Richten Sie den Dateizugriff über SMB ein

ONTAP 9

NetApp
May 09, 2024

Inhalt

Richten Sie den Dateizugriff über SMB ein

Konfigurieren Sie Sicherheitsstile

Einfluss der Sicherheitsstile auf den Datenzugriff

Was die Sicherheitsstile und ihre Auswirkungen sind

Es gibt vier verschiedene Sicherheitsarten: UNIX, NTFS, gemischt und vereinheitlicht. Jeder Sicherheitsstil hat unterschiedliche Auswirkungen auf den Umgang mit Berechtigungen für Daten. Sie müssen die verschiedenen Effekte verstehen, um sicherzustellen, dass Sie den entsprechenden Sicherheitsstil für Ihre Zwecke auswählen.

Es ist wichtig zu verstehen, dass Sicherheitsstile nicht bestimmen, welche Client-Typen auf Daten zugreifen können oder nicht. Sicherheitsstile bestimmen nur die Art der Berechtigungen, die ONTAP zur Kontrolle des Datenzugriffs verwendet, und welche Clienttypen diese Berechtigungen ändern können.

Wenn ein Volume beispielsweise UNIX-Sicherheitsstil verwendet, können SMB-Clients aufgrund der Multiprotokollart von ONTAP weiterhin auf Daten zugreifen (sofern sie sich ordnungsgemäß authentifizieren und autorisieren). 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	Dadurch effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
UNIX	NFS	Bits im NFSv3 Modus	UNIX	NFS und SMB
NFSv4.x ACLs	UNIX	NTFS	SMB	NTFS-ACLs
NTFS	Gemischt	NFS oder SMB	Bits im NFSv3 Modus	UNIX
NFSv4.x ACLs	UNIX	NTFS-ACLs	NTFS	Virtualisierung
NFS oder SMB	Bits im NFSv3 Modus	UNIX	NFSv4.1 ACLs	UNIX
NTFS-ACLs	NTFS	Unified (nur für Infinite Volumes, in ONTAP 9.4 und älteren Versionen.)	NFS oder SMB	Bits im NFSv3 Modus
Unix	NFSv4.1 ACLs			NTFS-ACLs

FlexVol Volumes unterstützen UNIX, NTFS und verschiedene Sicherheitsstile. Wenn der Sicherheitsstil gemischt oder vereinheitlicht ist, hängen die effektiven Berechtigungen vom Clienttyp ab, der die Berechtigungen zuletzt geändert hat, da Benutzer den Sicherheitsstil auf individueller Basis festlegen. Wenn der letzte Client, der die Berechtigungen geändert hat, ein NFSv3-Client war, sind die Berechtigungen UNIX NFSv3-Modus-Bits. 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 Unified Security-Stil ist nur mit Infinite Volumes verfügbar, die in ONTAP 9.5 und neueren Versionen nicht mehr unterstützt werden. Weitere Informationen finden Sie unter "Das Management von FlexGroup Volumes – Überblick".

Ab ONTAP 9.2 beginnt der `show-effective-permissions` Parameter für das `vserver security file-directory` Mit Befehl können Sie effektive Berechtigungen anzeigen, die einem Windows- oder UNIX-Benutzer im angegebenen Datei- oder Ordnerpfad gewährt werden. Darüber hinaus der optionale Parameter `-share-name` Ermöglicht Ihnen die Anzeige der effektiven Freigabeberechtigung.

> ONTAP legt zunächst einige Standarddateiberechtigungen fest. Standardmäßig ist der effektive Sicherheitsstil auf allen Daten in UNIX-, gemischten und Unified Security-Volumes UNIX und der effektive Berechtigungstyp UNIX Mode Bits (0755, sofern nicht anders angegeben), bis er von einem Client gemäß dem Standardsicherheitsstil konfiguriert wird. Standardmäßig ist der effektive Sicherheitsstil auf allen Daten in NTFS-Sicherheitsstil-Volumes NTFS und hat eine ACL, die allen die vollständige Kontrolle erlaubt.

Wo und wann Sicherheitsstile eingestellt werden sollen

Sicherheitsstile können auf FlexVol Volumes (Root-Volumes oder Daten-Volumes) und qtrees festgelegt werden. Sicherheitsstile können zum Zeitpunkt der Erstellung manuell eingestellt, automatisch geerbt oder zu einem späteren Zeitpunkt geändert werden.

Entscheiden Sie, welchen Sicherheitsstil auf SVMs verwendet werden soll

Um zu entscheiden, welchen Sicherheitsstil auf einem Volume verwendet werden soll, sollten Sie zwei Faktoren berücksichtigen. Der Hauptfaktor ist die Art des Administrators, der das Dateisystem verwaltet. Sekundär ist die Art des Benutzers oder Service, der auf die Daten des Volume zugreift.

Wenn Sie den Sicherheitsstil auf einem Volume konfigurieren, sollten Sie die Anforderungen Ihrer Umgebung berücksichtigen, um sicherzustellen, dass Sie den besten Sicherheitsstil wählen und Probleme beim Management von Berechtigungen vermeiden. Die folgenden Überlegungen helfen Ihnen bei der Auswahl:

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

Sicherheitsstil	Wählen Sie aus, ob…
Gemischt	Das Filesystem wird sowohl von UNIX- als auch von Windows-Administratoren gemanagt, und die Benutzer bestehen sowohl aus NFS- als auch SMB-Clients.

Wie funktioniert die Vererbung des Sicherheitsstils

Wenn Sie beim Erstellen eines neuen FlexVol Volumes oder eines qtree nicht den Sicherheitsstil festlegen, übernimmt dieser seinen Sicherheitsstil auf unterschiedliche Weise.

Sicherheitsstile werden auf folgende Weise vererbt:

- Ein FlexVol Volume erbt den Sicherheitsstil des Root-Volumes seiner enthaltenen SVM.
- Ein qtree übernimmt den Sicherheitsstil seines enthaltenen FlexVol Volume.
- Eine Datei oder ein Verzeichnis erbt den Sicherheitsstil, den sie FlexVol Volume oder qtree enthält.

Wie ONTAP UNIX-Berechtigungen bewahrt

Wenn Dateien in einem FlexVol-Volume mit derzeit UNIX-Berechtigungen von Windows-Anwendungen bearbeitet und gespeichert werden, kann ONTAP die UNIX-Berechtigungen beibehalten.

Wenn Anwendungen auf Windows-Clients Dateien bearbeiten und speichern, lesen sie die Sicherheitseinstellungen der Datei, erstellen eine neue temporäre Datei, wenden diese Eigenschaften auf die temporäre Datei an und geben der temporären Datei dann den ursprünglichen Dateinamen an.

Wenn Windows-Clients eine Abfrage für die Sicherheitseigenschaften durchführen, erhalten sie eine konstruierte ACL, die genau die UNIX-Berechtigungen repräsentiert. Der einzige Zweck dieser aufgebauten ACL besteht darin, die UNIX-Berechtigungen der Datei beizubehalten, da Dateien von Windows-Anwendungen aktualisiert werden, um sicherzustellen, dass die resultierenden Dateien dieselben UNIX-Berechtigungen haben. ONTAP legt keine NTFS-ACLs mithilfe der konstruierten ACL fest.

Verwalten Sie UNIX-Berechtigungen über die Registerkarte Windows-Sicherheit

Wenn Sie UNIX-Berechtigungen von Dateien oder Ordnern in gemischten Volumes oder qtrees auf SVMs manipulieren möchten, können Sie auf Windows-Clients die Registerkarte „Sicherheit“ verwenden. Alternativ können Sie Anwendungen verwenden, die Windows ACLs abfragen und festlegen können.

- Ändern der UNIX-Berechtigungen

  Mithilfe der Registerkarte Windows Security können Sie UNIX Berechtigungen für ein Volume oder einen qtree im gemischten Sicherheitsstil anzeigen und ändern. Wenn Sie die Windows-Hauptregisterkarte verwenden, um UNIX-Berechtigungen zu ändern, müssen Sie zuerst den vorhandenen ACE entfernen, den Sie bearbeiten möchten (dadurch werden die Modusbits auf 0 gesetzt), bevor Sie Ihre Änderungen vornehmen. Alternativ können Sie den erweiterten Editor verwenden, um Berechtigungen zu ändern.

  Bei Verwendung von Modusberechtigungen können Sie die Modusberechtigungen für die angegebene

UID, GID und andere (alle anderen mit einem Konto auf dem Computer) direkt ändern. Wenn die angezeigte UID beispielsweise r-x-Berechtigungen hat, können Sie die UID-Berechtigungen in rwx ändern.

- Ändern der UNIX-Berechtigungen in NTFS-Berechtigungen

  Sie können die Registerkarte Windows Security verwenden, um UNIX Sicherheitsobjekte durch Windows-Sicherheitsobjekte auf einem Volume mit gemischtem Sicherheitsstil oder qtree zu ersetzen, wobei die Dateien und Ordner einen effektiven UNIX-Sicherheitsstil haben.

  Sie müssen zuerst alle aufgeführten UNIX-Berechtigungseinträge entfernen, bevor Sie sie durch die gewünschten Windows-Benutzer- und Gruppenobjekte ersetzen können. Anschließend können Sie NTFS-basierte ACLs auf den Windows-Benutzerobjekten konfigurieren. Indem Sie alle UNIX-Sicherheitsobjekte entfernen und nur Windows-Benutzer und -Gruppen zu einer Datei oder einem Ordner in einem gemischten Volume oder qtree hinzufügen, ändern Sie den effektiven Sicherheitsstil auf der Datei oder dem Ordner von UNIX auf NTFS.

  Wenn Sie die Berechtigungen für einen Ordner ändern, ist das Windows-Standardverhalten, diese Änderungen auf alle Unterordner und Dateien zu übertragen. Daher müssen Sie die Ausbreitungsmöglichkeit auf die gewünschte Einstellung ändern, wenn Sie keine Änderung des Sicherheitsstils auf alle untergeordneten Ordner, Unterordner und Dateien übertragen möchten.

Sicherheitsstile für SVM-Root-Volumes konfigurieren

Sie konfigurieren den Sicherheitsstil des Root-Volumes der Storage Virtual Machine (SVM), um die Art der Berechtigungen zu ermitteln, die für Daten im Root-Volume der SVM verwendet werden.

Schritte

1. Verwenden Sie die `vserver create` Befehl mit dem `-rootvolume-security-style` Parameter zum Definieren des Sicherheitsstils.

   Mögliche Optionen für die Sicherheit im Root-Volume sind `unix`, `ntfs`, Oder `mixed`.

2. Anzeigen und Überprüfen der Konfiguration, einschließlich des Root-Volume-Sicherheitsstils der erstellten SVM: `vserver show -vserver` *`vserver_name`*

Konfigurieren Sie Sicherheitsstile auf FlexVol Volumes

Sie konfigurieren den Sicherheitsstil des FlexVol Volume, um die Art der Berechtigungen zu bestimmen, die für Daten in 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…
Ist noch nicht vorhanden	`volume create` Und nehmen Sie die auf `-security-style` Parameter, um den Sicherheitsstil anzugeben.

Ist bereits vorhanden	`volume modify` Und nehmen Sie die auf `-security-style` Parameter, um den Sicherheitsstil anzugeben.

Mögliche Optionen für den FlexVol Volume Security Stil sind `unix`, `ntfs`, Oder `mixed`.

Wenn Sie beim Erstellen eines FlexVol-Volumes keinen Sicherheitsstil festlegen, erbt das Volume den Sicherheitsstil des Root-Volumes.

Weitere Informationen zum `volume create` Oder `volume modify` Befehle, siehe "Logisches Storage-Management".

2. Um die Konfiguration anzuzeigen, einschließlich des Sicherheitsstils des erstellten FlexVol-Volumes, geben Sie den folgenden Befehl ein:

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

Security Styles auf qtrees konfigurieren

Sie konfigurieren den Sicherheitsstil des qtree Volume, um die Art der Berechtigungen zu bestimmen, die für Daten in qtrees verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn der qtree…	Verwenden Sie den Befehl…
Ist noch nicht vorhanden	`volume qtree create` Und nehmen Sie die auf `-security-style` Parameter, um den Sicherheitsstil anzugeben.
Ist bereits vorhanden	`volume qtree modify` Und nehmen Sie die auf `-security-style` Parameter, um den Sicherheitsstil anzugeben.

Die möglichen Optionen für den qtree-Sicherheitsstil sind `unix`, `ntfs`, Oder `mixed`.

