigungen mithilfe der Registerkarte Windows-Sicherheit konfigurieren

Informationen zu den Anforderungen an die Benennung von ONTAP SMB-Freigaben

Die ONTAP Anforderungen an die Benennung von Freigaben sind bei der Erstellung von SMB-Freigaben auf dem SMB-Server zu berücksichtigen.

Die Namenskonventionen für Freigaben unter ONTAP sind die gleichen wie unter Windows und umfassen die folgenden Anforderungen:

- Der Name jeder Freigabe muss für den SMB-Server eindeutig sein.
- Bei Share-Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.

- Die maximale Länge des Freigabenamens beträgt 80 Zeichen.
- Unicode-Freigabenamen werden unterstützt.
- Freigabenamen, die mit dem $-Zeichen enden, sind versteckte Freigaben.
- Bei ONTAP 9.7 und früheren Versionen werden die administrativen Freigaben admin$, ipc$ und c$ automatisch auf jedem CIFS-Server erstellt und sind reservierte Freigabenamen. Ab ONTAP 9.8 wird die Freigabe admin$ nicht mehr automatisch erstellt.
- Der Freigabename ONTAP_ADMIN$ kann beim Erstellen einer Freigabe nicht verwendet werden.
- Freigabenamen, die Leerzeichen enthalten, werden unterstützt:
  - Ein Leerzeichen darf weder als erstes noch als letztes Zeichen in einem Freigabenamen verwendet werden.
  - Freigabenamen, die ein Leerzeichen enthalten, müssen in Anführungszeichen gesetzt werden.

> Einfache Anführungszeichen gelten als Bestandteil des Freigabenamens und können nicht anstelle von Anführungszeichen verwendet werden.

- Folgende Sonderzeichen werden bei der Benennung von SMB-Freigaben unterstützt:

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- Die folgenden Sonderzeichen sind bei der Benennung von SMB-Freigaben nicht zulässig:

```
** [ ] " / \ : ; | < > , ? * =
```

Informationen zu den Anforderungen an die Groß-/Kleinschreibung von ONTAP SMB-Verzeichnissen beim Erstellen von Freigaben in einer Multiprotokollumgebung

Wenn Sie Freigaben in einer SVM erstellen, in der das 8.3-Namensschema verwendet wird, um zwischen Verzeichnisnamen zu unterscheiden, bei denen es nur Unterschiede in der Groß-/Kleinschreibung gibt, muss der 8.3-Name im Freigabepfad verwendet werden, damit der Client mit dem gewünschten Verzeichnispfad verbunden wird.

Im folgenden Beispiel wurden auf einem Linux-Client zwei Verzeichnisse mit den Namen „testdir“ und „TESTDIR“ erstellt. Der Verbindungspfad des Volumes, das die Verzeichnisse enthält, ist `/home`. Die erste Ausgabe stammt von einem Linux-Client, die zweite Ausgabe von einem SMB-Client.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir
```

```
 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Wenn Sie eine Freigabe für das zweite Verzeichnis erstellen, muss im Freigabepfad der 8.3-Name verwendet werden. In diesem Beispiel ist der Freigabepfad zum ersten Verzeichnis `/home/testdir` und der Freigabepfad zum zweiten Verzeichnis ist `/home/TESTDI~1`.

Freigabeeigenschaften zu bestehenden ONTAP SMB-Freigaben hinzufügen oder entfernen

Sie können eine bestehende SMB-Freigabe anpassen, indem Sie Freigabeeigenschaften hinzufügen oder entfernen.

Die verfügbaren Freigabeeigenschaften sind wie folgt:

Freigabeeigenschaften	Beschreibung
`oplocks`	Diese Eigenschaft legt fest, dass die Freigabe opportunistische Sperren verwendet, auch bekannt als Client-seitiges Caching.
`browsable`	Diese Eigenschaft ermöglicht Windows-Clients das Durchsuchen der Freigabe.
`showsnapshot`	Diese Eigenschaft legt fest, dass Snapshots von Clients angezeigt und durchsucht werden können.
`changenotify`	Diese Eigenschaft gibt an, dass die Freigabe Change Notify-Anforderungen unterstützt. Für Freigaben auf einer SVM ist dies eine standardmäßige Anfangseigenschaft.
`attributecache`	Diese Eigenschaft aktiviert das Caching von Dateiattributen auf der SMB-Freigabe, um einen schnelleren Zugriff auf Attribute zu ermöglichen. Standardmäßig ist das Attribut-Caching deaktiviert. Diese Eigenschaft sollte nur aktiviert werden, wenn Clients über SMB 1.0 auf Freigaben zugreifen. Diese Freigabeeigenschaft ist nicht anwendbar, wenn Clients über SMB 2.x oder SMB 3.0 auf Freigaben zugreifen.
`continuously-available`	Diese Eigenschaft ermöglicht es SMB-Clients, die sie unterstützen, Dateien dauerhaft zu öffnen. Dateien, die auf diese Weise geöffnet werden, sind vor Störungen wie Failover und Giveback geschützt.
`branchcache`	Diese Eigenschaft legt fest, dass die Freigabe es Clients ermöglicht, BranchCache-Hashwerte für die Dateien innerhalb dieser Freigabe anzufordern. Diese Option ist nur relevant, wenn „per-share“ als Betriebsmodus in der CIFS BranchCache-Konfiguration angegeben wird.
`access-based-enumeration`	Diese Eigenschaft legt fest, dass *Access Based Enumeration* (ABE) für diese Freigabe aktiviert ist. ABE-gefilterte freigegebene Ordner sind für einen Benutzer basierend auf dessen individuellen Zugriffsrechten sichtbar, wodurch die Anzeige von Ordnern oder anderen freigegebenen Ressourcen verhindert wird, auf die der Benutzer keine Zugriffsrechte hat.

Freigabeeigenschaften	Beschreibung
`namespace-caching`	Diese Eigenschaft legt fest, dass SMB-Clients, die sich mit dieser Freigabe verbinden, die von den CIFS-Servern zurückgegebenen Ergebnisse der Verzeichnisauflistung zwischenspeichern können, was die Leistung verbessern kann. Standardmäßig speichern SMB 1 Clients keine Ergebnisse der Verzeichnisauflistung. Da SMB 2 und SMB 3 Clients die Ergebnisse der Verzeichnisauflistung standardmäßig zwischenspeichern, bietet die Angabe dieser Freigabeeigenschaft nur SMB 1 Clientverbindungen Leistungsvorteile.
`encrypt-data`	Diese Eigenschaft legt fest, dass beim Zugriff auf diese Freigabe SMB-Verschlüsselung verwendet werden muss. SMB-Clients, die keine Verschlüsselung beim Zugriff auf SMB-Daten unterstützen, haben keinen Zugriff auf diese Freigabe.

Fügen Sie Freigabeeigenschaften zu bestehenden ONTAP SMB-Shares hinzu

Sie können eine bestehende SMB-Freigabe anpassen, indem Sie Freigabeeigenschaften hinzufügen. Dies kann hilfreich sein, wenn Sie die Freigabekonfiguration an geänderte Anforderungen in Ihrer Umgebung anpassen möchten.

Bevor Sie beginnen

Die Freigabe, deren Eigenschaften Sie ändern möchten, muss vorhanden sein.

Über diese Aufgabe

- Es besteht die Möglichkeit, eine oder mehrere Freigabeeigenschaften mithilfe einer durch Kommas getrennten Liste hinzuzufügen.
- Alle zuvor festgelegten Share-Eigenschaften bleiben bestehen.

  Neu hinzugefügte Eigenschaften werden der bestehenden Liste der Share-Eigenschaften hinzugefügt.
- Wenn für bereits auf die Freigabe angewendete Freigabeeigenschaften ein neuer Wert angegeben wird, ersetzt der neu angegebene Wert den ursprünglichen Wert.
- Sie können Freigabeeigenschaften mit dem `vserver cifs share properties add`Befehl nicht entfernen.

  Mit dem `vserver cifs share properties remove` Befehl lassen sich Freigabeeigenschaften entfernen.

Schritte

1. Freigabeeigenschaften hinzufügen:

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

2. Überprüfen Sie die Einstellungen der Freigabeeigenschaften:

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

Beispiel

Der folgende Befehl fügt die `showsnapshot`Share-Eigenschaft zu einer Freigabe mit dem Namen “share1” auf SVM vs1 hinzu:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

Entfernen Sie die Freigabeeigenschaften bestehender ONTAP SMB-Freigaben

Sie können eine bestehende SMB-Freigabe anpassen, indem Sie Freigabeeigenschaften entfernen. Dies kann hilfreich sein, wenn Sie die Freigabekonfiguration an geänderte Anforderungen in Ihrer Umgebung anpassen möchten.

Über diese Aufgabe

- Sie können eine oder mehrere Freigabeeigenschaften mithilfe einer durch Kommas getrennten Liste entfernen.
- Alle zuvor festgelegten, aber nicht entfernten Freigabeeigenschaften bleiben weiterhin wirksam.

Schritte

1. Eigenschaften der Freigabe entfernen:

   ```
   vserver cifs share properties remove -vserver <SVM_name> -share-name
   <share_name> -share-properties <properties>,...
   ```

2. Überprüfen Sie die Einstellungen der Freigabeeigenschaften:

   ```
   vserver cifs share show -vserver <SVM_name> -share-name <share_name>
   ```

Beispiel

Der folgende Befehl entfernt die `browsable` Freigabeeigenschaft von einer Freigabe mit dem Namen “share2” auf SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
```