Wenn Sie beim Erstellen eines qtree keinen Sicherheitsstil angeben, wird der Standardsicherheitsstil festgelegt `mixed`.

Weitere Informationen zum `volume qtree create` Oder `volume qtree modify` Befehle, siehe "Logisches Storage-Management".

2. Geben Sie zum Anzeigen der Konfiguration, einschließlich des Sicherheitsstils des erstellten qtree, den folgenden Befehl ein: `volume qtree show -qtree qtree_name -instance`

Daten-Volumes werden in NAS-Namespaces erstellt und gemanagt

Erstellen und Managen von Daten-Volumes in NAS-Namespaces – Übersicht

Um den Dateizugriff in einer NAS-Umgebung zu managen, müssen Daten-Volumes und Verbindungspunkte auf Ihrer Storage Virtual Machine (SVM) gemanagt werden. Das umfasst auch die Planung der Namespace-Architektur, das Erstellen von Volumes mit oder ohne Verbindungspunkte, das Mounten oder Aufheben von Volumes und das Anzeigen von Informationen zu Daten-Volumes und NFS-Server oder CIFS-Server-Namespaces.

Erstellung von Daten-Volumes mit festgelegten Verbindungspunkten

Sie können den Verbindungspunkt bei der Erstellung eines Daten-Volumes angeben. Das resultierende Volume wird automatisch am Verbindungspunkt gemountet und ist für den NAS-Zugriff sofort konfiguriert.

Bevor Sie beginnen

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

> Folgende Zeichen können nicht im Verbindungspfad verwendet werden: * # " > < ? \
>
> Darüber hinaus darf die Länge des Verbindungspfades nicht mehr als 255 Zeichen umfassen.

Schritte

1. Volume mit einem Verbindungspunkt 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 Root (/) beginnen und kann sowohl Verzeichnisse als auch Volumes enthalten. Der Verbindungspfad muss den Namen des Volumes nicht enthalten. Verbindungspfade sind unabhängig vom Volume-Namen.

   Die Angabe eines Volume-Sicherheitsstils ist optional. Wenn Sie keinen Sicherheitsstil angeben, erstellt ONTAP das Volume mit dem gleichen Sicherheitstyp, der auf das Root-Volume der SVM (Storage Virtual Machine) angewendet wird. Der Sicherheitsstil des Root-Volumes ist jedoch möglicherweise nicht der Sicherheitsstil, den Sie auf das von Ihnen erstellte Datenvolumen anwenden möchten. Es wird empfohlen, beim Erstellen des Volumes den Sicherheitsstil festzulegen, um Probleme mit dem Dateizugriff zu minimieren, die sich nur schwer beheben lassen.

   Die Groß-/Kleinschreibung des Verbindungspfads wird nicht berücksichtigt. `/ENG` Ist das gleiche wie `/eng`. Wenn Sie eine CIFS-Freigabe erstellen, behandelt Windows den Verbindungspfad so, als ob die Groß-/Kleinschreibung beachtet wird. Beispiel: Wenn die Verbindung lautet `/ENG`, Der Pfad einer CIFS-Freigabe muss mit beginnen `/ENG`, Nicht `/eng`.

   Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Weitere Informationen dazu finden Sie auf den man-Pages für die `volume create` Befehl.

2. Vergewissern Sie sich, dass das Volume mit dem gewünschten Verbindungspunkt erstellt wurde: `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „`home4`“ auf der SVM vs1 mit einem Verbindungspfad erstellt `/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
```

Erstellung von Daten-Volumes ohne Angabe von Verbindungspunkten

Sie können ein Daten-Volume erstellen, ohne einen Verbindungspunkt anzugeben. Das resultierende Volume wird nicht automatisch gemountet und steht für den NAS-Zugriff nicht zur Verfügung. Sie müssen das Volume mounten, bevor Sie SMB-Freigaben oder NFS-Exporte für dieses Volume konfigurieren können.

Bevor Sie beginnen

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

Schritte

1. Um das Volume ohne Verbindungspunkt zu erstellen, verwenden Sie folgenden Befehl: `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 Volume-Sicherheitsstils ist optional. Wenn Sie keinen Sicherheitsstil angeben, erstellt ONTAP das Volume mit dem gleichen Sicherheitstyp, der auf das Root-Volume der SVM (Storage Virtual Machine) angewendet wird. Der Sicherheitsstil des Root-Volumes ist jedoch möglicherweise nicht der Sicherheitsstil, den Sie auf das Datenvolumen anwenden möchten. Es wird empfohlen, beim Erstellen des Volumes den Sicherheitsstil festzulegen, um Probleme mit dem Dateizugriff zu minimieren, die sich nur schwer beheben lassen.

   Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Weitere Informationen dazu finden Sie auf den man-Pages für die `volume create` Befehl.

2. Vergewissern Sie sich, dass das Volume ohne Verbindungspunkt erstellt wurde: `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „`sales`“ auf der SVM vs1 erstellt, das nicht an einem Verbindungspunkt gemountet 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      -        -               -
```

Mounten oder Unmounten vorhandener Volumes im NAS Namespace

Ein Volume muss auf dem NAS Namespace gemountet werden, bevor Sie den NAS-Client-Zugriff auf Daten in den Storage Virtual Machine (SVM)-Volumes konfigurieren können. Sie können ein Volume an einen Verbindungspunkt mounten, wenn es derzeit nicht angehängt ist. Sie können auch die Bereitstellung von Volumes aufheben.

Über diese Aufgabe

Wenn Sie ein Volume unmounten und offline schalten, sind NAS-Clients nicht auf alle Daten innerhalb des Verbindungspunkts zugreifen können, einschließlich Daten in Volumes mit Verbindungspunkten im Namespace des nicht gemounteten Volumes.

> Um den NAS-Client-Zugriff auf ein Volume zu beenden, reicht es nicht aus, das Volume einfach zu entmounten. Sie müssen das Volume offline schalten oder andere Maßnahmen ergreifen, um sicherzustellen, dass die Client-seitigen Datei-Handle-Caches für ungültig erklärt werden. Weitere Informationen finden Sie im folgenden Knowledge Base-Artikel: "NFSv3-Clients haben nach Entfernen aus dem Namespace in ONTAP noch Zugriff auf ein Volume"

Wenn Sie das Mounten aufheben und ein Volume offline schalten, gehen die Daten auf dem Volume nicht verloren. Zusätzlich bleiben vorhandene Volume-Exportrichtlinien und SMB-Freigaben, die auf dem Volume oder auf Verzeichnissen und Verbindungspunkten innerhalb des nicht abgehängt Volume erstellt wurden, erhalten. Wenn Sie das nicht abgesetzte Volume erneut mounten, können NAS-Clients mithilfe vorhandener Exportrichtlinien und SMB-Freigaben auf die Daten im Volume zugreifen.

Schritte

1. Führen Sie die gewünschte Aktion aus:

Ihr Ziel ist	Geben Sie die Befehle ein…
Mounten Sie ein Volume	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*

Ihr Ziel ist	Geben Sie die Befehle ein…
Unmount eines Volumes aufheben	`volume unmount -vserver` *`svm_name`* `-volume` *`volume_name`* `volume offline -vserver` *`svm_name`* `-volume` *`volume_name`*

2. Vergewissern Sie sich, dass sich das Volume im gewünschten Mount-Status befindet:

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

Beispiele

Im folgenden Beispiel wird ein Volume mit dem Namen „`sales`“ auf SVM „`vs1`“ an den Knotenpunkt „`/Sales`“ gemountet:

```
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
```

Im folgenden Beispiel wird ein Volume mit dem Namen „`data`“ auf SVM „`vs1`“ abgehängt und dann offline geschaltet:

```
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
```

Anzeige von Informationen zu Volume Mount und Verbindungspunktpunkten

Sie können Informationen zu gemounteten Volumes für Storage Virtual Machines (SVMs)

und den Verbindungspunkten für die Volumes anzeigen. Sie können auch festlegen, welche Volumes nicht an einem Verbindungspunkt angehängt sind. Anhand dieser Informationen können Sie Ihren SVM-Namespace verstehen und managen.

Schritte

1. Führen Sie die gewünschte Aktion aus:

Sie möchten Folgendes anzeigen:	Geben Sie den Befehl ein…
Zusammenfassende Informationen über gemountete und abgehängt Volumes auf der SVM	`volume show -vserver vserver_name -junction`
Detaillierte Informationen zu gemounteten und abgehängt Volumes auf der SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Spezifische Informationen über gemountete und abgehängt Volumes auf der SVM	a. Bei Bedarf können Sie gültige Felder für das anzeigen `-fields` Parameter mit dem folgenden Befehl: `volume show -fields ?` b. Zeigen Sie die gewünschten Informationen mit dem an `-fields` Parameter: Volume show -vserver vserver_Name -fields fieldname,…

Beispiele

Im folgenden Beispiel werden eine Zusammenfassung der gemounteten und nicht abgehängt Volumes auf SVM vs1 angezeigt:

```
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
```

Im folgenden Beispiel werden Informationen zu den angegebenen Feldern für Volumes in SVM vs2 angezeigt:

```
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
```

Konfigurieren Sie Namenszuordnungen

Übersicht über Namenszuordnungen konfigurieren

ONTAP verwendet Namenszuweisung, um CIFS-Identitäten UNIX-Identitäten, Kerberos-Identitäten und UNIX-Identitäten den CIFS-Identitäten zuzuordnen. Es benötigt diese Informationen, um Benutzeranmeldeinformationen zu erhalten und ordnungsgemäßen Dateizugriff bereitzustellen, unabhängig davon, ob sie eine Verbindung von einem NFS-Client oder einem CIFS-Client herstellen.

Es gibt zwei Ausnahmen, in denen Sie keine Namenszuweisung verwenden müssen:

- Sie konfigurieren eine reine UNIX-Umgebung und planen keinen CIFS-Zugriff oder NTFS-Sicherheitsstil auf Volumes.
- Sie konfigurieren stattdessen den Standardbenutzer für die Verwendung.

  In diesem Szenario ist keine Namenszuweisung erforderlich, da anstelle der Zuordnung aller einzelnen Client-Anmeldeinformationen alle Client-Anmeldeinformationen demselben Standardbenutzer zugeordnet werden.

Beachten Sie, dass Sie die Namenszuordnung nur für Benutzer und nicht für Gruppen verwenden können.

Sie können jedoch einem bestimmten Benutzer eine Gruppe von einzelnen Benutzern zuordnen. Sie können beispielsweise alle AD-Benutzer, die mit DEM Wort „VERTRIEB“ beginnen oder enden, einem bestimmten UNIX-Benutzer und der UID des Benutzers zuordnen.

Funktionsweise der Namenszuweisung

Wenn ONTAP Anmeldeinformationen für einen Benutzer zuordnen muss, überprüft er zunächst die Datenbank für die Zuordnung von lokalen Namen und den LDAP-Server auf eine vorhandene Zuordnung. Überprüft wird, ob ein oder beide Einstellungen überprüft werden und in welcher Reihenfolge durch die Name-Service-Konfiguration der SVM bestimmt wird.

- Für die Zuordnung von Windows zu UNIX

  Wenn keine Zuordnung gefunden wird, überprüft ONTAP, ob der kleine Windows-Benutzername ein gültiger Benutzername in der UNIX-Domäne ist. Wenn dies nicht funktioniert, wird der Standard-UNIX-Benutzer verwendet, sofern er konfiguriert ist. Wenn der standardmäßige UNIX-Benutzer nicht konfiguriert ist und ONTAP auf diese Weise keine Zuordnung erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

- Für die Zuordnung von UNIX zu Windows

  Wenn keine Zuordnung gefunden wird, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der SMB-Standardbenutzer verwendet, vorausgesetzt, er ist konfiguriert. Wenn der standardmäßige CIFS-Benutzer nicht konfiguriert ist und ONTAP auch keine Zuordnung auf diese Weise erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

Computerkonten sind standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung des Computerkontos fehl.

- Ab ONTAP 9.5 können Sie Computerkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuordnen.
- In ONTAP 9.4 und früher können Sie Computerkonten nicht anderen Benutzern zuordnen.

  Auch wenn Namenszuordnungen für Computerkonten definiert sind, werden die Zuordnungen ignoriert.

Multidomain sucht nach Zuordnungen von UNIX-Benutzern zu Windows-Benutzernamen

ONTAP unterstützt Multidomain-Suchen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle erkannten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersatzmuster gesucht, bis ein passendes Ergebnis zurückgegeben wird. Alternativ können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren, die anstelle der Liste der erkannten vertrauenswürdigen Domänen verwendet wird und bis zur Rückgabe eines übereinstimmenden Ergebnisses durchsucht wird.