```
Vserver     Share   Path       Properties   Comment    ACL
---------   ------  --------   ----------   --------   -----------
vs1         share2  /share2    oplocks      -          Everyone / Full
Control
                               changenotify
```

Verwandte Informationen

Befehle zur Verwaltung von Freigaben

ONTAP SMB-Benutzerzugriff mit der Einstellung „force-group share“ optimieren

Wenn Sie über die ONTAP Befehlszeile eine Freigabe für Daten mit effektiver UNIX-Sicherheit erstellen, kann festgelegt werden, dass alle von SMB-Benutzern in dieser Freigabe erstellten Dateien derselben Gruppe angehören, der sogenannten *force-group*, die eine vordefinierte Gruppe in der UNIX-Gruppendatenbank sein muss. Die Verwendung einer Force-Group vereinfacht es, sicherzustellen, dass Dateien von SMB-Benutzern aus verschiedenen Gruppen abgerufen werden können.

Die Angabe einer Force-Gruppe ist nur dann sinnvoll, wenn sich die Freigabe in einem UNIX- oder gemischten qtree befindet. Für Freigaben in einem NTFS-Volume oder qtree ist keine Force-Gruppe erforderlich, da der Zugriff auf Dateien in diesen Freigaben durch Windows-Berechtigungen und nicht durch UNIX-GIDs bestimmt wird.

Wenn für eine Freigabe eine Force-Gruppe festgelegt wurde, gilt für diese Freigabe Folgendes:

- SMB-Benutzer in der Force-Gruppe, die auf diese Freigabe zugreifen, werden vorübergehend auf die GID der Force-Gruppe geändert.

  Diese GID ermöglicht ihnen den Zugriff auf Dateien in dieser Freigabe, die mit ihrer primären GID oder UID normalerweise nicht zugänglich sind.

- Alle von SMB-Benutzern in dieser Freigabe erstellten Dateien gehören derselben Force-Gruppe an, unabhängig von der primären GID des Dateibesitzers.

Wenn SMB-Benutzer versuchen, auf eine von NFS erstellte Datei zuzugreifen, bestimmen die primären GIDs der SMB-Benutzer die Zugriffsrechte.

Die Force-Gruppe hat keinen Einfluss darauf, wie NFS-Benutzer auf Dateien in dieser Freigabe zugreifen. Eine von NFS erstellte Datei erhält die GID vom Dateibesitzer. Die Zugriffsberechtigungen werden anhand der UID und der primären GID des NFS-Benutzers bestimmt, der versucht, auf die Datei zuzugreifen.

Die Verwendung einer Force-Group vereinfacht es, sicherzustellen, dass Dateien von SMB-Benutzern aus verschiedenen Gruppen abgerufen werden können. Wenn beispielsweise eine Freigabe erstellt werden soll, um die Webseiten des Unternehmens zu speichern und Benutzern aus den Abteilungen Engineering und Marketing Schreibzugriff zu gewähren, kann eine Freigabe erstellt und der Force-Group mit dem Namen „webgroup1“ Schreibzugriff erteilt werden. Aufgrund der Force-Group gehören alle von SMB-Benutzern in dieser Freigabe erstellten Dateien der Gruppe „webgroup1“. Zusätzlich wird Benutzern beim Zugriff auf die Freigabe automatisch die GID der Gruppe „webgroup1“ zugewiesen. So können alle Benutzer auf diese Freigabe schreiben, ohne dass die Zugriffsrechte der Benutzer in den Abteilungen Engineering und Marketing verwaltet werden müssen.

Verwandte Informationen

Freigaben mit der Einstellung „force-group share“ erstellen

ONTAP SMB-Freigaben mit der Einstellung „force-group share“ erstellen

Eine SMB-Freigabe mit der Einstellung „force-group share“ kann erstellt werden, wenn SMB-Benutzer, die auf Daten auf Volumes oder Qtrees mit UNIX-Dateisicherheit zugreifen, von ONTAP als Mitglieder derselben UNIX-Gruppe betrachtet werden sollen.

Schritt

1. Die SMB-Freigabe wird erstellt: `vserver cifs share create -vserver` *`vserver_name`* `-share -name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   Wenn der UNC-Pfad (`\\servername\sharename\filepath`) der Freigabe mehr als 256 Zeichen enthält (ohne das anfängliche „`\\`“ im UNC-Pfad), ist die Registerkarte **Sicherheit** im Windows-Eigenschaftenfenster nicht verfügbar. Dies ist ein Problem des Windows-Clients und nicht von ONTAP. Um dieses Problem zu vermeiden, sollten keine Freigaben mit UNC-Pfaden erstellt werden, die mehr als 256 Zeichen enthalten.

   Wenn die Erzwingungsgruppe nach der Erstellung der Freigabe entfernt werden soll, kann die Freigabe jederzeit bearbeitet und eine leere Zeichenfolge (""") als Wert für den `-force-group-for-create` Parameter angegeben werden. Wenn die Erzwingungsgruppe durch Bearbeiten der Freigabe entfernt wird, behalten alle bestehenden Verbindungen zu dieser Freigabe die zuvor festgelegte Erzwingungsgruppe als primäre GID bei.

Beispiel

Der folgende Befehl erstellt eine Freigabe „`webpages`“, die im Web im `/corp/companyinfo` Verzeichnis zugänglich ist, in dem alle Dateien, die SMB-Benutzer erstellen, der Gruppe webgroup1 zugewiesen werden:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Verwandte Informationen

Benutzerzugriff mit der Einstellung „force-group share“ optimieren

Informationen zu ONTAP SMB-Freigaben mit der MMC anzeigen

Informationen zu SMB-Freigaben auf Ihrer SVM lassen sich anzeigen und einige Verwaltungsaufgaben mithilfe der Microsoft Management Console (MMC) durchführen. Zum Anzeigen der Freigaben ist eine Verbindung der MMC mit der SVM erforderlich.

Über diese Aufgabe

Mit der MMC lassen sich die folgenden Aufgaben für in SVMs enthaltene Freigaben durchführen:

- Freigaben anzeigen
- Aktive Sitzungen anzeigen
- Offene Dateien anzeigen
- Die Liste der Sitzungen, Dateien und Baumverbindungen im System wird aufgezählt.
- Offene Dateien im System schließen

- Offene Sitzungen schließen
- Freigaben erstellen/verwalten

> Die von den vorherigen Funktionen angezeigten Ansichten sind knotenspezifisch und nicht clusterspezifisch. Daher wird bei Verwendung der MMC zur Verbindung mit dem SMB-Server-Hostnamen (das heißt cifs01.domain.local) abhängig von der DNS-Konfiguration zu einer einzelnen LIF innerhalb des Clusters weitergeleitet.

Die folgenden Funktionen werden in MMC für ONTAP nicht unterstützt:

- Erstellen neuer lokaler Benutzer/Gruppen
- Verwaltung/Anzeige bestehender lokaler Benutzer/Gruppen
- Anzeigen von Ereignissen oder Leistungsprotokollen
- Storage
- Dienste und Anwendungen

In Fällen, in denen die Operation nicht unterstützt wird, können Sie `remote procedure call failed`Fehler erleben.

"Häufig gestellte Fragen: Verwendung der Windows MMC mit ONTAP"

Schritte

1. Die Computer Management MMC auf einem beliebigen Windows Server wird in der **Systemsteuerung** unter **Verwaltung** > **Computerverwaltung** geöffnet.
2. **Aktion** > **Mit einem anderen Computer verbinden** auswählen.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.
3. Den Namen des Speichersystems eingeben oder auf **Durchsuchen** klicken, um das Speichersystem zu finden.
4. Klicken Sie auf **OK**.

   Der MMC stellt eine Verbindung zum SVM her.
5. Im Navigationsbereich auf **Freigegebene Ordner** > **Freigaben** klicken.

   Im rechten Anzeigebereich wird eine Liste der Shares auf der SVM angezeigt.
6. Die Freigabeeigenschaften einer Freigabe werden angezeigt, wenn auf die Freigabe doppelt geklickt wird, wodurch das Dialogfeld **Eigenschaften** geöffnet wird.
7. Wenn keine Verbindung zum Speichersystem über die MMC möglich ist, kann der Benutzer der Gruppe BUILTIN\Administrators oder BUILTIN\Power Users auf dem Speichersystem mit einem der folgenden Befehle hinzugefügt werden:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
```

```
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

ONTAP Befehle zur Verwaltung von SMB-Freigaben

Sie verwenden die `vserver cifs share`- und `vserver cifs share properties` -Befehle, um SMB-Freigaben zu verwalten.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Erstellen Sie eine SMB-Freigabe	`vserver cifs share create`
SMB-Freigaben anzeigen	`vserver cifs share show`
Ändern einer SMB-Freigabe	`vserver cifs share modify`
Eine SMB-Freigabe löschen	`vserver cifs share delete`
Freigabeeigenschaften zu einer bestehenden Freigabe hinzufügen	`vserver cifs share properties add`
Freigabeeigenschaften von einer bestehenden Freigabe entfernen	`vserver cifs share properties remove`
Informationen zu Aktieneigenschaften	`vserver cifs share properties show`

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

Sicherer Dateizugriff mithilfe von SMB-Freigabe-ACLs

Informationen zur Verwaltung von ONTAP SMB-ACLs auf Freigabeebene

Sie können die Zugriffssteuerungslisten (ACLs) auf Freigabeebene ändern, um Benutzern mehr oder weniger Zugriffsrechte auf die Freigabe zu gewähren. Sie können die ACLs auf Freigabeebene entweder mit Windows-Benutzern und -Gruppen oder mit UNIX-Benutzern und -Gruppen konfigurieren.

Standardmäßig gewährt die Freigabe-ACL der Standardgruppe „Jeder“ Vollzugriff. Vollzugriff in der ACL bedeutet, dass alle Benutzer in der Domäne und alle vertrauenswürdigen Domänen uneingeschränkten Zugriff auf die Freigabe haben. Das Zugriffslevel einer Freigabe-ACL lässt sich über die Microsoft Management Console (MMC) auf einem Windows-Client oder die ONTAP Befehlszeile steuern. "Freigabe-Zugriffskontrolllisten erstellen".

Bei der Verwendung des MMC gelten folgende Richtlinien:

- Die angegebenen Benutzer- und Gruppennamen müssen Windows-Namen sein.
- Es können nur Windows-Berechtigungen angegeben werden.

Die folgenden Richtlinien gelten bei Verwendung der ONTAP Befehlszeile:

- Die angegebenen Benutzer- und Gruppennamen können Windows-Namen oder UNIX-Namen sein.

  Wenn beim Erstellen oder Ändern von ACLs kein Benutzer- und Gruppentyp angegeben wird, ist der Standardtyp Windows-Benutzer und -Gruppen.

- Es können nur Windows-Berechtigungen angegeben werden.

Erstellen von ONTAP SMB-Freigabe-Zugriffssteuerungslisten

Die Konfiguration von Freigabeberechtigungen durch das Erstellen von Zugriffssteuerungslisten (ACLs) für SMB-Freigaben ermöglicht die Kontrolle der Zugriffsebene auf eine Freigabe für Benutzer und Gruppen.

Über diese Aufgabe