Wie Domain Trusts sich auf UNIX-Benutzer bei der Suche nach der Windows-User Name Mapping auswirken

Um zu verstehen, wie die Zuordnung von Benutzernamen mit mehreren Domänen funktioniert, müssen Sie verstehen, wie Domain Trusts mit ONTAP arbeiten. Active Directory-Vertrauensbeziehungen mit der Home-Domain des CIFS-Servers können ein bidirektionales Vertrauen sein oder eine von zwei Arten von unidirektionalen Trusts sein, entweder ein eingehendes Vertrauen oder ein ausgehendes Vertrauen. Die Home-Domäne ist die Domäne, zu der der CIFS-Server der SVM gehört.

- *Bidirektionales Vertrauen*

  Bei bidirektionalen Trusts vertrauen sich beide Domänen gegenseitig. Wenn die Home-Domain des CIFS-Servers bidirektional mit einer anderen Domäne vertraut ist, kann die Home-Domäne einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Domäne angehört, und umgekehrt.

  Die Suche nach der Zuordnung von UNIX-Benutzern zu Windows-Benutzernamen kann nur auf Domänen mit bidirektionalen Vertrauensstellungen zwischen der Home-Domain und der anderen Domain ausgeführt werden.

- *Outbound Trust*

  Mit einem ausgehenden Vertrauen vertraut die Home Domain der anderen Domain. In diesem Fall kann die Home-Domain einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Outbound-Domäne angehört.

  Eine Domäne mit einem abgehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern zu Windows-Benutzernamenzuordnung *not* durchsucht.

- *Inbound Trust*

  Mit einem eingehenden Vertrauen vertraut die andere Domäne auf die Home Domain des CIFS-Servers. In diesem Fall kann die Home-Domäne einen Benutzer der eingehenden vertrauenswürdigen Domäne nicht authentifizieren oder autorisieren.

  Eine Domäne mit einem eingehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern bei der Zuordnung von Windows-Benutzernamen *Not* durchsucht.

Wie Platzhalter (*) zum Konfigurieren von Mehrfachdomain-Suchen für das Namenszuordnungen verwendet werden

Suchvorgänge für die Zuordnung von Mehrfachdomänen werden durch die Verwendung von Wildcards im Domain-Bereich des Windows-Benutzernamens erleichtert. In der folgenden Tabelle wird veranschaulicht, wie Wildcards im Domain-Teil eines Namenszuordnungseintrags verwendet werden, um Mehrfachdomain-Suchen zu ermöglichen:

Muster	Austausch	Ergebnis
Stamm	*\\Administrator	Der UNIX-Benutzer „`root`“ ist dem Benutzer „`Administrator`“ zugeordnet. Alle vertrauenswürdigen Domains werden so lange durchsucht, bis der erste übereinstimmende Benutzer namens „`Administrator`“ gefunden wurde.
*	**	Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden so lange durchsucht, bis der erste übereinstimmende Benutzer mit diesem Namen gefunden wurde. Das Muster ** gilt nur für die Namenszuweisung von UNIX zu Windows, nicht umgekehrt.

Durchführen von Suchvorgängen mit mehreren Domänen

Sie können eine von zwei Methoden wählen, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für die Suche nach Namen mehrerer Domänen verwendet werden:

- Verwenden Sie die automatisch erkannte bidirektionale Vertrauensliste, die von ONTAP erstellt wurde
- Verwenden Sie die Liste der bevorzugten vertrauenswürdigen Domänen, die Sie kompilieren

Wenn ein UNIX-Benutzer einem Windows-Benutzer mit einem Platzhalter zugeordnet ist, der für den Domain-Abschnitt des Benutzernamens verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt angezeigt:

- Wenn eine bevorzugte Liste der vertrauenswürdigen Domäne konfiguriert ist, wird der zugeordnete Windows-Benutzer nur in dieser Suchliste in der entsprechenden Reihenfolge angezeigt.
- Wenn eine bevorzugte Liste der vertrauenswürdigen Domänen nicht konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Home-Domäne gesucht.
- Wenn es keine bidirektional vertrauenswürdigen Domänen für die Home-Domain gibt, wird der Benutzer in der Home-Domain angezeigt.

Wenn ein UNIX-Benutzer einem Windows-Benutzer ohne Domain-Abschnitt im Benutzernamen zugeordnet ist, wird der Windows-Benutzer in der Home-Domain angezeigt.

Konvertierungsregeln für Namenszuordnungen

Ein ONTAP System behält eine Reihe von Konversionsregeln für jede SVM bei. Jede Regel besteht aus zwei Teilen: Einem *pattern* und einem *Replacement*. Konvertierungen beginnen am Anfang der entsprechenden Liste und führen eine Substitution basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein normaler Ausdruck im UNIX-Stil. Der Ersatz ist eine Zeichenkette, die Escape-Sequenzen enthält, die Unterausdrücke aus dem Muster darstellen, wie im UNIX `sed` Programm.

Erstellen einer Namenszuweisung

Sie können das verwenden `vserver name-mapping create` Befehl zum Erstellen einer Namenszuweisung. Sie verwenden Namenszuordnungen, um Windows-Benutzern den Zugriff auf UNIX-Sicherheitsstil-Volumes zu ermöglichen und umgekehrt.

Über diese Aufgabe

Für jede SVM unterstützt ONTAP bis zu 12,500 Namenszuordnungen für jede Richtung.

Schritt

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

   > Der `-pattern` Und `-replacement` Aussagen können als reguläre Ausdrücke formuliert werden. Sie können auch die verwenden `-replacement` Anweisung, eine Zuordnung zum Benutzer durch Verwendung der leeren Ersatzzeichenfolge explizit zu verweigern `" "` (Das Leerzeichen). Siehe `vserver name-mapping create` Man-Page für Details.

   Beim Erstellen von Windows-zu-UNIX-Zuordnungen müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, abmelden und zurück anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Mit dem folgenden Befehl wird eine Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätenliste. Das Mapping 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"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätenliste. Hier sind Muster und Ersatz enthalten reguläre Ausdrücke. Das Mapping ordnet jedem 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"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Hier enthält das Muster „` €`“ als Element im Windows-Benutzernamen, das entkommen sein muss. Das Mapping ordnet den Windows-Benutzer eng\ john€3ps dem UNIX-Benutzer john_OPS zu.

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

Konfigurieren Sie den Standardbenutzer

Sie können einen Standardbenutzer so konfigurieren, dass er verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie nicht einzelne Benutzer zwischen UNIX und Windows zuordnen möchten. Wenn die Authentifizierung von nicht zugeordneten Benutzern fehlschlägt, sollten Sie keinen Standardbenutzer konfigurieren.

Über diese Aufgabe

Wenn Sie bei der CIFS-Authentifizierung nicht jeden Windows-Benutzer einem einzelnen UNIX-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen UNIX-Benutzer festlegen.

Wenn Sie bei der NFS-Authentifizierung nicht jeden UNIX-Benutzer einem einzelnen Windows-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen Windows-Benutzer festlegen.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Konfigurieren Sie den UNIX-Standardbenutzer	`vserver cifs options modify -default -unix-user` *`user_name`*
Konfigurieren Sie den Windows-Standardbenutzer	`vserver nfs modify -default-win-user` *`user_name`*

Befehle zum Verwalten von Name-Zuordnungen

Zum Verwalten von Name-Zuordnungen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen einer Namenszuweisung	`vserver name-mapping create`

Ihr Ziel ist	Befehl
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Namenszuordnungen anzeigen	`vserver name-mapping show`
Tauschen Sie die Position von zwei Namenszuordnungen aus Ein Austausch ist nicht zulässig, wenn die Namenszuordnung mit einem ip-Qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Ändern einer Namenszuweisung	`vserver name-mapping modify`
Löschen einer Namenszuweisung	`vserver name-mapping delete`
Überprüfen Sie die richtige Namenszuweisung	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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

Konfigurieren Sie Suchen zur Namenszuweisung für mehrere Domänen

Aktivieren oder deaktivieren Sie Suchvorgänge für die Zuordnung von multidomain-Namen

Bei der Suche nach multidomain Name Mapping können Sie eine Platzhalter (*) im Domain-Teil eines Windows-Namens verwenden, wenn Sie UNIX-Benutzer in die Zuordnung von Windows-Benutzernamen konfigurieren. Durch die Verwendung einer Platzhalter (*) im Domain-Teil des Namens kann ONTAP alle Domänen durchsuchen, denen ein bidirektionales Vertrauen zu der Domäne besteht, die das Computerkonto des CIFS-Servers enthält.

Über diese Aufgabe

Als Alternative zum Durchsuchen aller bidirektional vertrauenswürdigen Domänen können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren. Wenn eine Liste der bevorzugten vertrauenswürdigen Domänen konfiguriert wird, verwendet ONTAP die bevorzugte Liste der vertrauenswürdigen Domänen anstelle der ermittelten bidirektional vertrauenswürdigen Domänen, um Suchen zum Zuordnen von Namen für mehrere Domänen durchzuführen.

- Die Suche nach der Zuordnung von Mehrfachdomänen ist standardmäßig aktiviert.

- Diese Option ist auf der erweiterten Berechtigungsebene verfügbar.

Schritte

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

Wenn Sie Suchvorgänge zur Zuordnung von multidomain wünschen, sind…	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 Administratorberechtigungsebene: `set -privilege admin`

Verwandte Informationen

Verfügbare SMB-Server-Optionen

Vertrauenswürdige Domains zurücksetzen und neu entdecken

Sie können die erneute Ermittlung aller vertrauenswürdigen Domänen erzwingen. Dies kann nützlich sein, wenn die vertrauenswürdigen Domänenserver nicht angemessen reagieren oder sich die Vertrauensbeziehungen geändert haben. Es werden nur Domänen erkannt, die bidirektional mit der Home Domain vertraut sind, d. h. die Domäne, die das Computerkonto des CIFS-Servers enthält.

Schritt

1. Setzen Sie vertrauenswürdige Domänen zurück, und entdecken Sie sie erneut, indem Sie den verwenden `vserver cifs domain trusts rediscover` Befehl.

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

Verwandte Informationen

Anzeigen von Informationen zu erkannten vertrauenswürdigen Domänen

Zeigt Informationen zu erkannten vertrauenswürdigen Domänen an

Sie können Informationen über die erkannten vertrauenswürdigen Domänen für die Home Domain des CIFS-Servers anzeigen, die die Domäne ist, die das Computerkonto des CIFS-Servers enthält. Dies kann nützlich sein, wenn Sie wissen möchten, welche vertrauenswürdigen Domänen erkannt werden und wie sie in der Liste „erkannte vertrauenswürdige Domains“ bestellt werden.

Über diese Aufgabe

Es werden nur die Domains mit bidirektionalen Trusts mit der Home Domain entdeckt. Da der Domänencontroller (DC) der Home-Domain die Liste der vertrauenswürdigen Domänen in einer vom DC bestimmten Reihenfolge zurückgibt, kann die Reihenfolge der Domänen innerhalb der Liste nicht vorhergesagt werden. Wenn Sie die Liste der vertrauenswürdigen Domänen anzeigen, können Sie die Suchreihenfolge für Suchvorgänge mit mehreren Domänen-Namenszuordnungen bestimmen.

Die angezeigten vertrauenswürdigen Domäneninformationen werden nach Node und Storage Virtual Machine (SVM) gruppiert.

Schritt

1. Zeigen Sie Informationen über erkannte vertrauenswürdige Domänen mithilfe des an `vserver cifs domain trusts show` Befehl.