Sie können Zugriffssteuerungslisten auf Freigabeebene konfigurieren, indem Sie lokale oder Domänen-Windows-Benutzer- oder Gruppennamen oder UNIX-Benutzer- oder Gruppennamen verwenden.

Bevor Sie eine neue ACL erstellen, sollten Sie die standardmäßige Freigabe-ACL `Everyone / Full Control` löschen, da diese ein Sicherheitsrisiko darstellt.

Im Arbeitsgruppenmodus ist der lokale Domänenname der SMB-Servername.

Schritte

1. Die Standard-Freigabe-ACL löschen: `vserver cifs share access-control delete -vserver <vserver_name> -share <share_name> -user-or-group Everyone`
2. Die neue Zugriffssteuerungsliste (ACL) konfigurieren:

Wenn Sie Zugriffssteuerungslisten (ACLs) mithilfe von… konfigurieren möchten	Geben Sie den Befehl ein…
Windows Benutzer	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Windows Gruppe	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
UNIX-Benutzer	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIX-Gruppe	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Es kann überprüft werden, ob die auf die Freigabe angewendete Zugriffssteuerungsliste (ACL) korrekt ist, indem der `vserver cifs share access-control show` Befehl verwendet wird.

Beispiel

Der folgende Befehl erteilt `Change` der Windows-Gruppe “Sales Team” Berechtigungen für die Freigabe “sales” auf der “vs1.example.com”-SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

Der folgende Befehl erteilt `Read` der UNIX-Gruppe „engineering“ die Berechtigung für die Freigabe „eng“ auf der SVM „vs2.example.com“:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

Die folgenden Befehle erteilen `Change`der lokalen Windows-Gruppe „Tiger Team“ und `Full_Control`dem lokalen Windows-Benutzer „Sue Chang“ die Berechtigung für die Freigabe „datavol5“ auf der SVM „vs1“:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
```

```
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

ONTAP Befehle zur Verwaltung von SMB-Freigabezugriffskontrolllisten

Sie müssen die Befehle zur Verwaltung von SMB-Zugriffskontrolllisten (ACLs) kennen, einschließlich deren Erstellung, Anzeige, Änderung und Löschung.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine neue ACL erstellen	`vserver cifs share access-control create`
ACLs anzeigen	`vserver cifs share access-control show`
Eine ACL ändern	`vserver cifs share access-control modify`
Eine ACL löschen	`vserver cifs share access-control delete`

Dateizugriff mithilfe von Dateiberechtigungen absichern

Erweiterte NTFS-Dateiberechtigungen mithilfe der Registerkarte „Windows-Sicherheit“ für ONTAP SMB SVMs konfigurieren

Standard-NTFS-Dateiberechtigungen für Dateien und Ordner lassen sich über die Registerkarte **Windows-Sicherheit** im Fenster „Windows-Eigenschaften“ konfigurieren.

Bevor Sie beginnen

Der Administrator, der diese Aufgabe ausführt, muss über ausreichende NTFS-Berechtigungen verfügen, um die Berechtigungen für die ausgewählten Objekte zu ändern.

Über diese Aufgabe

Die Konfiguration von NTFS-Dateiberechtigungen erfolgt auf einem Windows-Host durch Hinzufügen von

Einträgen zu NTFS-Zugriffskontrolllisten (DACLs), die einem NTFS-Sicherheitsdeskriptor zugeordnet sind. Der Sicherheitsdeskriptor wird anschließend auf NTFS-Dateien und Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows-Benutzeroberfläche übernommen.

Schritte

1. Im Menü **Extras** des Windows Explorers **Netzlaufwerk verbinden** auswählen.
2. Das Dialogfeld **Netzlaufwerk verbinden** ausfüllen:

   a. Einen Laufwerksbuchstaben auswählen.

   b. Geben Sie im Feld **Ordner** den Namen des CIFS-Servers ein, der die Freigabe enthält, die die Daten enthält, für die Berechtigungen angewendet werden sollen, sowie den Namen der Freigabe.

      Wenn der Name Ihres CIFS-Servers “CIFS_SERVER” ist und Ihre Freigabe “share1” heißt, sollte `\\CIFS_SERVER\share1` eingegeben werden.

      Sie können die IP-Adresse der Datenschnittstelle für den CIFS-Server anstelle des CIFS-Servernamens angeben.

   c. Klicken Sie auf **Finish**.

   Das von Ihnen ausgewählte Laufwerk ist eingebunden und einsatzbereit, wobei das Windows Explorer-Fenster die in der Freigabe enthaltenen Dateien und Ordner anzeigt.

3. Wählen Sie die Datei oder das Verzeichnis aus, für das NTFS-Dateiberechtigungen festgelegt werden sollen.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis und wählen Sie dann **Eigenschaften**.
5. Die Registerkarte **Sicherheit** auswählen.

   Die Registerkarte **Sicherheit** zeigt die Liste der Benutzer und Gruppen an, für die NTFS-Berechtigungen festgelegt sind. Das Feld **Berechtigungen für** zeigt eine Liste der für jeden ausgewählten Benutzer oder jede ausgewählte Gruppe geltenden Allow- und Deny-Berechtigungen an.

6. Auf **Erweitert** klicken.

   Das Fenster „Windows-Eigenschaften“ zeigt Informationen zu bestehenden Dateiberechtigungen an, die Benutzern und Gruppen zugewiesen sind.

7. **Berechtigungen ändern** auswählen.

   Das Berechtigungsfenster wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie möchten…	Führen Sie folgende Schritte aus…
Erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe festlegen	a. Klicken Sie auf **Add**. b. Im Feld **Geben Sie den Namen des auszuwählenden Objekts ein** den Namen des Benutzers oder der Gruppe eingeben, die hinzugefügt werden soll. c. Klicken Sie auf **OK**.

Wenn Sie möchten…	Führen Sie folgende Schritte aus…
Erweiterte NTFS-Berechtigungen eines Benutzers oder einer Gruppe ändern	a. Im Feld **Berechtigungseinträge:** den Benutzer oder die Gruppe auswählen, deren erweiterte Berechtigungen geändert werden sollen. b. Klicken Sie auf **Bearbeiten**.
Erweiterte NTFS-Berechtigungen für einen Benutzer oder eine Gruppe entfernen	a. Im Feld **Berechtigungseinträge:** den Benutzer oder die Gruppe auswählen, die entfernt werden soll. b. Klicken Sie auf **Entfernen**. c. Weiter zu Schritt 13.

Wenn erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe hinzugefügt oder die erweiterten NTFS-Berechtigungen für einen bestehenden Benutzer oder eine bestehende Gruppe geändert werden, öffnet sich das Dialogfeld „Berechtigungseintrag für <Object>“.

9. Im Feld **Anwenden auf** kann ausgewählt werden, wie dieser NTFS-Dateiberechtigungseintrag angewendet werden soll.

   Wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei einrichten, ist das Feld **Anwenden auf** nicht aktiv. Die Einstellung **Anwenden auf** ist standardmäßig auf **Nur dieses Objekt** festgelegt.

10. Im Feld **Berechtigungen** werden die Kontrollkästchen **Zulassen** oder **Verweigern** für die erweiterten Berechtigungen ausgewählt, die auf dieses Objekt angewendet werden sollen.

    - Um den angegebenen Zugriff zuzulassen, das Kontrollkästchen **Zulassen** auswählen.
    - Um den angegebenen Zugriff nicht zuzulassen, das Kontrollkästchen **Verweigern** auswählen. Berechtigungen können für die folgenden erweiterten Rechte festgelegt werden:
    - **Volle Kontrolle**

      Wenn diese erweiterte Berechtigung ausgewählt wird, werden alle anderen erweiterten Berechtigungen automatisch ausgewählt (entweder „Erlauben“ oder „Verweigern“).

    - **Ordner durchsuchen / Datei ausführen**
    - **Ordner auflisten / Daten lesen**
    - **Attribute lesen**
    - **Erweiterte Attribute lesen**
    - **Dateien erstellen / Daten schreiben**
    - **Ordner erstellen / Daten anhängen**
    - **Attribute schreiben**
    - **Erweiterte Attribute schreiben**
    - **Unterordner und Dateien löschen**
    - **Löschen**
    - **Leseberechtigungen**
    - **Berechtigungen ändern**
    - **Verantwortung übernehmen**

Falls einzelne Kontrollkästchen für erweiterte Berechtigungen nicht auswählbar sind, liegt dies daran, dass die Berechtigungen vom übergeordneten Objekt geerbt werden.

11. Wenn Unterordner und Dateien dieses Objekts diese Berechtigungen erben sollen, aktivieren Sie das Kontrollkästchen **Diese Berechtigungen nur auf Objekte und/oder Container innerhalb dieses Containers anwenden**.
12. Klicken Sie auf **OK**.
13. Nachdem das Hinzufügen, Entfernen oder Bearbeiten von NTFS-Berechtigungen abgeschlossen ist, wird die Vererbungseinstellung für dieses Objekt festgelegt:
    - Das Kontrollkästchen **Vererbbare Berechtigungen vom übergeordneten Objekt einbeziehen** auswählen.

      Dies ist die Standardeinstellung.
    - Das Kontrollkästchen **Alle Berechtigungen von untergeordneten Objekten durch von diesem Objekt vererbbare Berechtigungen ersetzen** auswählen.

      Diese Einstellung ist im Dialogfeld „Berechtigungen“ nicht vorhanden, wenn NTFS-Dateiberechtigungen für eine einzelne Datei festgelegt werden.

      Seien Sie bei der Auswahl dieser Einstellung vorsichtig. Diese Einstellung entfernt alle vorhandenen Berechtigungen auf allen untergeordneten Objekten und ersetzt sie durch die Berechtigungseinstellungen dieses Objekts. Es könnten versehentlich Berechtigungen entfernt werden, die nicht entfernt werden sollten. Dies ist besonders relevant beim Festlegen von Berechtigungen in einem Volume oder qtree mit gemischtem Sicherheitsstil. Wenn untergeordnete Objekte einen effektiven UNIX-Sicherheitsstil aufweisen, führt das Übertragen von NTFS-Berechtigungen auf diese untergeordneten Objekte dazu, dass ONTAP diese Objekte vom UNIX-Sicherheitsstil in den NTFS-Sicherheitsstil ändert und alle UNIX-Berechtigungen auf diesen untergeordneten Objekten durch NTFS-Berechtigungen ersetzt werden.
    - Wählen Sie beide Kästchen aus.
    - Keines der Kästchen wird ausgewählt.
14. Klicken Sie auf **OK**, um das Fenster **Berechtigungen** zu schließen.
15. Klicken Sie auf **OK**, um das Fenster **Erweiterte Sicherheitseinstellungen für <Object>** zu schließen.

    Weitere Informationen zum Festlegen erweiterter NTFS-Berechtigungen enthält die Windows-Dokumentation.

Verwandte Informationen

- NTFS-Sicherheitsdeskriptoren auf Servern erstellen
- Informationen zur Dateisicherheit auf NTFS Security-Style-Volumes
- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

ONTAP Befehle für SMB NTFS-Dateiberechtigungen

NTFS-Dateiberechtigungen für Dateien und Verzeichnisse lassen sich mithilfe der

ONTAP-Befehlszeilenschnittstelle konfigurieren. Dies ermöglicht die Konfiguration von NTFS-Dateiberechtigungen, ohne dass eine Verbindung zu den Daten über eine SMB-Freigabe auf einem Windows-Client erforderlich ist.

Sie können NTFS-Dateiberechtigungen konfigurieren, indem Sie Einträge zu den NTFS-Zugriffskontrolllisten (DACLs) hinzufügen, die einem NTFS-Sicherheitsdeskriptor zugeordnet sind. Der Sicherheitsdeskriptor wird anschließend auf NTFS-Dateien und Verzeichnisse angewendet.

NTFS-Dateiberechtigungen können nur über die Befehlszeile konfiguriert werden. NFSv4-ACLs können über die Befehlszeile nicht konfiguriert werden.

Schritte

1. Ein NTFS-Sicherheitsdeskriptor wird erstellt.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. DACLs zum NTFS-Sicherheitsdeskriptor hinzufügen.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. Eine Datei-/Verzeichnissicherheitsrichtlinie erstellen.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

UNIX-Dateiberechtigungen bieten Zugriffskontrolle beim Zugriff auf Dateien über ONTAP SMB-Server.

Ein FlexVol volume kann einen von drei Sicherheitsstilen aufweisen: NTFS, UNIX oder gemischt. Der Zugriff auf Daten über SMB ist unabhängig vom Sicherheitsstil möglich; für den Zugriff auf Daten mit effektiver UNIX-Sicherheit sind jedoch entsprechende UNIX-Dateiberechtigungen erforderlich.

Beim Datenzugriff über SMB kommen verschiedene Zugriffskontrollen zum Einsatz, um festzustellen, ob ein Benutzer zur Ausführung einer angeforderten Aktion berechtigt ist:

- Exportberechtigungen

  Die Konfiguration von Exportberechtigungen für den SMB-Zugriff ist optional.

- Freigabeberechtigungen
- Dateiberechtigungen

  Folgende Arten von Dateiberechtigungen können für die Daten angewendet werden, auf denen der Benutzer eine Aktion ausführen möchte:

  - NTFS

- UNIX NFSv4-ACLs
- UNIX-Modusbits

Für Daten mit NFSv4-ACLs oder gesetzten UNIX-Modusbits werden UNIX-Style-Berechtigungen verwendet, um die Dateizugriffsrechte auf die Daten zu bestimmen. Der SVM-Administrator muss die entsprechenden Dateiberechtigungen festlegen, damit Benutzer die Rechte haben, die gewünschte Aktion durchzuführen.

Daten in einem Volume mit gemischtem Sicherheitsstil können entweder den effektiven Sicherheitsstil NTFS oder UNIX aufweisen. Wenn die Daten den effektiven UNIX-Sicherheitsstil haben, werden NFSv4-Berechtigungen oder UNIX-Modusbits verwendet, um die Dateizugriffsrechte für die Daten zu bestimmen.

Sicherer Dateizugriff durch Dynamic Access Control (DAC)

Informationen zur DAC-Dateizugriffsicherheit für ONTAP SMB-Server

Sie können den Zugriff sichern, indem Sie die dynamische Zugriffssteuerung nutzen und zentrale Zugriffsrichtlinien in Active Directory erstellen und diese über angewendete Gruppenrichtlinienobjekte (GPOs) auf Dateien und Ordner auf SVMs anwenden. Es besteht die Möglichkeit, die Protokollierung so zu konfigurieren, dass zentrale Zugriffsrichtlinien-Staging-Ereignisse verwendet werden, um die Auswirkungen von Änderungen an zentralen Zugriffsrichtlinien zu sehen, bevor diese angewendet werden.

Ergänzungen zu den CIFS-Anmeldeinformationen

Vor der dynamischen Zugriffssteuerung enthielt eine CIFS-Anmeldeinformation die Identität des Sicherheitsprinzipals (des Benutzers) und die Windows-Gruppenzugehörigkeit. Mit der dynamischen Zugriffssteuerung werden der Anmeldeinformation drei weitere Informationstypen hinzugefügt: Geräteidentität, Geräteansprüche und Benutzeransprüche.

- Geräteidentität

  Das Analogon zu den Identitätsinformationen des Benutzers, nur dass es sich um die Identität und Gruppenzugehörigkeit des Geräts handelt, von dem sich der Benutzer einloggt.

- Geräteansprüche

  Aussagen über einen Gerätesicherheitsprinzipal. Beispielsweise könnte eine Geräteaussage lauten, dass das Gerät Mitglied einer bestimmten Organisationseinheit (OU) ist.

- Benutzeransprüche

  Aussagen über einen Benutzer-Sicherheitsprinzipal. Beispielsweise könnte eine Benutzer-Assertion lauten, dass das AD-Konto Mitglied einer bestimmten OU ist.

Zentrale Zugriffsrichtlinien

Zentrale Zugriffsrichtlinien für Dateien ermöglichen Organisationen, Autorisierungsrichtlinien, die bedingte Ausdrücke mit Benutzergruppen, Benutzeransprüchen, Geräteansprüchen und Ressourceneigenschaften enthalten, zentral bereitzustellen und zu verwalten.

Beispielsweise muss ein Benutzer, um auf geschäftskritische Daten zuzugreifen, Vollzeitbeschäftigter sein und darf nur von einem verwalteten Gerät aus auf die Daten zugreifen. Zentrale Zugriffsrichtlinien werden in Active Directory definiert und über den GPO-Mechanismus an Dateiserver verteilt.

Zentrale Bereitstellung von Zugriffsrichtlinien mit erweiterter Protokollierung

Zentrale Zugriffsrichtlinien können „staged“ werden, wobei sie bei Dateizugriffsprüfungen in einer „what-if“-Manier ausgewertet werden. Die Ergebnisse dessen, was passiert wäre, wenn die Richtlinie wirksam gewesen wäre, und wie sich das von der aktuellen Konfiguration unterscheidet, werden als Protokollierungsereignis erfasst. Auf diese Weise können Administratoren Protokollierungsereignisse nutzen, um die Auswirkungen einer Änderung der Zugriffsrichtlinie zu untersuchen, bevor die Richtlinie tatsächlich angewendet wird. Nach der Bewertung der Auswirkungen einer Änderung der Zugriffsrichtlinie kann die Richtlinie über GPOs auf die gewünschten SVMs bereitgestellt werden.

Verwandte Informationen

- Informationen zu unterstützten Gruppenrichtlinienobjekten (GPOs)
- Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- GPO-Unterstützung auf Servern aktivieren oder deaktivieren
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln
- Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf Servern zu sichern.
- Informationen zur Serversicherheit
- "SMB und NFS Auditierung und Sicherheitsverfolgung"

Unterstützte DAC-Funktionalität für ONTAP SMB Server

Wenn Sie Dynamic Access Control (DAC) auf Ihrem CIFS-Server verwenden möchten, ist es wichtig zu verstehen, wie ONTAP die Dynamic Access Control Funktionalität in Active Directory-Umgebungen unterstützt.

Unterstützt für Dynamic Access Control

ONTAP unterstützt die folgende Funktionalität, wenn die Dynamic Access Control auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Ansprüche im Dateisystem	Ansprüche sind einfache Namens-Wert-Paare, die eine bestimmte Wahrheit über einen Benutzer aussagen. Benutzeranmeldeinformationen enthalten Anspruchsinformationen, und Sicherheitsdeskriptoren von Dateien können Zugriffsprüfungen durchführen, die auch Anspruchsprüfungen umfassen. Dies gibt Administratoren eine feinere Kontrolle darüber, wer auf Dateien zugreifen kann.

Funktionalität	Kommentare
Bedingte Ausdrücke für Dateizugriffsprüfungen	Beim Ändern der Sicherheitsparameter einer Datei können Benutzer dem Sicherheitsdeskriptor der Datei beliebig komplexe bedingte Ausdrücke hinzufügen. Der bedingte Ausdruck kann Prüfungen auf Claims enthalten.
Zentrale Steuerung des Dateizugriffs über zentrale Zugriffsrichtlinien	Zentrale Zugriffsrichtlinien sind eine Art Zugriffskontrollliste (ACL), die in Active Directory gespeichert und einer Datei zugeordnet werden kann. Der Zugriff auf die Datei wird nur gewährt, wenn sowohl die Zugriffsprüfungen des Sicherheitsdeskriptors auf dem Datenträger als auch die zugeordnete zentrale Zugriffsrichtlinie den Zugriff erlauben. Dies ermöglicht Administratoren, den Zugriff auf Dateien zentral (in Active Directory) zu steuern, ohne den Sicherheitsdeskriptor auf dem Datenträger ändern zu müssen.
Staging der zentralen Zugriffsrichtlinie	Fügt die Möglichkeit hinzu, Sicherheitsänderungen auszuprobieren, ohne den tatsächlichen Dateizugriff zu beeinflussen, indem eine Änderung an den zentralen Zugriffsrichtlinien „gestagt“ wird und die Auswirkung der Änderung in einem Prüfbericht angezeigt wird.
Unterstützung für die Anzeige von Informationen zur zentralen Zugriffsrichtliniensicherheit mithilfe der ONTAP CLI	Erweitert den `vserver security file-directory show` Befehl, um Informationen über angewendete zentrale Zugriffsrichtlinien anzuzeigen.
Sicherheitsverfolgung einschließlich zentraler Zugriffsrichtlinien	Erweitert die `vserver security trace`Befehlsfamilie und zeigt Ergebnisse an, die Informationen über angewendete zentrale Zugriffsrichtlinien enthalten.

Nicht unterstützt für Dynamic Access Control

ONTAP unterstützt die folgende Funktionalität nicht, wenn die Dynamic Access Control auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Automatische Klassifizierung von NTFS-Dateisystemobjekten	Dies ist eine Erweiterung der Windows-Dateiklassifizierungsinfrastruktur, die in ONTAP nicht unterstützt wird.
Erweiterte Überwachung mit Ausnahme des Stagings von zentralen Zugriffsrichtlinien	Nur das zentrale Staging von Zugriffsrichtlinien wird für erweiterte Prüfverfahren unterstützt.

Informationen zur Verwendung von DAC und zentralen Zugriffsrichtlinien mit ONTAP SMB-Servern

Bei der Verwendung von Dynamic Access Control (DAC) und zentralen Zugriffsrichtlinien zum Schutz von Dateien und Ordnern auf CIFS-Servern sind bestimmte Aspekte zu berücksichtigen.

Der NFS-Zugriff kann dem Root-Benutzer verweigert werden, wenn eine Richtlinienregel für den Benutzer „domain\administrator“ gilt.

Unter bestimmten Umständen kann der NFS-Zugriff auf Root verweigert werden, wenn auf die Daten, auf die der Root-Benutzer zugreifen möchte, eine zentrale Zugriffsrichtlinie angewendet wird. Das Problem tritt auf, wenn die zentrale Zugriffsrichtlinie eine Regel enthält, die auf domain\administrator angewendet wird und das Root-Konto dem domain\administrator-Konto zugeordnet ist.