   ```
   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 Domains werden zurückgesetzt und neu erkannt

Vertrauenswürdige Domänen in bevorzugten Listen vertrauenswürdiger Domänen hinzufügen, entfernen oder ersetzen

Sie können vertrauenswürdige Domains aus der Liste der bevorzugten vertrauenswürdigen Domänen für den SMB-Server hinzufügen oder entfernen oder die aktuelle Liste ändern. Wenn Sie eine bevorzugte Liste der vertrauenswürdigen Domänen konfigurieren, wird diese Liste anstelle der gefundenen bidirektionalen vertrauenswürdigen Domänen verwendet, wenn Sie Suchvorgänge für die Zuordnung von Namen mit mehreren Domänen ausführen.

Über diese Aufgabe

- Wenn Sie einer vorhandenen Liste vertrauenswürdige Domains hinzufügen, wird die neue Liste mit der vorhandenen Liste mit den neuen Einträgen am Ende zusammengeführt Die vertrauenswürdigen Domänen werden in der Reihenfolge durchsucht, in der sie in der Liste der vertrauenswürdigen Domäne angezeigt werden.
- Wenn Sie vertrauenswürdige Domänen aus der vorhandenen Liste entfernen und keine Liste angeben, wird die gesamte vertrauenswürdige Domänenliste für die angegebene Storage Virtual Machine (SVM) entfernt.
- Wenn Sie die vorhandene Liste der vertrauenswürdigen Domänen ändern, überschreibt die neue Liste die vorhandene Liste.

> Sie sollten nur bidirektional vertrauenswürdige Domains in die Liste der bevorzugten vertrauenswürdigen Domänen eingeben. Auch wenn Sie ausgehende oder eingehende Vertrauensdomänen in die bevorzugte Domain-Liste eingeben können, werden diese nicht verwendet, wenn Sie Suchvorgänge für die Zuordnung von Namen für mehrere Domänen ausführen. ONTAP überspringt den Eintrag für die unidirektionale Domain und wechselt zur nächsten bidirektionalen vertrauenswürdigen Domain in der Liste.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Folgendes mit der Liste der bevorzugten vertrauenswürdigen Domains tun möchten…	Verwenden Sie den Befehl…
Fügen Sie vertrauenswürdige Domains zur Liste hinzu	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Vertrauenswürdige Domains aus der Liste entfernen	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Die vorhandene Liste ändern	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Beispiele

Mit dem folgenden Befehl werden zwei vertrauenswürdige Domänen (cifs1.example.com und cifs2.example.com) zur bevorzugten vertrauenswürdigen Domain-Liste hinzugefügt, die von SVM vs1 verwendet wird:

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

Mit dem folgenden Befehl werden zwei vertrauenswürdige Domänen aus der Liste der SVM vs1 entfernt:

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

Mit dem folgenden Befehl wird die von SVM vs1 verwendete Liste der vertrauenswürdigen Domäne geändert. Die ursprüngliche Liste wird durch die neue Liste ersetzt:

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

Verwandte Informationen

Informationen zur Liste der bevorzugten vertrauenswürdigen Domänen werden angezeigt

Informationen zur Liste der bevorzugten vertrauenswürdigen Domänen anzeigen

Sie können Informationen darüber anzeigen, welche vertrauenswürdigen Domänen sich in der Liste der bevorzugten vertrauenswürdigen Domäne befinden, und die Reihenfolge, in der sie durchsucht werden, wenn die Suche nach einer Multidomain-Namenszuordnung aktiviert ist. Sie können eine Liste der bevorzugten vertrauenswürdigen Domänen als Alternative zur Verwendung der automatisch ermittelten Liste vertrauenswürdiger Domänen konfigurieren.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über die folgenden anzeigen möchten…	Verwenden Sie den Befehl…
Alle bevorzugten vertrauenswürdigen Domänen im Cluster nach Storage Virtual Machine (SVM) gruppiert	`vserver cifs domain name-mapping-search show`
Alle bevorzugten vertrauenswürdigen Domänen für eine angegebene SVM	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

Mit dem folgenden Befehl werden Informationen zu allen bevorzugten vertrauenswürdigen Domänen auf dem Cluster angezeigt:

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

Verwandte Informationen

Hinzufügen, Entfernen oder Ersetzen von vertrauenswürdigen Domänen in bevorzugten vertrauenswürdigen

SMB-Freigaben erstellen und konfigurieren

SMB-Freigaben erstellen und konfigurieren – Übersicht

Bevor Benutzer und Applikationen über SMB auf Daten auf dem CIFS-Server zugreifen können, müssen SMB-Freigaben erstellt und konfiguriert werden. Hierbei handelt es sich um einen Zugriffspunkt in einem Volume. Sie können Freigaben durch Festlegen von Freigabeparametern und Freigabeigenschaften anpassen. Sie können eine vorhandene Freigabe jederzeit ändern.

Wenn Sie eine SMB-Freigabe erstellen, erstellt ONTAP eine Standard-ACL für die Freigabe mit Full-Control-Berechtigungen für jeden Benutzer.

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 damit verbundene CIFS-Server aus der SVM gelöscht wird. Wenn Sie den CIFS-Server auf der SVM neu erstellen, müssen Sie die SMB-Freigaben erneut erstellen.

Verwandte Informationen

Verwalten Sie den Dateizugriff mit SMB

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

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

Wie die standardmäßigen administrativen Freigaben sind

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

ONTAP erstellt beim Erstellen des CIFS-Servers die folgenden Standard-Administratorfreigaben:

> Ab ONTAP 9.8 wird der Anteil der Admin-Kosten nicht mehr standardmäßig erstellt.

- ipc-Kosten
- Admin-Kosten (nur ONTAP 9.7 und früher)
- c€

Da die mit dem Zeichen € enden Freigaben verborgene Freigaben sind, werden die standardmäßigen administrativen Freigaben nicht auf meinem Computer angezeigt, Sie können sie jedoch mithilfe von freigegebenen Ordnern anzeigen.

Wie die standardanteile von ipc € und Admin€ verwendet werden

Die ipc-Kosten und die Admin-Dollar-Freigaben werden von ONTAP genutzt und können von Windows-Administratoren nicht für den Zugriff auf die auf der SVM gespeicherten Daten verwendet werden.

- ipc-Aktie

  Der ipc-USD-Anteil ist eine Ressource, die die benannten Rohre teilt, die für die Kommunikation zwischen den Programmen wesentlich sind. Die ipc-€-Freigabe wird während der Remote-Administration eines Computers und bei der Anzeige der gemeinsam genutzten Ressourcen eines Computers verwendet. Sie können die Freigabereinstellungen, Freigabeigenschaften oder ACLs der ipc-€-Freigabe nicht ändern. Sie können die ipc-€-Freigabe auch nicht umbenennen oder löschen.

- Anteil von Admin-Dollar (nur ONTAP 9.7 und früher)

  > Ab ONTAP 9.8 wird der Anteil der Admin-Kosten nicht mehr standardmäßig erstellt.

  Der Anteil der Admin-Kosten wird bei der Remote-Administration der SVM verwendet. Der Pfad dieser Ressource ist immer der Pfad zum SVM-Stammverzeichnis. Sie können die Freigabeneinstellungen, Freigabeigenschaften oder ACLs für die USD-Freigabe nicht ändern. Sie können auch die „Administrator-Dollar-Freigabe“ nicht umbenennen oder löschen.

Wie der Standardanteil c€ verwendet wird

Die C€-Freigabe ist eine administrative Freigabe, die der Cluster- oder SVM-Administrator zum Zugriff und Managen des SVM-Root-Volumes verwenden kann.

Die folgenden Merkmale sind die c-Dollar-Aktie:

- Der Pfad für diese Freigabe ist immer der Pfad zum SVM-Root-Volume und kann nicht geändert werden.
- Die Standard-ACL für die Aktie von c€ ist Administrator / Full Control.

  Dieser Benutzer ist der BUILTIN\Administrator. Standardmäßig kann der BUILTIN\-Administrator Dateien und Ordner im zugeordneten Stammverzeichnis teilen und anzeigen, erstellen, ändern oder löschen. Beim Verwalten von Dateien und Ordnern in diesem Verzeichnis ist Vorsicht geboten.

- Sie können die ACL der c€-Aktie ändern.
- Sie können die Einstellungen für die gemeinsame Nutzung von € ändern und Eigenschaften freigeben.
- Sie können die Freigabe von € nicht löschen.
- Der SVM-Administrator kann über die Namespace-Verbindungen auf den Rest des SVM Namespace zugreifen und dabei die zugewiesene C€-Freigabe verwenden.
- Auf die C€-Aktie kann über die Microsoft Management Console zugegriffen werden.

Verwandte Informationen

Konfigurieren erweiterter NTFS-Dateiberechtigungen mithilfe der Registerkarte Windows-Sicherheit

Benennungsanforderungen für die SMB-Freigabe

Beim Erstellen von SMB-Shares auf Ihrem SMB Server sollten Sie die Benennungsanforderungen für ONTAP-Freigaben berücksichtigen.

Die Namenskonventionen für ONTAP entsprechen denen für Windows und enthalten die folgenden Anforderungen:

- Der Name der einzelnen Shares muss für den SMB-Server eindeutig sein.

- Freigeben von Namen beachten Sie nicht die Groß-/Kleinschreibung.
- Die maximale Länge des Share-Namens beträgt 80 Zeichen.
- Unicode-Freigabnamen werden unterstützt.
- Share-Namen, die mit dem Zeichen € enden, sind ausgeblendete Aktien.
- Bei ONTAP 9.7 und älteren Versionen werden die Admin-Dollar, ipc-Kosten und c€-administrativen Freigaben automatisch auf jedem CIFS-Server erstellt und sind Freigabnamen. Ab ONTAP 9.8 wird der Anteil der Admin-Kosten nicht mehr automatisch erstellt.
- Sie können den Share-Namen ONTAP_ADMIN nicht verwenden, wenn Sie eine Freigabe erstellen.
- Freigabnamen mit Leerzeichen werden unterstützt:
  - Sie können kein Leerzeichen als erstes Zeichen oder als letztes Zeichen in einem Freigabennamen verwenden.
  - Sie müssen Freigabennamen einschließen, die ein Leerzeichen in Anführungszeichen enthalten.

> Einzelne Anführungszeichen gelten als Teil des Freigabennamens und können nicht anstelle von Anführungszeichen verwendet werden.

- Die folgenden Sonderzeichen werden unterstützt, wenn Sie SMB-Freigaben nennen:

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

- Die folgenden Sonderzeichen werden nicht unterstützt, wenn Sie SMB-Freigaben nennen:
  - " / \ : ; < > , ? * =

Verzeichnis von Anforderungen bezüglich der Groß-/Kleinschreibung beim Erstellen von Freigaben in einer Multi-Protokoll-Umgebung

Wenn Sie in einer SVM Freigaben erstellen, bei denen das Benennungsschema 8.3 verwendet wird, um zwischen Verzeichnisnamen zu unterscheiden, bei denen nur Groß-/Kleinschreibung zwischen den Namen besteht, müssen Sie den Namen 8.3 im Freigabepfad verwenden, um sicherzustellen, dass der Client eine Verbindung zum gewünschten Verzeichnispfad herstellt.

Im folgenden Beispiel wurden auf einem Linux-Client zwei Verzeichnisse mit dem Namen „`testdir`“ und „`TESTDIR`“ erstellt. Der Verbindungspfad des Volumes, das die Verzeichnisse enthält, lautet `/home`. Die erste Ausgabe stammt von einem Linux-Client und die zweite Ausgabe stammt 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, müssen Sie den Namen 8.3 im Freigabepfad verwenden. In diesem Beispiel lautet der Freigabepfad zum ersten Verzeichnis `/home/testdir` Und der Freigabepfad zum zweiten Verzeichnis lautet `/home/TESTDI~1`.

Verwenden Sie die SMB-Share-Eigenschaften

Verwenden Sie die Übersicht über die Eigenschaften der SMB-Freigabe

Sie können die Eigenschaften von SMB-Freigaben anpassen.

Die verfügbaren Freigabeneigenschaften sind wie folgt:

Eigenschaften freigeben	Beschreibung
`oplocks`	Diese Eigenschaft gibt an, dass die Freigabe opportunistische Sperren verwendet, die auch als Client-seitiges Caching bezeichnet werden.
`browsable`	Mit dieser Eigenschaft können Windows-Clients die Freigabe durchsuchen.
`showsnapshot`	Diese Eigenschaft gibt an, dass Snapshot Kopien von Clients angezeigt und durch sie geleitet werden können.
`changenotify`	Diese Eigenschaft gibt an, dass die Freigabe Anforderungen für Änderungsbenachrichtigungsanfragen unterstützt. Bei Freigaben auf einer SVM handelt es sich hierbei um eine Standardeigenschaft.
`attributecache`	Durch diese Eigenschaft kann das Caching von Dateiattributen auf der SMB-Freigabe für schnelleren Zugriff auf Attribute ermöglicht werden. Der Standardwert besteht darin, das Attribut-Caching zu deaktivieren. Diese Eigenschaft sollte nur aktiviert werden, wenn Clients eine Verbindung zu Freigaben über SMB 1.0 herstellen. Diese Freigabegenschaft ist nicht anwendbar, wenn Clients eine Verbindung zu Freigaben über SMB 2.x oder SMB 3.0 herstellen.

Eigenschaften freigeben	Beschreibung
`continuously-available`	Mit dieser Eigenschaft können SMB-Clients Dateien persistent öffnen. Auf diese Weise geöffnete Dateien werden vor Ereignissen wie Failover und Giveback geschützt.
`branchcache`	Diese Eigenschaft gibt an, dass die Freigabe es Clients ermöglicht, BranchCache-Hash für die Dateien in dieser Freigabe anzufordern. Diese Option ist nur dann nützlich, wenn Sie in der CIFS-BranchCache-Konfiguration „`per-share`“ als Betriebsmodus angeben.
`access-based-enumeration`	Diese Eigenschaft gibt an, dass *Access Based Enumeration* (ABE) für diese Freigabe aktiviert ist. FREIGEGEBENE Ordner MIT ABE-Filter sind für einen Benutzer auf der Grundlage der Zugriffsrechte des jeweiligen Benutzers sichtbar. Dadurch wird verhindert, dass Ordner oder andere freigegebene Ressourcen angezeigt werden, auf die der Benutzer keine Zugriffsrechte besitzt.
`namespace-caching`	Diese Eigenschaft gibt an, dass die mit dieser Freigabe verbundenen SMB-Clients die von den CIFS-Servern zurückgegebenen Verzeichnisauflierationsergebnisse zwischenspeichern können, was eine bessere Leistung bieten kann. SMB 1-Clients speichern standardmäßig keine Ergebnisse der Verzeichnisenumeration. Da SMB 2- und SMB 3-Clients standardmäßig Ergebnisse der Cache-Verzeichnisauflistung erzielen, bietet die Angabe dieser Share-Eigenschaft nur für SMB 1-Client-Verbindungen Performance-Vorteile.
`encrypt-data`	Diese Eigenschaft gibt an, dass SMB-Verschlüsselung beim Zugriff auf diese Freigabe verwendet werden muss. SMB-Clients, die Verschlüsselung beim Zugriff auf SMB-Daten nicht unterstützen, können nicht auf diese Freigabe zugreifen.

Fügen Sie Share-Eigenschaften für eine vorhandene SMB-Freigabe hinzu oder entfernen Sie sie

Sie können eine vorhandene SMB-Freigabe anpassen, indem Sie Eigenschaften für die Freigabe hinzufügen oder entfernen. Dies kann nützlich sein, wenn Sie die Share-Konfiguration ändern möchten, um den sich ändernden Anforderungen in Ihrer Umgebung gerecht zu werden.

Bevor Sie beginnen

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

Über diese Aufgabe

Richtlinien zum Hinzufügen von Freigabeigenschaften:

- Sie können eine oder mehrere Share-Eigenschaften hinzufügen, indem Sie eine durch Komma getrennte Liste verwenden.
- Alle zuvor angegebenen Freigabeigenschaften bleiben wirksam.

  Neu hinzugefügte Eigenschaften werden an die vorhandene Liste der Freigabeliegenschaften angehängt.

- Wenn Sie einen neuen Wert für die Freigabeigenschaften angeben, die bereits auf die Freigabe angewendet wurden, ersetzt der neu angegebene Wert den ursprünglichen Wert.
- Sie können die Freigabeneigenschaften nicht mithilfe des entfernen `vserver cifs share properties add` Befehl.

  Sie können das verwenden `vserver cifs share properties remove` Befehl zum Entfernen der Freigabeigenschaften.

Richtlinien zum Entfernen von Share-Eigenschaften:

- Sie können eine oder mehrere Share-Eigenschaften entfernen, indem Sie eine durch Komma getrennte Liste verwenden.
- Alle zuvor angegebenen Freigabeigenschaften, die jedoch nicht entfernt wurden, bleiben wirksam.

Schritte

1. Geben Sie den entsprechenden Befehl ein:

Ihr Ziel ist	Geben Sie den Befehl ein…
Eigenschaften für die Freigabe hinzufügen	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Eigenschaften für die Freigabe entfernen	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Überprüfen Sie die Einstellungen für die Freigabegeneigenschaft: `vserver cifs share show -vserver vserver_name -share-name share_name`

Beispiele

Mit dem folgenden Befehl wird der hinzugefügt `showsnapshot` Eigenschaft als Freigabe für einen Share namens „`share1`“ auf SVM vs1:

```
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
```

Mit dem folgenden Befehl wird das entfernt `browsable` Eigenschaft von einem Share namens „`share2`“ auf SVM vs1 freigeben:

```
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 zum Verwalten von SMB-Freigaben

Optimieren Sie den SMB-Benutzerzugriff mit der Einstellung Force-Group-Freigabe

Wenn Sie eine Freigabe von der ONTAP-Befehlszeile zu Daten mit UNIX-effektiver Sicherheit erstellen, können Sie angeben, dass alle Dateien, die von SMB-Benutzern in dieser Freigabe erstellt wurden, zur gleichen Gruppe gehören, die als *Force-Group* bezeichnet wird. Dies muss eine vordefinierte Gruppe in der UNIX-Gruppendatenbank sein. Durch die Verwendung einer Force-Group ist es einfacher sicherzustellen, dass SMB-Benutzer, die zu verschiedenen Gruppen gehören, auf Dateien zugreifen können.

Die Angabe einer Force-Group ist nur dann sinnvoll, wenn sich der Share in einem Unix oder einem gemischten qtree befindet. Es muss keine Force-Group für Shares in einem NTFS-Volume oder qtree festgelegt werden, da der Zugriff auf Dateien in diesen Shares durch Windows-Berechtigungen und nicht durch UNIX GIDs bestimmt wird.

Wenn für eine Freigabe eine Force-Group angegeben wurde, gilt die Freigabe folgendermaßen:

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

Mit dieser GID können sie auf Dateien in dieser Freigabe zugreifen, auf die normalerweise mit ihrer primären GID oder UID nicht zugegriffen werden kann.

- Alle von SMB-Benutzern in diesem Share erstellten Dateien gehören zur gleichen Force-Gruppe, unabhängig von der primären GID des Dateiinhabers.

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

Die Force-Group hat keinen Einfluss darauf, wie NFS-Benutzer auf Dateien in dieser Freigabe zugreifen. Eine von NFS erstellte Datei erwirbt die GID vom Eigentümer der Datei. Die Festlegung der Zugriffsberechtigungen basiert auf der UID und der primären GID des NFS-Benutzers, der versucht, auf die Datei zuzugreifen.

Durch die Verwendung einer Force-Group ist es einfacher sicherzustellen, dass SMB-Benutzer, die zu verschiedenen Gruppen gehören, auf Dateien zugreifen können. Wenn Sie beispielsweise eine Freigabe erstellen möchten, um die Webseiten des Unternehmens zu speichern und Benutzern in den Bereichen Engineering und Marketing Schreibzugriff zu geben, können Sie eine Freigabe erstellen und einer Force-Group namens „`webgroup1`“ Schreibzugriff gewähren. Aufgrund der Force-Group sind alle Dateien, die von SMB-Benutzern in dieser Freigabe erstellt wurden, Eigentum der Gruppe „`webgroup1`“. Außerdem wird den Benutzern beim Zugriff auf die Freigabe automatisch die GID der Gruppe „`webgroup1`“ zugewiesen. Dadurch können alle Benutzer auf diese Freigabe schreiben, ohne dass Sie die Zugriffsrechte der Benutzer in den Bereichen Engineering und Marketing verwalten müssen.

Verwandte Informationen

Erstellen einer SMB-Freigabe mit der Force-Group-Freigabe-Einstellung

Erstellen Sie eine SMB-Freigabe mit der Force-Group-Freigabe-Einstellung

Sie können eine SMB-Freigabe mit der Force-Group-Freigabe-Einstellung erstellen, wenn Sie möchten, dass SMB-Benutzer auf Daten auf Volumes oder qtrees mit UNIX Dateisicherheit zugreifen, die von ONTAP als zu derselben UNIX-Gruppe gehören.

Schritt

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

   Wenn der UNC-Pfad verwendet wird (`\\servername\sharename\filepath`) Der Aktie enthält mehr als 256 Zeichen (ohne die erste “`\\`” Im UNC-Pfad) ist die Registerkarte **Sicherheit** im Feld Windows-Eigenschaften nicht verfügbar. Dies ist ein Problem mit dem Windows-Client und kein ONTAP-Problem. Um dieses Problem zu vermeiden, erstellen Sie keine Freigaben mit UNC-Pfaden mit mehr als 256 Zeichen.

   Wenn Sie die Force-Group nach dem Erstellen der Freigabe entfernen möchten, können Sie die Freigabe jederzeit ändern und einen leeren String ("") als Wert für das angeben `-force-group-for-create` Parameter. Wenn Sie die Force-Group durch Ändern der Freigabe entfernen, haben alle vorhandenen Verbindungen zu dieser Freigabe weiterhin die zuvor eingestellte Force-Group als primäre GID.

Beispiel

Mit dem folgenden Befehl wird eine Freigabe von „`Webseiten`“ erstellt, die im im Web verfügbar ist `/corp/companyinfo` Verzeichnis, in dem alle Dateien, die SMB-Benutzer erstellen, der webgroup1-Gruppe zugewiesen werden:

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

Verwandte Informationen

Optimieren Sie den SMB-Benutzerzugriff mit der Einstellung Force-Group-Freigabe

Zeigen Sie Informationen zu SMB-Freigaben mithilfe von MMC an

Sie können Informationen zu SMB-Freigaben auf Ihrer SVM anzeigen und verschiedene Managementaufgaben mithilfe der Microsoft Management Console (MMC) ausführen. Bevor Sie die Freigaben anzeigen können, müssen Sie MMC mit der SVM verbinden.

Über diese Aufgabe

Sie können die folgenden Aufgaben für Shares in SVMs mithilfe des MMC ausführen:

- Freigaben anzeigen
- Anzeigen aktiver Sitzungen
- Öffnen Sie Dateien anzeigen
- Listen Sie die Liste der Sitzungen, Dateien und Baumverbindungen im System auf
- Schließen Sie offene Dateien im System
- Offene Sitzungen schließen
- Freigaben erstellen/managen

> Die von den vorhergehenden Funktionen angezeigten Ansichten sind Node-spezifisch und nicht Cluster-spezifisch. Wenn Sie die MMC verwenden, um sich mit dem Host-Namen des SMB-Servers (d. h. cifs01.Domain.local) zu verbinden, werden Sie, basierend auf der Art und Weise, wie Sie DNS eingerichtet haben, an eine einzelne LIF innerhalb Ihres Clusters weitergeleitet.

Die folgenden Funktionen werden in MMC für ONTAP nicht unterstützt:

- Erstellen neuer lokaler Benutzer/Gruppen
- Verwalten/Anzeigen vorhandener lokaler Benutzer/Gruppen
- Anzeigen von Ereignissen oder Performance-Protokollen
- Storage
- Services und Applikationen

In Fällen, in denen der Vorgang nicht unterstützt wird, können Sie möglicherweise Erfahrung haben `remote procedure call failed` Fehler.

"FAQ: Verwendung von Windows MMC mit ONTAP"

Schritte

1. Um Computer Management MMC auf einem beliebigen Windows-Server zu öffnen, wählen Sie in der Systemsteuerung* die Option **Verwaltung** > **Computerverwaltung**.
2. Wählen Sie **Aktion** > **Verbindung zu einem anderen Computer**.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.

3. Geben Sie den Namen des Speichersystems ein, oder klicken Sie auf **Durchsuchen**, um das Speichersystem zu finden.
4. Klicken Sie auf **OK**.

   Der MMC stellt eine Verbindung zur SVM her.

5. Klicken Sie im Navigationsbereich auf **freigegebene Ordner** > **Freigaben**.

   Im rechten Anzeigefenster wird eine Liste der Freigaben auf der SVM angezeigt.

6. Um die Freigabeigenschaften für eine Freigabe anzuzeigen, doppelklicken Sie auf die Freigabe, um das Dialogfeld **Eigenschaften** zu öffnen.
7. Wenn Sie mithilfe von MMC keine Verbindung zum Speichersystem herstellen können, können Sie den Benutzer zur BUILTIN\Administrators Group oder BUILTIN\Power Users Group hinzufügen, indem Sie einen der folgenden Befehle auf dem Speichersystem verwenden:

```
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>
```

Befehle zum Verwalten von SMB-Freigaben

Sie verwenden das `vserver cifs share` Und `vserver cifs share properties` Befehle zum Management von SMB-Freigaben.