Anstatt die Regel auf den Benutzer domain\administrator anzuwenden, sollte die Regel auf eine Gruppe mit administrativen Rechten angewendet werden, wie zum Beispiel die domain\administrators Gruppe. Auf diese Weise kann root dem domain\administrator Konto zugeordnet werden, ohne dass root von diesem Problem betroffen ist.

Die Gruppe BUILTIN\Administrators des CIFS-Servers hat Zugriff auf Ressourcen, wenn die angewendete zentrale Zugriffsrichtlinie in Active Directory nicht gefunden wird.

Es ist möglich, dass auf Ressourcen innerhalb des CIFS-Servers zentrale Zugriffsrichtlinien angewendet werden. Wenn der CIFS-Server versucht, mithilfe der SID der zentralen Zugriffsrichtlinie Informationen aus Active Directory abzurufen, stimmt die SID mit keiner vorhandenen SID einer zentralen Zugriffsrichtlinie in Active Directory überein. Unter diesen Umständen wendet der CIFS-Server die lokale Standardwiederherstellungsrichtlinie für diese Ressource an.

Die lokale Standardwiederherstellungsrichtlinie gewährt der Gruppe BUILTIN\Administrators des CIFS-Servers Zugriff auf diese Ressource.

DAC für ONTAP SMB-Server aktivieren oder deaktivieren

Die Option, mit der Sie Dynamic Access Control (DAC) zum Schutz von Objekten auf Ihrem CIFS-Server verwenden können, ist standardmäßig deaktiviert. Die Option muss aktiviert werden, wenn Dynamic Access Control auf dem CIFS-Server verwendet werden soll. Falls später entschieden wird, Dynamic Access Control nicht mehr zum Schutz von auf dem CIFS-Server gespeicherten Objekten zu verwenden, kann die Option deaktiviert werden.

Informationen darüber, wie die dynamische Zugriffssteuerung in Active Directory konfiguriert wird, sind in der Microsoft TechNet Library zu finden.

"Microsoft TechNet: Übersicht über Szenarien zur dynamischen Zugriffskontrolle"

Über diese Aufgabe

Sobald die dynamische Zugriffskontrolle aktiviert ist, kann das Dateisystem ACLs mit Einträgen zur dynamischen Zugriffskontrolle enthalten. Wenn die dynamische Zugriffskontrolle deaktiviert ist, werden die aktuellen Einträge zur dynamischen Zugriffskontrolle ignoriert und neue werden nicht zugelassen.

Diese Option ist nur auf der Stufe „Erweitert“ verfügbar.

Schritt

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

Wenn Sie möchten, dass die Dynamic Access Control…	Geben Sie den Befehl ein…

Aktiviert	`vserver cifs options modify -vserver vserver_name -is-dac-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -is-dac-enabled false`

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

Verwandte Informationen

Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf Servern zu sichern.

Verwaltung von ACLs mit DAC-ACEs, wenn DAC auf ONTAP SMB-Servern deaktiviert ist

Wenn Sie Ressourcen haben, auf die ACLs mit Dynamic Access Control ACEs angewendet wurden, und Sie Dynamic Access Control auf der Storage Virtual Machine (SVM) deaktivieren, müssen Sie die Dynamic Access Control ACEs entfernen, bevor Sie die nicht-Dynamic Access Control ACEs auf dieser Ressource verwalten können.

Über diese Aufgabe

Nachdem die dynamische Zugriffskontrolle deaktiviert ist, können bestehende nicht-dynamische Zugriffskontroll-ACEs weder entfernt noch neue nicht-dynamische Zugriffskontroll-ACEs hinzugefügt werden, bis die bestehenden dynamischen Zugriffskontroll-ACEs entfernt wurden.

Sie können das Tool, das Sie normalerweise zur Verwaltung von ACLs verwenden, für diese Schritte einsetzen.

Schritte

1. Ermitteln, welche Dynamic Access Control ACEs auf die Ressource angewendet sind.
2. Die ACEs der dynamischen Zugriffssteuerung aus der Ressource entfernen.
3. Nicht-dynamische Zugriffskontroll-ACEs können nach Bedarf zur Ressource hinzugefügt oder daraus entfernt werden.

Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf ONTAP SMB Servern zu schützen

Es sind mehrere Schritte erforderlich, um den Zugriff auf Daten auf dem CIFS-Server mithilfe zentraler Zugriffsrichtlinien zu sichern, darunter das Aktivieren der Dynamic Access Control (DAC) auf dem CIFS-Server, das Konfigurieren zentraler Zugriffsrichtlinien in Active Directory, das Anwenden der zentralen Zugriffsrichtlinien auf Active Directory Container mit Gruppenrichtlinienobjekten (GPOs) und das Aktivieren von GPOs auf dem CIFS-Server.

Bevor Sie beginnen

- Das Active Directory muss so konfiguriert sein, dass zentrale Zugriffsrichtlinien verwendet werden.
- Sie benötigen ausreichende Zugriffsrechte auf den Active Directory Domänencontrollern, um zentrale Zugriffsrichtlinien zu erstellen und GPOs auf die Container zu erstellen und anzuwenden, die die CIFS-Server enthalten.

- Sie benötigen ausreichende administrative Zugriffsrechte auf der Storage Virtual Machine (SVM), um die erforderlichen Befehle auszuführen.

Über diese Aufgabe

Zentrale Zugriffsrichtlinien werden definiert und auf Gruppenrichtlinienobjekte (GPOs) in Active Directory angewendet. Informationen zur Konfiguration zentraler Zugriffsrichtlinien in Active Directory sind in der Microsoft TechNet Library verfügbar.

"Microsoft TechNet: Szenario für zentrale Zugriffsrichtlinie"

Schritte

1. Die dynamische Zugriffskontrolle auf der SVM kann aktiviert werden, falls sie noch nicht aktiviert ist, indem der `vserver cifs options modify` Befehl verwendet wird.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Gruppenrichtlinienobjekte (GPOs) auf dem CIFS-Server können aktiviert werden, falls sie noch nicht aktiviert sind, indem der `vserver cifs group-policy modify` Befehl verwendet wird.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Zentrale Zugriffsregeln und zentrale Zugriffsrichtlinien in Active Directory erstellen.
4. Ein Gruppenrichtlinienobjekt (GPO) wird erstellt, um die zentralen Zugriffsrichtlinien auf Active Directory bereitzustellen.
5. Die Gruppenrichtlinie wird auf den Container angewendet, in dem sich das Computerkonto des CIFS-Servers befindet.
6. Die auf den CIFS-Server angewendeten GPOs werden mit dem `vserver cifs group-policy update` Befehl manuell aktualisiert.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Es sollte überprüft werden, ob die zentrale Zugriffsrichtlinie des Gruppenrichtlinienobjekts (GPO) auf die Ressourcen auf dem CIFS-Server angewendet wird, indem der `vserver cifs group-policy show-applied` Befehl verwendet wird.

   Das folgende Beispiel zeigt, dass die Default Domain Policy zwei zentrale Zugriffsrichtlinien enthält, die auf den CIFS-Server angewendet werden:

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
   ```

```
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
```

```
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Verwandte Informationen

- Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln
- DAC für Server aktivieren oder deaktivieren

Informationen zur DAC-Sicherheit für ONTAP SMB-Server

Sie können Informationen zur dynamischen Zugriffssteuerung (DAC) auf NTFS-Volumes und zu Daten mit effektiver NTFS-Sicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen. Dies umfasst Informationen zu bedingten ACEs, Ressourcen-ACEs und zentralen Zugriffsrichtlinien-ACEs. 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.

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`
Wo die Ausgabe mit Gruppen- und Benutzer-SIDs angezeigt wird	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Informationen zur Datei- und Verzeichnissicherheit für Dateien und Verzeichnisse, bei denen die hexadezimale Bitmaske in ein Textformat übersetzt wird	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Beispiele

Das folgende Beispiel zeigt Sicherheitsinformationen zur Dynamic Access Control über den Pfad `/vol1` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
               File Inode Number: 112
                  Security Style: mixed
                 Effective Style: ntfs
                  DOS Attributes: 10
            DOS Attributes in Text: ----D---
            Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
            Unix Mode Bits in Text: rwxrwxrwx
                              ACLs: NTFS Security Descriptor
                                    Control:0xbf14
                                    Owner:CIFS1\Administrator
                                    Group:CIFS1\Domain Admins
                                    SACL - ACEs
                                       ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                       RESOURCE ATTRIBUTE-Everyone-0x0
```

```
("Department_MS",TS,0x10020,"Finance")
                                        POLICY ID-All resources - No Write-
0x0-OI|CI
                                    DACL - ACEs
                                        ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                        ALLOW-Everyone-0x1f01ff-OI|CI
                                        ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Verwandte Informationen

- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln

Überlegungen zum Zurücksetzen von DAC auf ONTAP SMB-Servern

Sie sollten sich darüber im Klaren sein, was passiert, wenn auf eine Version von ONTAP zurückgesetzt wird, die Dynamic Access Control (DAC) nicht unterstützt, und was vor und nach dem Zurücksetzen zu tun ist.

Wenn der Cluster auf eine Version von ONTAP zurückgesetzt werden soll, die Dynamic Access Control nicht unterstützt, und Dynamic Access Control auf einer oder mehreren Storage Virtual Machines (SVMs) aktiviert ist, sind vor dem Zurücksetzen die folgenden Schritte erforderlich:

- Die dynamische Zugriffskontrolle muss auf allen SVMs deaktiviert werden, auf denen sie im Cluster aktiviert ist.
- Sie müssen alle Überwachungskonfigurationen auf dem Cluster, die den `cap-staging` Ereignistyp enthalten, so ändern, dass nur der `file-op` Ereignistyp verwendet wird.

Einige wichtige Überlegungen zum Zurücksetzen von Dateien und Ordnern mit Dynamic Access Control-ACEs sollten verstanden und berücksichtigt werden:

- Wenn der Cluster zurückgesetzt wird, werden bestehende Dynamic Access Control ACEs nicht entfernt; sie werden jedoch bei Dateizugriff-Prüfungen ignoriert.
- Da Dynamic Access Control-ACEs nach der Rücksetzung ignoriert werden, ändert sich der Zugriff auf Dateien mit Dynamic Access Control-ACEs.

  Dies könnte dazu führen, dass Benutzer auf Dateien zugreifen können, auf die sie zuvor keinen Zugriff hatten, oder umgekehrt, dass sie auf Dateien nicht mehr zugreifen können, auf die sie zuvor Zugriff hatten.

- Nicht-dynamische Zugriffskontroll-ACEs sollten auf die betroffenen Dateien angewendet werden, um deren vorheriges Sicherheitsniveau wiederherzustellen.

  Dies kann entweder vor dem Zurücksetzen oder unmittelbar nach Abschluss der Rücksetzung erfolgen.

Da Dynamic Access Control-ACEs nach dem Zurücksetzen ignoriert werden, ist es nicht erforderlich, sie zu entfernen, wenn nicht-Dynamic Access Control-ACEs auf die betroffenen Dateien angewendet werden. Falls gewünscht, können sie manuell entfernt werden.

SMB-Zugriff mithilfe von Exportrichtlinien absichern

Informationen zur Verwendung von Exportrichtlinien mit ONTAP SMB-Zugriff

Wenn auf dem SMB-Server Exportregeln für den SMB-Zugriff aktiviert sind, werden Exportregeln verwendet, um den Zugriff von SMB-Clients auf SVM-Volumes zu steuern. Für den Datenzugriff kann eine Exportregel erstellt werden, die den SMB-Zugriff erlaubt, und anschließend der Richtlinie die Volumes zugeordnet werden, die SMB-Freigaben enthalten.

Für eine Exportregel gilt eine oder mehrere Regeln, die festlegen, welche Clients Zugriff auf die Daten erhalten und welche Authentifizierungsprotokolle für Lese- und Schreibzugriff unterstützt werden. Exportregeln können so konfiguriert werden, dass der Zugriff über SMB für alle Clients, ein Subnetz von Clients oder einen bestimmten Client erlaubt ist und dass die Authentifizierung mittels Kerberos-Authentifizierung, NTLM-Authentifizierung oder sowohl Kerberos- als auch NTLM-Authentifizierung bei der Bestimmung des Lese- und Schreibzugriffs auf Daten zulässig ist.

Nach der Verarbeitung aller auf die Exportregel angewendeten Exportregeln kann ONTAP feststellen, ob dem Client Zugriff gewährt wird und welche Zugriffsebene gewährt wird. Exportregeln gelten für Client-Rechner, nicht für Windows-Benutzer und -Gruppen. Exportregeln ersetzen nicht die Windows-Benutzer- und -gruppenbasierte Authentifizierung und Autorisierung. Exportregeln bieten eine zusätzliche Sicherheitsebene zum Schutz des Zugriffs, zusätzlich zu den Berechtigungen für Freigaben und Dateizugriff.

Jedem Volume wird genau eine Exportregel zugeordnet, um den Clientzugriff auf das Volume zu konfigurieren. Jede SVM kann mehrere Exportregeln enthalten. Dadurch ergeben sich für SVMs mit mehreren Volumes folgende Möglichkeiten:

- Weisen Sie jedem Volume der SVM unterschiedliche Exportrichtlinien zu, um die Zugriffskontrolle für jeden einzelnen Client auf jedes Volume in der SVM zu ermöglichen.
- Dieselbe Exportregel kann mehreren Volumes der SVM zugewiesen werden, sodass eine identische Clientzugriffskontrolle möglich ist, ohne für jedes Volume eine neue Exportregel erstellen zu müssen.

Jede SVM verfügt über mindestens eine Export-Richtlinie namens „`default`“, die keine Regeln enthält. Sie können diese Export-Richtlinie nicht löschen, aber Sie können sie umbenennen oder ändern. Jedes Volume auf der SVM ist standardmäßig der Standard-Export-Richtlinie zugeordnet. Wenn Export-Richtlinien für den SMB-Zugriff auf der SVM deaktiviert sind, hat die Export-Richtlinie „`default`“ keine Auswirkungen auf den SMB-Zugriff.

Es ist möglich, Regeln zu konfigurieren, die sowohl NFS- als auch SMB-Hosts Zugriff gewähren, und diese Regel mit einer Exportregel zu verknüpfen, die anschließend dem Volume zugeordnet werden kann, das Daten enthält, auf die sowohl NFS- als auch SMB-Hosts zugreifen müssen. Alternativ kann für einige Volumes, auf die nur SMB-Clients zugreifen müssen, eine Exportregel mit Regeln konfiguriert werden, die ausschließlich den Zugriff über das SMB-Protokoll erlauben und für die Authentifizierung bei Lese- und Schreibzugriffen ausschließlich Kerberos oder NTLM (oder beides) verwenden. Die Exportregel wird dann den Volumes zugeordnet, bei denen ausschließlich SMB-Zugriff erforderlich ist.

Wenn Exportregeln für SMB aktiviert sind und ein Client eine Zugriffsanfrage stellt, die von der entsprechenden Exportregel nicht zugelassen wird, schlägt die Anfrage mit einer „Zugriff verweigert“-Meldung fehl. Wenn ein

Client keiner Regel in der Exportregel des Volumes entspricht, wird der Zugriff verweigert. Ist eine Exportregel leer, werden alle Zugriffe implizit verweigert. Dies gilt auch dann, wenn die Freigabe- und Dateiberechtigungen den Zugriff ansonsten erlauben würden. Das bedeutet, dass die Exportregel auf Volumes mit SMB-Freigaben mindestens Folgendes zulassen muss:

- Zugriff für alle Clients oder die entsprechende Teilmenge der Clients zulassen
- Zugriff über SMB zulassen
- Angemessener Lese- und Schreibzugriff durch Kerberos- oder NTLM-Authentifizierung (oder beides) möglich

Informationen dazu "Konfiguration und Verwaltung von Exportrichtlinien".

Informationen zu ONTAP SMB Exportregeln

Exportregeln sind die funktionalen Elemente einer Exportregel. Exportregeln gleichen Clientzugriffsanfragen an ein Volume mit spezifischen, von Ihnen konfigurierten Parametern ab, um festzulegen, wie die Clientzugriffsanfragen behandelt werden.

Eine Exportregel muss mindestens in einer Exportregel enthalten sein, damit Clients Zugriff erhalten. Wenn eine Exportregel mehr als eine Regel enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportregel erscheinen. Die Reihenfolge der Regeln wird durch die Regelindexnummer bestimmt. Wenn eine Regel auf einen Client zutrifft, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Wenn keine Regel zutrifft, wird dem Client der Zugriff verweigert.

Exportregeln können so konfiguriert werden, dass die Clientzugriffsberechtigungen anhand der folgenden Kriterien bestimmt werden:

- Das vom Client, der die Anfrage sendet, verwendete Protokoll für den Dateizugriff, beispielsweise NFSv4 oder SMB.
- Eine Client-Kennung, zum Beispiel Hostname oder IP-Adresse.

  Die maximale Größe des `-clientmatch` Feldes beträgt 4096 Zeichen.

- Der vom Client zur Authentifizierung verwendete Sicherheitstyp, beispielsweise Kerberos v5, NTLM oder AUTH_SYS.

Wenn eine Regel mehrere Kriterien festlegt, muss der Client alle erfüllen, damit die Regel Anwendung findet.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Clientzugriffsanfrage wird mit dem NFSv3-Protokoll gesendet und der Client hat die IP-Adresse 10.1.17.37.

Obwohl das Client-Zugriffsprotokoll übereinstimmt, befindet sich die IP-Adresse des Clients in einem anderen Subnetz als dem in der Exportregel angegebenen. Daher schlägt die Clientzuordnung fehl und diese Regel gilt

für diesen Client nicht.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Clientzugriffsanfrage wird mit dem NFSv4-Protokoll gesendet und der Client hat die IP-Adresse 10.1.16.54.

Das Protokoll für den Dateizugriff stimmt überein und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientübereinstimmung erfolgreich und diese Regel gilt für diesen Client. Der Client erhält unabhängig von seinem Sicherheitstyp lesen/schreiben-Zugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 hat die IP-Adresse 10.1.16.207, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und hat sich mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und hat sich mit AUTH_SYS authentifiziert.

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der Parameter „Schreibgeschützt“ ermöglicht allen Clients Lesezugriff, unabhängig vom Sicherheitstyp, mit dem sie sich authentifiziert haben. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese- und Schreibzugriff, da er sich mit dem genehmigten Sicherheitstyp Kerberos v5 authentifiziert hat. Client #2 erhält keinen Lese- und Schreibzugriff.

Beispiele für ONTAP Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen

Die Beispiele zeigen, wie Exportrichtlinienregeln erstellt werden, die den Zugriff über SMB auf einer SVM einschränken oder zulassen, auf der Exportrichtlinien für SMB-Zugriff aktiviert sind.

Exportrichtlinien für den SMB-Zugriff sind standardmäßig deaktiviert. Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen, sind nur zu konfigurieren, wenn Exportrichtlinien für den SMB-Zugriff aktiviert wurden.

Exportregel nur für SMB-Zugriff

Der folgende Befehl erstellt eine Exportregel auf der SVM mit dem Namen “vs1”, die die folgende Konfiguration aufweist:

- Richtlinienname: cifs1
- Indexnummer: 1
- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: Ermöglicht nur SMB-Zugriff
- Schreibgeschützter Zugriff: Für Clients mit NTLM- oder Kerberos-Authentifizierung
- Lese- und Schreibzugriff: Für Clients mit Kerberos-Authentifizierung

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Exportregel für SMB- und NFS-Zugriff

Der folgende Befehl erstellt eine Exportregel auf der SVM namens "vs1", die die folgende Konfiguration aufweist:

- Richtlinienname: cifsnfs1
- Indexnummer: 2
- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: SMB und NFS-Zugriff
- Nur-Lese-Zugriff: Für alle Clients
- Lese- und Schreibzugriff: Für Clients, die Kerberos (NFS und SMB) oder NTLM-Authentifizierung (SMB) verwenden
- Zuordnung für UNIX-Benutzer-ID 0 (Null): Zuordnung zur Benutzer-ID 65534 (die typischerweise dem Benutzernamen nobody zugeordnet ist)
- SUID- und SGID-Zugriff: Ermöglicht

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch
192.168.1.0/255.255.255.0 -rorule any -rwrule krb5,ntlm -anon 65534 -allow
-suid true
```