Ihr Ziel ist	Befehl
Erstellen Sie eine SMB-Freigabe	`vserver cifs share create`
Anzeigen von SMB-Freigaben	`vserver cifs share show`
Ändern einer SMB-Freigabe	`vserver cifs share modify`
Löschen einer SMB-Freigabe	`vserver cifs share delete`
Fügen Sie eine Freigabeneigenschaft zu einer vorhandenen Freigabe hinzu	`vserver cifs share properties add`
Entfernen Sie die Freigabeigenschaften aus einer vorhandenen Freigabe	`vserver cifs share properties remove`
Zeigt Informationen zu Freigabeigenschaften an	`vserver cifs share properties show`

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

Sicherer Dateizugriff über SMB-Share-ACLs

Richtlinien zum Management von SMB-ACLs auf Share-Ebene

Sie können ACLs auf Share-Ebene ändern, um Benutzern mehr oder weniger Zugriffsrechte für die Freigabe zu gewähren. Sie können ACLs auf Share-Ebene entweder mithilfe von Windows-Benutzern und -Gruppen oder UNIX-Benutzern und -Gruppen konfigurieren.

Nachdem Sie eine Freigabe erstellt haben, gewährt die share-Level ACL standardmäßig Lesezugriff auf die Standardgruppe namens Everyone. Lesezugriff in der ACL bedeutet, dass alle Benutzer in der Domäne und alle vertrauenswürdigen Domänen nur Lesezugriff auf die Freigabe haben.

Sie können eine Zugriffssteuerungsliste auf der Share-Ebene ändern, indem Sie die Microsoft Management Console (MMC) in einem Windows-Client oder in der ONTAP-Befehlszeile verwenden.

Die folgenden Richtlinien gelten, wenn Sie die MMC verwenden:

- Der angegebene Benutzer- und Gruppenname muss Windows-Namen sein.
- Sie können nur Windows-Berechtigungen angeben.

Wenn Sie die ONTAP-Befehlszeile verwenden, gelten die folgenden Richtlinien:

- Der angegebene Benutzer- und Gruppenname kann Windows- oder UNIX-Namen sein.

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

- Sie können nur Windows-Berechtigungen angeben.

Erstellen Sie SMB-Zugriffssteuerungslisten

Durch die Konfiguration von Freigabeberechtigungen durch die Erstellung von Zugriffssteuerungslisten (ACLs) für SMB-Freigaben können Sie die Zugriffsebene für eine Freigabe für Benutzer und Gruppen steuern.

Über diese Aufgabe

Sie können ACLs auf Share-Ebene mithilfe lokaler oder Domain-Windows-Benutzer- oder Gruppennamen oder UNIX-Benutzer- oder Gruppennamen konfigurieren.

Bevor Sie eine neue ACL erstellen, sollten Sie die Standard-Freigabe-ACL löschen `Everyone / Full Control`, Die ein Sicherheitsrisiko ist.

Im Arbeitsgruppenmodus ist der Name der lokalen Domäne der Name des SMB-Servers.

Schritte

1. Löschen Sie die Standard-Freigabe-ACL:`vserver cifs share Access-control delete -vserver *vserver_Name* -share *share_Name* -user-or-Group everyone`
2. Konfigurieren Sie die neue ACL:

Wenn Sie ACLs mit… 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. Überprüfen Sie, ob die ACL, die auf die Freigabe angewendet wurde, korrekt ist, indem Sie die verwenden `vserver cifs share access-control show` Befehl.

Beispiel

Der folgende Befehl gibt `Change` Berechtigungen für die Windows-Gruppe „`Sales Team`“ für den „`sales`“-Share 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 gibt `Read` Genehmigung der UNIX Gruppe „`Engineering`“ für den „`eng`“-Share auf der „`vs2.example.com` SVM:

```
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 geben an `Change` Berechtigung für die lokale Windows-Gruppe namens “Tiger Team” und `Full_Control` Berechtigung für den lokalen Windows-Benutzer namens „`Sue Chang`“ für die Freigabe „`datavol5`“ auf der „`vs1` SVM:

```
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
```

Befehle zum Managen von SMB-Zugriffssteuerungslisten

Sie müssen die Befehle zum Verwalten von SMB Access Control Lists (ACLs) kennen, die das Erstellen, Anzeigen, Ändern und Löschen von ihnen umfassen.

Ihr Ziel ist	Befehl
Neue ACL erstellen	`vserver cifs share access-control create`
ACLs anzeigen	`vserver cifs share access-control show`
Ändern Sie eine ACL	`vserver cifs share access-control modify`
Löschen einer ACL	`vserver cifs share access-control delete`

Sicherer Dateizugriff durch Verwenden von Dateiberechtigungen

Konfigurieren Sie die erweiterten NTFS-Dateiberechtigungen mithilfe der Registerkarte Windows-Sicherheit

Sie können Standard-NTFS-Dateiberechtigungen für Dateien und Ordner konfigurieren,

indem Sie im Fenster Windows-Eigenschaften die Registerkarte **Windows-Sicherheit** verwenden.

Bevor Sie beginnen

Der Administrator, der diese Aufgabe ausführt, muss über ausreichende NTFS-Berechtigungen verfügen, um 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-Ermessensary Access Control Lists (DACLs), die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows GUI übernommen.

Schritte

1. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
2. Füllen Sie das Dialogfeld **Map Network Drive** aus:

   a. Wählen Sie einen **Drive**-Buchstaben aus.

   b. Geben Sie im Feld **Ordner** den CIFS-Servernamen ein, der den Share enthält, der die Daten enthält, auf die Sie Berechtigungen anwenden möchten, und den Namen der Freigabe.

   Wenn der Name Ihres CIFS-Servers „`CIFS_SERVER`“ lautet und Ihre Freigabe „`share1`“ heißt, sollten Sie eingeben `\\CIFS_SERVER\share1`.

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

   c. Klicken Sie Auf **Fertig Stellen**.

   Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

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

   Auf der Registerkarte **Sicherheit** wird die Liste der Benutzer und Gruppen angezeigt, für die NTFS-Berechtigungen festgelegt sind. Im Feld **Berechtigungen für** wird eine Liste mit Berechtigungen für jeden ausgewählten Benutzer oder jede ausgewählte Gruppe angezeigt.

6. Klicken Sie Auf **Erweitert**.

   Im Fenster Windows-Eigenschaften werden Informationen über vorhandene Dateiberechtigungen angezeigt, die Benutzern und Gruppen zugewiesen sind.

7. Klicken Sie Auf **Berechtigungen Ändern**.

   Das Fenster Berechtigungen wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Einrichten erweiterter NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe	a. Klicken Sie Auf **Hinzufügen**. b. Geben Sie in das Feld *Geben Sie den Objektnamen ein, den Sie auswählen möchten. Geben Sie den Namen des Benutzers oder der Gruppe ein, den Sie hinzufügen möchten. c. Klicken Sie auf **OK**.
Ändern Sie erweiterte NTFS-Berechtigungen von einem Benutzer oder einer Gruppe	a. Wählen Sie im Feld **Berechtigungen Einträge:** den Benutzer oder die Gruppe aus, deren erweiterte Berechtigungen Sie ändern möchten. b. Klicken Sie Auf **Bearbeiten**.
Entfernen Sie erweiterte NTFS-Berechtigungen für einen Benutzer oder eine Gruppe	a. Wählen Sie im Feld **Berechtigungen Einträge:** den Benutzer oder die Gruppe aus, die Sie entfernen möchten. b. Klicken Sie Auf **Entfernen**. c. Weiter mit Schritt 13.

Wenn Sie erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe hinzufügen oder die erweiterten NTFS-Berechtigungen für einen vorhandenen Benutzer oder eine vorhandene Gruppe ändern, wird das Feld Berechtigung für <Objekt> geöffnet.

9. Wählen Sie im Feld **Apply to** aus, wie Sie diesen NTFS-Dateiberechtigungseintrag anwenden möchten.

   Wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei einrichten, ist das Feld **Apply to** nicht aktiv. Die Einstellung **Apply to** ist standardmäßig auf **nur dieses Objekt** eingestellt.

10. Wählen Sie im Feld **Berechtigungen** die Felder **erlauben** oder **verweigern** für die erweiterten Berechtigungen, die Sie für dieses Objekt festlegen möchten.

    - Um den angegebenen Zugriff zuzulassen, wählen Sie das Feld **Zulassen** aus.
    - Um den angegebenen Zugriff nicht zuzulassen, wählen Sie das Feld **Deny** aus. Sie können Berechtigungen für die folgenden erweiterten Rechte festlegen:
    - **Volle Kontrolle**

      Wenn Sie dieses erweiterte Recht wählen, werden alle anderen erweiterten Rechte automatisch ausgewählt (entweder Rechte zulassen oder verweigern).

    - **Traverse Ordner / Datei ausführen**
    - **Ordner auflisten / Daten lesen**
    - **Attribute lesen**
    - **Erweiterte Attribute lesen**
    - **Dateien erstellen / Daten schreiben**
    - **Ordner erstellen / Daten anhängen**
    - **Attribute schreiben**

- **Erweiterte Attribute schreiben**
- **Löschen von Unterordnern und Dateien**
- **Löschen**
- **Berechtigungen lesen**
- **Berechtigungen ändern**
- **Besitzrechte übernehmen**

> Wenn eines der Felder mit erweiterten Berechtigungen nicht ausgewählt werden kann, liegt dies daran, dass die Berechtigungen vom übergeordneten Objekt übernommen werden.

11. Wenn Sie möchten, dass Unterordner und Dateien dieses Objekts diese Berechtigungen erben, wählen Sie das Feld **Diese Berechtigungen auf Objekte und/oder Container innerhalb dieses Containers only** anwenden.
12. Klicken Sie auf **OK**.
13. Geben Sie nach dem Hinzufügen, Entfernen oder Bearbeiten von NTFS-Berechtigungen die Vererbung für dieses Objekt an:

    - Wählen Sie aus dem Feld **include inheritable Berechtigungen aus dem übergeordneten** dieses Objekts aus.

      Dies ist die Standardeinstellung.

    - Wählen Sie aus diesem Objekt* das Feld *Alle Berechtigungen für untergeordnete Objekte mit vererbbaren Berechtigungen ersetzen aus.

      Diese Einstellung ist nicht im Feld Berechtigungen vorhanden, wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei festlegen.

      > Gehen Sie bei der Auswahl dieser Einstellung vorsichtig vor. Mit dieser Einstellung werden alle bestehenden Berechtigungen für alle untergeordneten Objekte entfernt und durch die Berechtigungseinstellungen dieses Objekts ersetzt. Sie können versehentlich Berechtigungen entfernen, die Sie nicht entfernen möchten. Es ist besonders wichtig, wenn Berechtigungen in einem gemischten Volume oder qtree im Sicherheitsstil festgelegt werden. Wenn untergeordnete Objekte einen effektiven UNIX-Sicherheitsstil haben, führt die Weitergabe von NTFS-Berechtigungen an diese untergeordneten Objekte dazu, dass ONTAP diese Objekte vom UNIX-Sicherheitsstil auf den NTFS-Sicherheitsstil ändert. Alle UNIX-Berechtigungen für diese untergeordneten Objekte werden durch NTFS-Berechtigungen ersetzt.

    - Wählen Sie beide Felder aus.
    - Wählen Sie keine der Kontrollkästchen aus.
14. Klicken Sie auf **OK**, um das Feld **Berechtigungen** zu schließen.
15. Klicken Sie auf **OK**, um das Feld **Erweiterte Sicherheitseinstellungen für <Objekt>** zu schließen.

    Weitere Informationen zum Festlegen erweiterter NTFS-Berechtigungen finden Sie in der Windows-Dokumentation.

Verwandte Informationen

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

Anzeigen von Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes

Anzeigen von Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart

Anzeigen von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Konfigurieren Sie die NTFS-Dateiberechtigungen mit der ONTAP-CLI

Sie können NTFS-Dateiberechtigungen für Dateien und Verzeichnisse mithilfe der ONTAP-CLI konfigurieren. Auf diese Weise können Sie NTFS-Dateiberechtigungen konfigurieren, ohne eine Verbindung mit den Daten über eine SMB-Freigabe auf einem Windows-Client herstellen zu müssen.

Sie können NTFS-Dateiberechtigungen konfigurieren, indem Sie Einträge zu den NTFS-Ermessensary-Zugriffssteuerungslisten (DACLs) hinzufügen, die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet.

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

Schritte

1. Erstellen Sie einen NTFS-Sicherheitsdeskriptor.

   ```
   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. Fügen Sie DACLs zum NTFS-Sicherheitsdeskriptor hinzu.