Exportregel für SMB-Zugriff ausschließlich über NTLM

Der folgende Befehl erstellt eine Exportregel auf der SVM mit dem Namen “vs1”, die die folgende Konfiguration aufweist:

- Richtlinienname: ntlm1
- Indexnummer: 1

- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: Ermöglicht nur SMB-Zugriff
- Schreibgeschützter Zugriff: Nur für Clients, die NTLM verwenden
- Lese- und Schreibzugriff: Nur für Clients, die NTLM verwenden

> Wenn Sie die Option „Nur lesen“ oder „Lesen/Schreiben“ für den NTLM-only-Zugriff konfigurieren, müssen Sie IP-adressbasierte Einträge in der Client-Match-Option verwenden. Andernfalls erhalten Sie `access denied` Fehler. Dies ist darauf zurückzuführen, dass ONTAP bei Verwendung eines Hostnamens zur Überprüfung der Zugriffsrechte des Clients Kerberos Service Principal Names (SPN) verwendet. NTLM-Authentifizierung unterstützt keine SPN-Namen.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule ntlm -rwrule ntlm
```

ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren

Sie können Exportrichtlinien für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Die Verwendung von Exportrichtlinien zur Steuerung des SMB-Zugriffs auf Ressourcen ist optional.

Bevor Sie beginnen

Die folgenden Voraussetzungen gelten für die Aktivierung von Exportrichtlinien für SMB:

- Der Client muss über einen "PTR"-Eintrag im DNS verfügen, bevor die Exportregeln für diesen Client erstellt werden.
- Ein zusätzlicher Satz von „A“- und „PTR“-Einträgen für Hostnamen ist erforderlich, wenn die SVM Zugriff auf NFS-Clients bereitstellt und der Hostname, der für den NFS-Zugriff verwendet werden soll, sich vom CIFS-Servernamen unterscheidet.

Über diese Aufgabe

Beim Einrichten eines neuen CIFS-Servers auf Ihrer SVM ist die Verwendung von Exportrichtlinien für den SMB-Zugriff standardmäßig deaktiviert. Exportrichtlinien für den SMB-Zugriff können aktiviert werden, wenn der Zugriff basierend auf Authentifizierungsprotokoll, Client-IP-Adressen oder Hostnamen gesteuert werden soll. Exportrichtlinien für den SMB-Zugriff können jederzeit aktiviert oder deaktiviert werden.

> Durch die Aktivierung von Exportrichtlinien für CIFS/SMB in einer NFS-fähigen SVM kann ein Linux-Client den `showmount -e` Befehl auf der SVM verwenden, um die Verbindungspfade aller SMB-Volumes mit zugehörigen Exportrichtlinienregeln anzuzeigen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Exportrichtlinien aktivieren oder deaktivieren:
   - Exportrichtlinien aktivieren: `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`

- Exportrichtlinien deaktivieren: `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled false`

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

Beispiel

Das folgende Beispiel ermöglicht die Verwendung von Exportrichtlinien zur Steuerung des SMB-Clientzugriffs auf Ressourcen 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-exportpolicy
-enabled true

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

Die SMB-Exportregel des ONTAP SVM-Root-Volumes öffnen

Wenn Sie SMB-Exportrichtlinienregeln aktiviert haben, muss die Standardexportrichtlinie des SVM-Root-Volumes eine Regel enthalten, die allen Clients offenen Zugriff über SMB erlaubt. Ohne eine solche Regel wird allen SMB-Clients der Zugriff auf die SVM und ihre Volumes verweigert. Exportrichtlinienregeln sind standardmäßig deaktiviert.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine Standard-Exportregel (genannt default) für das Root-Volume der SVM erstellt. Es müssen eine oder mehrere Regeln für die Standard-Exportregel erstellt werden, bevor Clients auf Daten auf der SVM zugreifen können.

Es empfiehlt sich zu überprüfen, ob der gesamte SMB-Zugriff in der Standard-Exportregel offen ist, und den Zugriff auf einzelne Volumes später durch das Erstellen benutzerdefinierter Exportregeln für einzelne Volumes oder qtrees einzuschränken.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, überprüfen Sie die Standard-Exportregel für das Root-Volume: `vserver export-policy rule show`

   Die Ausgabe des Befehls sollte in etwa wie folgt aussehen:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                Vserver: vs1.example.com
                            Policy Name: default
                             Rule Index: 1
                        Access Protocol: cifs
```

```
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                            RO Access Rule: any
                            RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: any
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Existiert eine solche Regel, die offenen Zugang erlaubt, ist diese Aufgabe abgeschlossen. Falls nicht, folgt der nächste Schritt.

2. Eine Exportregel für das SVM-Root-Volume erstellen: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Die Regelerstellung kann mithilfe des `vserver export-policy rule show` Befehls überprüft werden.

Ergebnisse

Jeder SMB-Client kann nun auf jedes Volume oder jeden Qtree zugreifen, der auf der SVM erstellt wurde.

Verwandte Informationen

"Erfahren Sie, wie Sie ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren".

Sicherer Dateizugriff mit Storage Level Access Guard

Informationen zum sicheren ONTAP SMB Dateizugriff mit Storage-Level Access Guard

Zusätzlich zur Sicherung des Zugriffs durch native Dateisicherheits- sowie Export- und Freigabesicherheitsmechanismen kann Storage-Level Access Guard konfiguriert werden, eine dritte Sicherheitsebene, die von ONTAP auf Volume-Ebene angewendet wird. Storage-Level Access Guard gilt für den Zugriff aus allen NAS-Protokollen auf das Speicherobjekt, auf das sie angewendet wird.

Es werden ausschließlich NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP Sicherheitsprüfungen für UNIX-Benutzer beim Zugriff auf Daten auf Volumes durchführen kann, für die Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM zugeordnet sein, der das Volume besitzt.

Verhalten des Storage-Level Access Guard

- Storage-Level Access Guard gilt für alle Dateien oder alle Verzeichnisse in einem Storage-Objekt.

  Da alle Dateien oder Verzeichnisse in einem Volume den Einstellungen des Storage-Level Access Guard unterliegen, ist eine Vererbung durch Weitergabe nicht erforderlich.

- Storage-Level Access Guard kann so konfiguriert werden, dass es nur für Dateien, nur für Verzeichnisse oder sowohl für Dateien als auch für Verzeichnisse innerhalb eines Volumes gilt.
  - Datei- und Verzeichnissicherheit

Gilt für jedes Verzeichnis und jede Datei innerhalb des Speicherobjekts. Dies ist die Standardeinstellung.

- Dateisicherheit

  Gilt für jede Datei innerhalb des Speicherobjekts. Die Anwendung dieser Sicherheitsmaßnahme wirkt sich nicht auf den Zugriff auf oder die Überwachung von Verzeichnissen aus.

- Verzeichnissicherheit

  Gilt für jedes Verzeichnis innerhalb des Speicherobjekts. Die Anwendung dieser Sicherheitsmaßnahme wirkt sich nicht auf den Zugriff auf oder die Überwachung von Dateien aus.

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

  Es gibt niemals zusätzliche Zugriffsrechte.

- Wenn die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus angezeigt werden, ist die Storage-Level Access Guard Sicherheit nicht sichtbar.

  Sie wird auf Ebene des Speicherobjekts angewendet und in den Metadaten gespeichert, die zur Bestimmung der effektiven Berechtigungen verwendet werden.

- Die Sicherheit auf Storage-Ebene kann einem Client nicht entzogen werden, auch nicht von einem Systemadministrator (Windows oder UNIX).

  Es ist so konzipiert, dass es nur von Speicheradministratoren geändert werden kann.

- Sie können Storage-Level Access Guard auf Volumes mit NTFS- oder gemischtem Sicherheitsstil anwenden.
- Sie können Storage-Level Access Guard auf Volumes mit UNIX-Sicherheitsstil anwenden, sofern auf der SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist.
- Wenn Volumes unter einem Volume Verbindungspfad gemountet werden und Storage-Level Access Guard auf diesem Pfad vorhanden ist, wird es nicht auf die darunter gemounteten Volumes übertragen.
- Der Storage-Level Access Guard Sicherheitsdeskriptor wird mit SnapMirror Datenreplizierung und mit SVM-Replikation repliziert.
- Für Virenscanner gelten Sonderregelungen.

  Diesen Servern wird ein Ausnahmezugriff zum Durchsuchen von Dateien und Verzeichnissen gewährt, selbst wenn Storage-Level Access Guard den Zugriff auf das Objekt verweigert.

- FPolicy-Benachrichtigungen werden nicht gesendet, wenn der Zugriff aufgrund von Storage-Level Access Guard verweigert wird.

Reihenfolge der Zugriffskontrollen

Der Zugriff auf eine Datei oder ein Verzeichnis wird durch die kombinierte Wirkung der Export- oder Freigabeberechtigungen, der auf Volumes festgelegten Storage-Level Access Guard-Berechtigungen und der nativ auf Dateien und/oder Verzeichnisse angewendeten Dateiberechtigungen bestimmt. Alle Sicherheitsebenen werden ausgewertet, um zu bestimmen, welche effektiven Berechtigungen eine Datei oder ein Verzeichnis hat. Die Sicherheitszugriffsprüfungen erfolgen in folgender Reihenfolge:

1. SMB-Freigabe- oder NFS-Export-Berechtigungen

2. Zugriffsschutz auf Storage-Ebene
3. NTFS-Datei-/Ordnerzugriffskontrolllisten (ACLs), NFSv4-ACLs oder UNIX-Modusbits

Anwendungsfälle für den Einsatz von Storage-Level Access Guard

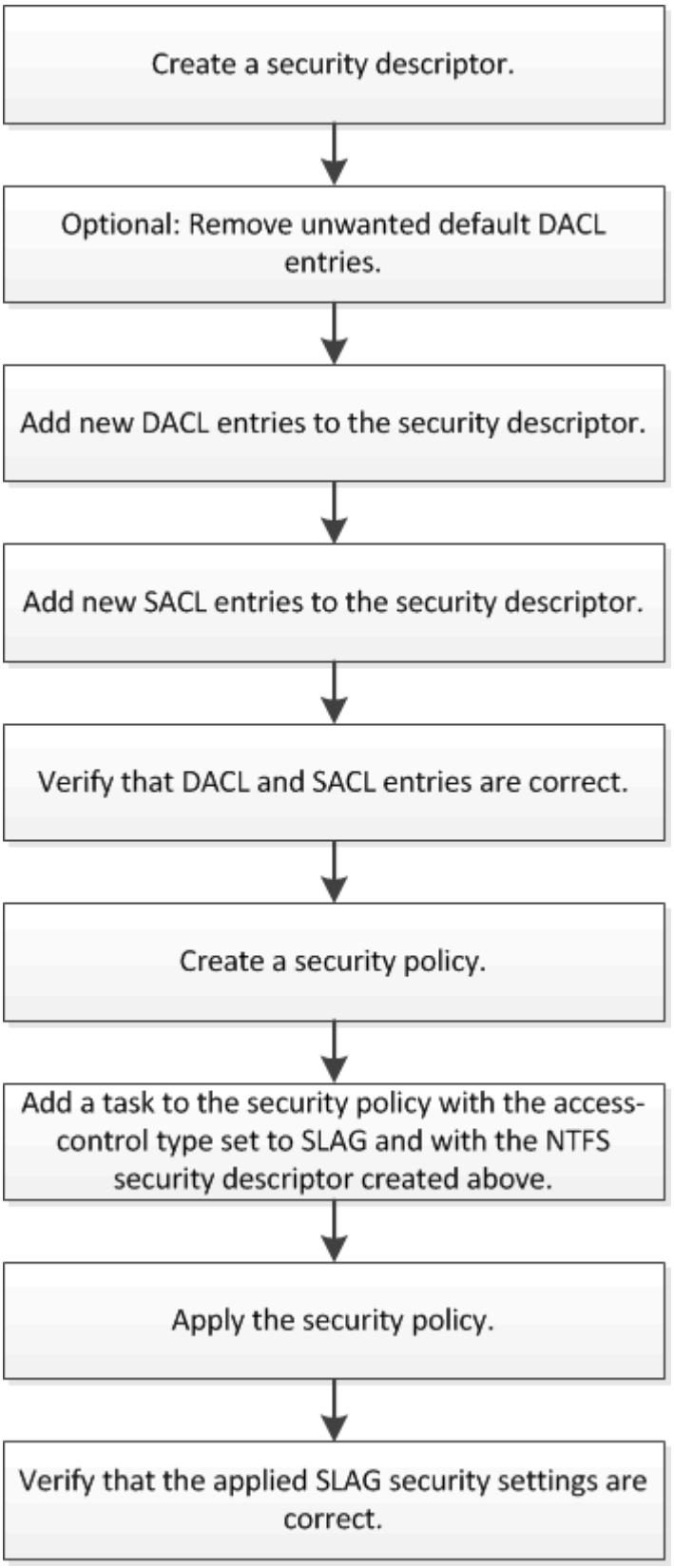
Storage-Level Access Guard bietet zusätzliche Sicherheit auf Speicherebene, die für Clients nicht sichtbar ist, daher kann sie weder von Benutzern noch von Administratoren von ihren Desktops aus aufgehoben werden. In bestimmten Anwendungsfällen ist die Möglichkeit, den Zugriff auf Speicherebene zu steuern, von Vorteil.

Typische Anwendungsfälle für diese Funktion umfassen die folgenden Szenarien:

- Schutz des geistigen Eigentums durch Prüfung und Kontrolle aller Benutzerzugriffe auf Speicherebene
- Storage für Finanzdienstleistungsunternehmen, einschließlich Banken und Handelsgruppen
- Regierungsdienste mit separatem Dateispeicher für einzelne Abteilungen
- Universitäten schützen alle Studentendateien

Konfigurationsworkflow für Storage-Level Access Guard auf ONTAP SMB Servern

Der Workflow zur Konfiguration von Storage-Level Access Guard (SLAG) verwendet dieselben ONTAP CLI-Befehle wie die Konfiguration von NTFS-Dateiberechtigungen und Überwachungsrichtlinien. Statt den Datei- und Verzeichniszugriff auf einem bestimmten Ziel zu konfigurieren, wird SLAG auf dem entsprechenden Volume der Storage Virtual Machine (SVM) konfiguriert.



Verwandte Informationen

Storage Level Access Guard auf Servern konfigurieren

Storage-Level Access Guard auf ONTAP SMB-Servern konfigurieren

Es sind mehrere Schritte erforderlich, um Storage-Level Access Guard auf einem Volume oder Qtree zu konfigurieren. Storage-Level Access Guard bietet eine Zugriffssicherheit, die auf Speicherebene festgelegt wird. Sie bietet eine Sicherheit, die für alle Zugriffe aller NAS-Protokolle auf das Speicherobjekt gilt, auf das sie angewendet wurde.

Schritte

1. Ein Sicherheitsdeskriptor wird mithilfe des `vserver security file-directory ntfs create` Befehls erstellt.

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

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Ein Sicherheitsdeskriptor wird mit den folgenden vier Standard-DACL-Zugriffskontrolleinträgen (ACEs) erstellt:

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Wenn Sie bei der Konfiguration von Storage-Level Access Guard nicht die Standardeinträge verwenden möchten, können Sie diese entfernen, bevor Sie eigene ACEs erstellen und dem Sicherheitsdeskriptor hinzufügen.

2. Entfernen Sie alle standardmäßigen DACL-ACEs aus dem Sicherheitsdeskriptor, die nicht mit Storage-

Level Access Guard Sicherheit konfiguriert werden sollen:

a. Unerwünschte DACL-ACEs lassen sich mit dem `vserver security file-directory ntfs dacl remove` Befehl entfernen.

   In diesem Beispiel werden drei Standard-DACL-ACEs aus dem Sicherheitsdeskriptor entfernt: BUILTIN\Administrators, BUILTIN\Users und CREATOR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Es sollte überprüft werden, dass die DACL-ACEs, die nicht für die Storage-Level Access Guard Sicherheit verwendet werden sollen, mithilfe des `vserver security file-directory ntfs dacl show` Befehls aus dem Sicherheitsdeskriptor entfernt wurden.

   In diesem Beispiel bestätigt die Ausgabe des Befehls, dass drei Standard-DACL-ACEs aus dem Sicherheitsdeskriptor entfernt wurden, sodass nur noch der NT AUTHORITY\SYSTEM Standard-DACL-ACE-Eintrag übrig bleibt:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Einem Sicherheitsdeskriptor können mit dem `vserver security file-directory ntfs dacl add` Befehl ein oder mehrere DACL-Einträge hinzugefügt werden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei DACL-ACEs hinzugefügt:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Einem Sicherheitsdeskriptor können mit dem `vserver security file-directory ntfs sacl add` Befehl ein oder mehrere SACL-Einträge hinzugefügt werden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei SACL-ACEs hinzugefügt:

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   ```