   ```
   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. Erstellen Sie eine Datei-/Verzeichnissicherheitsrichtlinie.

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

Wie UNIX-Dateiberechtigungen beim Zugriff auf Dateien über SMB Zugriffskontrolle bieten

Ein FlexVol Volume kann einen von drei Arten von Sicherheitstyp haben: NTFS, UNIX oder gemischt. Sie können unabhängig vom Sicherheitsstil auf Daten über SMB zugreifen. Für den Zugriff auf Daten mit UNIX-Sicherheit sind jedoch entsprechende UNIX-Dateiberechtigungen erforderlich.

Wenn über SMB auf Daten zugegriffen wird, gibt es mehrere Zugriffskontrollen, die bei der Entscheidung, ob ein Benutzer zur Durchführung einer angeforderten Aktion berechtigt ist, verwendet werden:

- Exportberechtigungen

Die Konfiguration von Exportberechtigungen für SMB-Zugriff ist optional.

- Freigabeberechtigungen
- Dateiberechtigungen

  Die folgenden Arten von Dateiberechtigungen können auf die Daten angewendet werden, auf die der Benutzer eine Aktion ausführen möchte:

  - NTFS
  - UNIX NFSv4-ACLs
  - Bits im UNIX-Modus

Für Daten mit festgelegten NFSv4-ACLs oder UNIX-Modus-Bits werden Berechtigungen im UNIX-Stil verwendet, um die Zugriffsrechte für die Daten auf den Dateizugriff zu ermitteln. Der SVM-Administrator muss die entsprechende Dateiberechtigung festlegen, um sicherzustellen, dass Benutzer über die Rechte zur Durchführung der gewünschten Aktion verfügen.

> Bei Daten in einem Volume mit gemischtem Sicherheitsstil sind möglicherweise NTFS oder UNIX Sicherheitstyp aktiviert. Wenn die Daten über einen effektiven UNIX-Sicherheitsstil verfügen, werden NFSv4-Berechtigungen oder UNIX-Modus-Bits verwendet, wenn die Zugriffsrechte auf die Daten bestimmt werden.

Sicherer Dateizugriff über Dynamic Access Control (DAC)

Sicherer Dateizugriff über Dynamic Access Control (DAC) mit Übersicht

Der Zugriff lässt sich mithilfe der dynamischen Zugriffssteuerung und der Erstellung zentraler Zugriffsrichtlinien in Active Directory sichern. Darüber hinaus werden sie über Applicate Group Policy Objects (GPOs) auf Dateien und Ordner auf SVMs angewendet. Sie können die Prüfung so konfigurieren, dass zentrale Zugriffs-Policy-Staging-Ereignisse verwendet werden, um die Auswirkungen von Änderungen auf zentrale Zugriffsrichtlinien zu sehen, bevor Sie sie anwenden.

Erweiterung zu CIFS-Anmeldeinformationen

Vor der Dynamic Access Control wurde eine CIFS-Berechtigung mit der Identität eines Sicherheitprinzipals (des Benutzers) und der Mitgliedschaft in einer Windows-Gruppe ausgestattet. Mit der Dynamic Access Control werden drei weitere Arten von Informationen zu den Anmeldeinformationsinformationen, Geräteansprüchen und Benutzeransprüchen hinzugefügt:

- Geräteidentität

  Analog zu den Identitätsinformationen des Benutzers, außer es handelt sich um die Identität und die Gruppenmitgliedschaft des Geräts, von dem sich der Benutzer anmeldet.

- Geräteforderungen

  Behauptungen über einen Sicherheitprinzipal des Geräts. Ein Geräteanspruch kann beispielsweise sein, dass er Mitglied einer bestimmten Organisationseinheit ist.

- Benutzerforderungen

  Behauptungen zu einem Sicherheitprinzipal des Benutzers. Beispielsweise kann eine Benutzerforderung sein, dass ihr AD Konto Mitglied einer bestimmten Organisationseinheit ist.

Zentrale Zugriffsrichtlinien

Zentrale Zugriffsrichtlinien für Dateien ermöglichen Unternehmen die zentrale Bereitstellung und Verwaltung von Autorisierungsrichtlinien, die bedingte Ausdrücke mit Benutzergruppen, Benutzerforderungen, Geräteforderungen und Ressourceneigenschaften beinhalten.

Zum Beispiel muss ein Benutzer zum Zugriff auf Daten mit großen geschäftlichen Auswirkungen ein Vollzeit-Mitarbeiter sein und nur über ein gemanagtes Gerät auf die Daten zugreifen können. Zentrale Zugriffsrichtlinien werden in Active Directory definiert und über den GPO-Mechanismus auf Dateiserver verteilt.

Zentrale Zugriffsrichtlinien-Staging mit erweitertem Auditing

Zentrale Zugriffsrichtlinien können „`steed`“ sein, in diesem Fall werden sie während der Dateizugriffskontrollen auf „`Was-wäre-wenn`“ geprüft. Die Ergebnisse dessen, was passiert wäre, wenn die Richtlinie wirksam wäre und wie sich diese von den derzeit konfigurierten unterscheidet, werden als Audit-Ereignis protokolliert. Auf diese Weise können Administratoren mithilfe von Audit-Ereignisprotokollen die Auswirkungen einer Änderung der Zugriffsrichtlinie untersuchen, bevor diese tatsächlich eingesetzt wird. Nachdem Sie die Auswirkungen einer Änderung der Zugriffsrichtlinien evaluiert haben, kann die Richtlinie über Gruppenrichtlinienobjekte zu den gewünschten SVMs implementiert werden.

Verwandte Informationen

Unterstützte Gruppenrichtlinienobjekte

Werden Gruppenrichtlinienobjekte auf CIFS-Server angewendet

Aktivieren oder Deaktivieren der GPO-Unterstützung auf einem CIFS-Server

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Konfiguration von zentralen Zugriffsrichtlinien zur Sicherung von Daten auf CIFS-Servern

Anzeigen von Informationen zur Dynamic Access Control-Sicherheit

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

Unterstützte Dynamic Access Control-Funktionen

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

Wird für Dynamic Access Control unterstützt

ONTAP unterstützt die folgenden Funktionen, wenn die dynamische Zugriffssteuerung auf dem CIFS-Server

aktiviert ist:

Funktionalität	Kommentare
Forderungen an das Filesystem	Forderungen sind einfache Name- und Wertpaare, die die Wahrheit über einen Benutzer angeben. Benutzerkennung enthält Informationen zu Ansprüchen, und Sicherheitsbeschreibungen in Dateien können Zugriffsprüfungen durchführen, die Schadenprüfungen umfassen. So erhalten Administratoren mehr Kontrolle darüber, wer auf Dateien zugreifen kann.
Bedingte Ausdrücke zu Dateizugriffsprüfungen	Beim Ändern der Sicherheitsparameter einer Datei können Benutzer willkürlich komplexe bedingte Ausdrücke zum Sicherheitsdeskriptor der Datei hinzufügen. Der bedingte Ausdruck kann Prüfungen für Forderungen enthalten.
Zentrale Steuerung des Dateizugriffs über zentrale Zugriffsrichtlinien	Zentrale Zugriffsrichtlinien sind eine Art ACL, die in Active Directory gespeichert ist und mit einer Datei gekennzeichnet werden kann. Der Zugriff auf die Datei wird nur gewährt, wenn die Zugriffskontrollen sowohl des Sicherheitsdeskriptors auf der Festplatte als auch der getaggten zentralen Zugriffsrichtlinie den Zugriff ermöglichen.auf diese Weise können Administratoren den Zugriff auf Dateien von einem zentralen Speicherort (AD) aus steuern, ohne den Sicherheitsdeskriptor auf der Festplatte ändern zu müssen.
Zentrale Zugriffsrichtlinien-Staging	Fügt die Möglichkeit hinzu, Sicherheitsänderungen auszuprobieren, ohne den tatsächlichen Dateizugriff zu beeinträchtigen, indem Sie „`staging`“ eine Änderung der zentralen Zugriffsrichtlinien vornehmen und die Auswirkung der Änderung in einem Audit-Bericht sehen.
Unterstützung zum Anzeigen von Informationen zur Sicherheit zentraler Zugriffsrichtlinien über die ONTAP-CLI	Erweitert die `vserver security file-directory show` Befehl zum Anzeigen von Informationen über angewandte zentrale Zugriffsrichtlinien.
Verfolgung der Sicherheit, einschließlich zentraler Zugriffsrichtlinien	Erweitert die `vserver security trace` Befehlsfamilie, um Ergebnisse anzuzeigen, die Informationen zu angewandten zentralen Zugriffsrichtlinien enthalten.

Nicht unterstützt für Dynamic Access Control

ONTAP unterstützt die folgenden Funktionen nicht, wenn die dynamische Zugriffssteuerung auf dem CIFS-

Server aktiviert ist:

Funktionalität	Kommentare
Automatische Klassifizierung von NTFS-Dateisystemobjekten	Dies ist eine Erweiterung der Windows File Classification Infrastructure, die in ONTAP nicht unterstützt wird.
Erweiterte Audits außer der zentralen Zugriffsrichtlinien-Staging	Für erweiterte Audits wird nur das Staging von zentralen Zugriffsrichtlinien unterstützt.

Überlegungen bei der Verwendung von Dynamic Access Control und zentralen Zugriffsrichtlinien mit CIFS-Servern

Bei der Verwendung von Dynamic Access Control (DAC) und zentralen Zugriffsrichtlinien zum Sichern von Dateien und Ordnern auf CIFS-Servern müssen Sie bestimmte Überlegungen beachten.

Der NFS-Zugriff kann auf Root verweigert werden, wenn eine Richtlinienregel auf Domain\Administrator-Benutzer angewendet wird

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

Statt eine Regel auf den Domänenadministrator\anzuwenden, sollten Sie die Regel auf eine Gruppe mit Administratorrechten anwenden, z. B. die Gruppe Domain\Administratoren. Auf diese Weise können Sie Root dem Domain\Administrator-Konto zuordnen, ohne dass Root von diesem Problem betroffen ist.

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

Es ist möglich, dass Ressourcen innerhalb des CIFS-Servers zentrale Zugriffsrichtlinien auf sie angewendet werden, aber wenn der CIFS-Server die SID der zentralen Zugriffsrichtlinie verwendet, um zu versuchen, Informationen aus Active Directory abzurufen, stimmt die SID keiner vorhandenen zentralen Zugriffsrichtlinien-SIDs in Active Directory überein. Unter diesen Umständen wendet der CIFS-Server die lokale Standard-Recovery-Richtlinie für diese Ressource an.

Die lokale Standard-Wiederherstellungsrichtlinie ermöglicht den Zugriff der BUILTIN\-Administratorgruppe des CIFS-Servers auf diese Ressource.

Aktiviert oder deaktiviert die Übersicht über die dynamische Zugriffskontrolle

Die Option, mit der Sie Dynamic Access Control (DAC) zum Sichern von Objekten auf Ihrem CIFS-Server verwenden können, ist standardmäßig deaktiviert. Sie müssen die Option aktivieren, wenn Sie die dynamische Zugriffssteuerung auf Ihrem CIFS-Server verwenden möchten. Wenn Sie später entscheiden, dass Sie Dynamic Access Control nicht zum Sichern von auf dem CIFS-Server gespeicherten Objekten verwenden möchten, können Sie die Option deaktivieren.

Über diese Aufgabe

Ist die Dynamic Access Control aktiviert, kann das Dateisystem ACLs mit Einträgen im Zusammenhang mit Dynamic Access Control enthalten. Wenn die dynamische Zugriffskontrolle deaktiviert ist, werden die aktuellen Einträge für die dynamische Zugriffskontrolle ignoriert und neue Einträge werden nicht zugelassen.

Diese Option ist nur auf der erweiterten Berechtigungsebene verfügbar.

Schritt

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

Wenn Sie die dynamische Zugriffskontrolle benötigen,	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 Administratorberechtigungsebene: `set -privilege admin`

Verwandte Informationen

Konfiguration von zentralen Zugriffsrichtlinien zur Sicherung von Daten auf CIFS-Servern

Managen Sie ACLs, die dynamische Zugriffssteuerung enthalten, wenn die dynamische Zugriffskontrolle deaktiviert ist

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

Über diese Aufgabe

Nachdem die Dynamic Access Control deaktiviert ist, können Sie vorhandene nicht-dynamische Access Control Aces nicht entfernen oder neue nicht-dynamische Access Control Aces hinzufügen, bis Sie die vorhandenen Dynamic Access Control Aces entfernt haben.

Sie können das jeweils verwendete Tool zum Verwalten von ACLs verwenden, um diese Schritte durchzuführen.

Schritte

1. Legen Sie fest, welche Dynamic Access Control Aces auf die Ressource angewendet werden.