```
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Es sollte überprüft werden, ob die DACL- und SACL-ACEs mithilfe der `vserver security file-directory ntfs dacl show`- und `vserver security file-directory ntfs sacl show` -Befehle jeweils korrekt konfiguriert sind.

   In diesem Beispiel zeigt der folgende Befehl Informationen über DACL-Einträge für den Sicherheitsdeskriptor “sd1” an:

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

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   In diesem Beispiel zeigt der folgende Befehl Informationen über SACL-Einträge für den Sicherheitsdeskriptor “sd1” an:

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

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        failure  read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        success  full-control   this-folder, sub-folders,
   ```

```
files
```

6. Eine Sicherheitsrichtlinie kann mithilfe des `vserver security file-directory policy create` Befehls erstellt werden.

   Das folgende Beispiel erstellt eine Richtlinie mit dem Namen “policy1”:

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

7. Es kann mithilfe des `vserver security file-directory policy show` Befehls überprüft werden, ob die Richtlinie korrekt konfiguriert ist.

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

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. Eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor wird zur Sicherheitsrichtlinie hinzugefügt, indem der `vserver security file-directory policy task add` Befehl mit dem `-access -control` Parameter, der auf `slag` gesetzt ist, verwendet wird.

   Eine Richtlinie kann zwar mehrere Storage-Level Access Guard Aufgaben enthalten, jedoch ist es nicht möglich, eine Richtlinie so zu konfigurieren, dass sie sowohl Datei-Verzeichnis- als auch Storage-Level Access Guard Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

   In diesem Beispiel wird der Richtlinie mit dem Namen „policy1“ eine Aufgabe hinzugefügt, die dem Sicherheitsdeskriptor „sd1“ zugewiesen ist. Sie ist dem `/datavol1` Pfad mit dem Zugriffskontrolltyp „slag“ zugeordnet.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Es kann überprüft werden, ob die Aufgabe korrekt konfiguriert ist, indem der `vserver security file-directory policy task show` Befehl verwendet wird.

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

   ```
    Vserver: vs1
     Policy: policy1

      Index  File/Folder  Access           Security  NTFS       NTFS
   Security
             Path         Control          Type      Mode       Descriptor
   Name
   ```

```
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Die Sicherheitsrichtlinie „Storage-Level Access Guard“ wird mithilfe des `vserver security file-directory apply` Befehls angewendet.

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

    Der Auftrag zur Anwendung der Sicherheitsrichtlinie ist terminiert.

11. Es kann mithilfe des `vserver security file-directory show` Befehls überprüft werden, ob die angewendeten Storage-Level Access Guard Sicherheitseinstellungen korrekt sind.

    In diesem Beispiel zeigt die Ausgabe des Befehls, dass die Storage-Level Access Guard-Sicherheit auf das NTFS-Volume angewendet wurde `/datavol1`. Auch wenn die standardmäßige DACL, die Vollzugriff für Everyone erlaubt, weiterhin besteht, beschränkt und protokolliert die Storage-Level Access Guard-Sicherheit den Zugriff auf die in den Storage-Level Access Guard-Einstellungen definierten Gruppen.

    `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

- Befehle zur Verwaltung der NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und des Storage-Level Access Guard
- Konfigurationsworkflow für Storage-Level Access Guard auf Servern
- Informationen zu Storage-Level Access Guard auf Servern
- Storage-Level Access Guard auf Servern entfernen

Effektive SLAG-Matrix auf ONTAP SMB Servern

Sie können SLAG auf einem Volume, einem Qtree oder beiden konfigurieren. Die SLAG-Matrix definiert, auf welchem Volume oder Qtree die SLAG-Konfiguration in den verschiedenen, in der Tabelle aufgeführten Szenarien anwendbar ist.

	Volume SLAG in einem AFS	Volume SLAG in einer Snapshot	Qtree SLAG in einem AFS	Qtree SLAG in einem Snapshot
Volume-Zugriff in einem Access File System (AFS)	JA	NEIN	k. A.	k. A.
Volumenzugriff in einer Snapshot	JA	NEIN	k. A.	k. A.
Qtree-Zugriff in einem AFS (wenn SLAG im Qtree vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in einem AFS (wenn SLAG nicht im Qtree vorhanden ist)	JA	NEIN	NEIN	NEIN
Qtree-Zugriff in einem Snapshot (wenn SLAG im Qtree-AFS vorhanden ist)	NEIN	NEIN	JA	NEIN

	Volume SLAG in einem AFS	Volume SLAG in einer Snapshot	Qtree SLAG in einem AFS	Qtree SLAG in einem Snapshot
Qtree-Zugriff in einem Snapshot (wenn SLAG im Qtree-AFS nicht vorhanden ist)	JA	NEIN	NEIN	NEIN

Informationen zu Storage-Level Access Guard auf ONTAP SMB-Servern

Storage-Level Access Guard ist eine dritte Sicherheitsebene, die auf ein Volume oder einen Qtree angewendet wird. Storage-Level Access Guard-Einstellungen können nicht über das Windows-Eigenschaftenfenster angezeigt werden. Zur Anzeige von Informationen zur Storage-Level Access Guard-Sicherheit, die zur Validierung der Konfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden können, ist die ONTAP CLI zu nutzen.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zum Volume oder Qtree angeben, dessen Storage-Level Access Guard Sicherheitsinformationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

Schritt

1. Storage-Level Access Guard-Sicherheitseinstellungen 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 Storage-Level Access Guard-Sicherheitsinformationen für das NTFS-Sicherheitsvolume 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
```

Das folgende Beispiel zeigt die Storage-Level Access Guard-Informationen zum Volume mit gemischtem Sicherheitsstil am Pfad `/datavol5` in SVM vs1. Die oberste Ebene dieses Volumes hat 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
                        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
```

Storage-Level Access Guard auf ONTAP SMB-Servern entfernen

Sie können den Storage-Level Access Guard für ein Volume oder einen Qtree entfernen, wenn Sie die Zugriffssicherheit nicht mehr auf Storage-Level festlegen möchten. Das Entfernen des Storage-Level Access Guard ändert oder entfernt die reguläre NTFS-Datei- und Verzeichnissicherheit nicht.

Schritte

1. Es kann mithilfe des `vserver security file-directory show` Befehls überprüft werden, ob für das Volume oder den Qtree Storage-Level Access Guard konfiguriert ist.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

   ```
                    Vserver: vs1
                  File Path: /datavol2
          File Inode Number: 99
             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:0xbf14
                             Owner:BUILTIN\Administrators
   ```

```
                          Group:BUILTIN\Administrators
                          SACL - ACEs
                            AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                          DACL - ACEs
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                            ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                          Storage-Level Access Guard security
                          DACL (Applies to Directories):
                            ALLOW-BUILTIN\Administrators-0x1f01ff
                            ALLOW-CREATOR OWNER-0x1f01ff
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                          DACL (Applies to Files):
                            ALLOW-BUILTIN\Administrators-0x1f01ff
                            ALLOW-CREATOR OWNER-0x1f01ff
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Storage-Level Access Guard kann mit dem `vserver security file-directory remove-slag` Befehl entfernt werden.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Es kann mit dem `vserver security file-directory show` Befehl überprüft werden, ob Storage-Level Access Guard vom Volume oder Qtree entfernt wurde.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         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:0xbf14
                         Owner:BUILTIN\Administrators
```

```
                          Group:BUILTIN\Administrators
                          SACL - ACEs
                            AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                          DACL - ACEs
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                            ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

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.