2. Entfernen Sie die Dynamic Access Control Aces aus der Ressource.
3. Hinzufügen oder Entfernen von nicht-dynamischen Zugriffssteuerungsaces wie gewünscht aus der Ressource.

Konfiguration von zentralen Zugriffsrichtlinien zur Sicherung von Daten auf CIFS-Servern

Sie müssen verschiedene Schritte Unternehmen, um den Zugriff auf Daten auf dem CIFS-Server mithilfe von zentralen Zugriffsrichtlinien zu sichern. Hierzu zählen die Aktivierung von Dynamic Access Control (DAC) auf dem CIFS-Server, die Konfiguration zentraler Zugriffsrichtlinien in Active Directory, die Anwendung der zentralen Zugriffsrichtlinien auf Active Directory-Container mit GPOs, Und Aktivieren der Gruppenrichtlinienobjekte auf dem CIFS-Server.

Bevor Sie beginnen

- Active Directory muss so konfiguriert sein, dass zentrale Zugriffsrichtlinien verwendet werden.
- Sie müssen über ausreichende Zugriffsmöglichkeiten auf den Active Directory-Domänencontrollern verfügen, um zentrale Zugriffsrichtlinien zu erstellen und Gruppenrichtlinienobjekte zu erstellen und auf die Container anzuwenden, die die CIFS-Server enthalten.
- Sie müssen über ausreichenden administrativen Zugriff auf der Storage Virtual Machine (SVM) verfügen, um die erforderlichen Befehle auszuführen.

Über diese Aufgabe

Zentrale Zugriffsrichtlinien werden definiert und auf Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, GPOs) in Active Directory angewendet. Anweisungen zur Konfiguration zentraler Zugriffsrichtlinien und Gruppenrichtlinienobjekte finden Sie in der Microsoft TechNet-Bibliothek.

"Microsoft TechNet-Bibliothek"

Schritte

1. Aktivieren Sie Dynamic Access Control auf der SVM, wenn sie nicht bereits über die aktiviert ist `vserver cifs options modify` Befehl.

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

2. Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, Gruppenrichtlinienobjekte) auf dem CIFS-Server aktivieren, wenn sie nicht bereits mit dem aktiviert sind `vserver cifs group-policy modify` Befehl.

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

3. Zentrale Zugriffsregeln und zentrale Zugriffsrichtlinien für Active Directory erstellen
4. Erstellen eines Gruppenrichtlinienobjekts (GPO), um die zentralen Zugriffsrichtlinien in Active Directory zu implementieren.
5. Wenden Sie das GPO auf den Container an, in dem sich das CIFS-Servercomputer-Konto befindet.
6. Aktualisieren Sie manuell die Gruppenrichtlinienobjekte, die auf den CIFS-Server angewendet wurden, indem Sie auf das verwenden `vserver cifs group-policy update` Befehl.

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

7. Überprüfen Sie, ob die GPO Central Access Policy auf die Ressourcen auf dem CIFS-Server angewendet wird. Verwenden Sie dazu die `vserver cifs group-policy show-applied` Befehl.

   Das folgende Beispiel zeigt, dass die Standard-Domänenrichtlinie zwei zentrale Zugriffsrichtlinien hat, 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

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Aktivieren oder Deaktivieren der Dynamic Access Control

Zeigt Informationen zur Dynamic Access Control-Sicherheit an

Sie können Informationen zur Dynamic Access Control (DAC)-Sicherheit auf NTFS-Volumes und zu Daten mit NTFS-effektiver Sicherheit für gemischte Security-Volumes anzeigen. Dazu gehören Informationen über bedingte Asse, Ressourcen-Asse und zentrale Zugangspolitik Aces. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

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

Schritt

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

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Wobei Ausgabe mit Gruppen- und Benutzer-SIDs angezeigt wird	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Über die Datei- und Verzeichnissicherheit für Dateien und Verzeichnisse, in denen die hexadezimale Bitmaske in das Textformat übersetzt wird	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen zu Dynamic Access Control über den Pfad angezeigt `/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

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Überlegungen zur Dynamic Access Control zurücksetzen

Sie sollten sich dessen bewusst sein, was beim Zurücksetzen auf eine Version von ONTAP passiert, die die dynamische Zugriffssteuerung (Dynamic Access Control, DAC) nicht unterstützt, und was Sie vor und nach dem Zurücksetzen tun müssen.

Wenn Sie das Cluster auf eine Version von ONTAP zurücksetzen möchten, die keine dynamische Zugriffssteuerung unterstützt, und die dynamische Zugriffssteuerung ist auf einer oder mehreren Storage Virtual Machines (SVMs) aktiviert, müssen Sie vor dem Zurücksetzen die folgenden Schritte ausführen:

- Sie müssen Dynamic Access Control auf allen SVMs deaktivieren, auf denen sie auf dem Cluster aktiviert ist.
- Sie müssen alle Überwachungskonfigurationen auf dem Cluster ändern, die den enthalten `cap-staging` Ereignistyp, um nur das zu verwenden `file-op` Ereignistyp.

Sie müssen einige wichtige Überlegungen zum Zurücksetzen von Dateien und Ordnern mit Dynamic Access Control Aces verstehen und ausführen:

- Wenn der Cluster zurückgesetzt wird, werden vorhandene Dynamic Access Control Aces nicht entfernt. Diese werden jedoch bei der Überprüfung des Dateizugriffs ignoriert.
- Da Dynamic Access Control Aces nach der Reversion ignoriert werden, wird der Zugriff auf Dateien mit Dynamic Access Control Aces geändert.

  Dadurch konnten die Benutzer auf Dateien zugreifen, die zuvor nicht oder gar nicht auf Dateien zugreifen konnten.

- Sie sollten nicht-dynamische Zugriffssteuerung Aces auf die betroffenen Dateien anwenden, um ihre vorherige Sicherheitsstufe wiederherzustellen.

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

> Da Dynamic Access Control Aces nach der Reversion ignoriert werden, ist es nicht erforderlich, dass Sie sie entfernen, wenn Sie nicht-dynamische Access Control Aces auf die betroffenen Dateien anwenden. Sie können sie jedoch bei Bedarf manuell entfernen.

Hier finden Sie weitere Informationen zur Konfiguration und Verwendung von Dynamic Access Control und zentralen Zugriffsrichtlinien

Weitere Ressourcen unterstützen Sie bei der Konfiguration und Verwendung von Dynamic Access Control und zentralen Zugriffsrichtlinien.

Informationen zum Konfigurieren von Dynamic Access Control und zentralen Zugriffsrichtlinien in Active Directory finden Sie in der Microsoft TechNet-Bibliothek.

"Microsoft TechNet: Dynamic Access Control Scenario Overview"

"Microsoft TechNet: Zentrales Zugriffspolitik-Szenario"

Mithilfe der folgenden Referenzen können Sie den SMB-Server für die Verwendung und Unterstützung von Dynamic Access Control und zentralen Zugriffsrichtlinien konfigurieren:

- **Verwendung von GPOs auf dem SMB-Server**

  Werden Gruppenrichtlinienobjekte auf SMB-Server angewendet

- **Konfiguration der NAS-Prüfung auf dem SMB-Server**

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

Sicherer SMB-Zugriff über Exportrichtlinien

Verwendung von Exportrichtlinien mit SMB-Zugriff

Wenn Exportrichtlinien für SMB-Zugriff auf dem SMB-Server aktiviert sind, werden Exportrichtlinien verwendet, um den Zugriff auf SVM-Volumes durch SMB-Clients zu steuern. Um auf Daten zuzugreifen, können Sie eine Exportrichtlinie erstellen, über die SMB-Zugriff möglich ist, und die Richtlinie dann den Volumes mit SMB-Freigaben zuordnen.

Eine Exportrichtlinie hat eine oder mehrere Regeln angewendet, die festlegen, welche Clients Zugriff auf die Daten haben und welche Authentifizierungsprotokolle für schreibgeschützten und schreibgeschützten Zugriff unterstützt werden. Sie können Exportrichtlinien konfigurieren, um allen Clients, einem Subnetz von Clients oder einem bestimmten Client den Zugriff über SMB zu ermöglichen, und um die Authentifizierung über Kerberos-Authentifizierung, NTLM-Authentifizierung oder sowohl Kerberos- als auch NTLM-Authentifizierung zu ermöglichen, wenn der schreibgeschützten und der Lese-/Schreibzugriff auf Daten bestimmt wird.

Nach der Verarbeitung aller auf die Exportrichtlinie angewandten Exportregeln kann ONTAP bestimmen, ob dem Client der Zugriff gewährt wird und welche Zugriffsstufe gewährt wird. Exportregeln gelten für Clientcomputer, nicht für Windows-Benutzer und -Gruppen. Exportregeln ersetzen die Authentifizierung und Autorisierung von Windows-Benutzern und -Gruppen nicht. Exportregeln bieten zusätzlich zu Freigabeberechtigungen und Zugriffsberechtigungen eine weitere Zugriffsebene.

Sie ordnen jedem Volume genau eine Exportrichtlinie zu, um den Client-Zugriff auf das Volume zu konfigurieren. Jede SVM kann mehrere Exportrichtlinien enthalten. Dies ermöglicht Ihnen bei SVMs mit mehreren Volumes folgende Aufgaben:

- Jedem Volume der SVM sollten für jedes Volume in der SVM unterschiedliche Exportrichtlinien zugewiesen werden, um für jedes Volume in der SVM eine individuelle Client-Zugriffskontrolle zu ermöglichen.
- Weisen Sie für eine identische Client-Zugriffskontrolle dieselbe Exportrichtlinie mehreren Volumes der SVM zu, ohne für jedes Volume eine neue Exportrichtlinie erstellen zu müssen.

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

Sie können Regeln konfigurieren, die Zugriff auf NFS- und SMB-Hosts gewähren, und diese Regel einer Exportrichtlinie zuordnen. Diese kann dann dem Volume zugeordnet werden, das Daten enthält, auf die sowohl NFS- als auch SMB-Hosts zugreifen müssen. Falls es einige Volumes gibt, auf denen nur SMB-Clients Zugriff benötigen, können Sie eine Exportrichtlinie mit Regeln konfigurieren, die nur den Zugriff über das SMB-Protokoll gestattet. Darüber hinaus wird nur Kerberos oder NTLM (oder beides) für die Authentifizierung für Read-Only- und Write-Zugriff verwendet. Die Exportrichtlinie wird dann den Volumes zugeordnet, auf denen nur SMB-Zugriff gewünscht wird.

Wenn Exportrichtlinien für SMB aktiviert sind und ein Client eine Zugriffsanfrage stellt, die von der entsprechenden Exportrichtlinie nicht zulässig ist, schlägt die Anforderung mit einer Meldung, die eine Berechtigung verweigert hat, fehl. Wenn ein Client keine Regeln in der Exportrichtlinie des Volumes erfüllt, wird der Zugriff verweigert. Wenn eine Exportrichtlinie leer ist, werden alle Zugriffe implizit verweigert. Dies gilt auch dann, wenn die Freigabe- und Dateiberechtigungen ansonsten den Zugriff erlauben würden. Das bedeutet, dass Sie Ihre Exportrichtlinie so konfigurieren müssen, dass bei Volumes mit SMB-Freigaben Folgendes minimal zulässig ist:

- Zugriff auf alle Clients oder die entsprechende Untergruppe von Clients zulassen
- Zugriff über SMB zulassen
- Mit Kerberos- oder NTLM-Authentifizierung (oder beides) ist ein angemessener Lese- und Schreibzugriff möglich.

Erfahren Sie mehr über "Konfigurieren und Verwalten von Exportrichtlinien".

Wie Exportregeln funktionieren

Exportregeln sind die funktionalen Elemente einer Exportrichtlinie. Exportregeln stimmen die Client-Zugriffsanforderungen auf ein Volume ab. Dabei werden bestimmte Parameter verwendet, die Sie konfigurieren, um zu bestimmen, wie die Clientzugriffsanforderungen verarbeitet werden sollen.

Eine Exportrichtlinie muss mindestens eine Exportregel enthalten, um den Zugriff auf Clients zu ermöglichen. Wenn eine Exportrichtlinie mehrere Regeln enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportrichtlinie angezeigt werden. Die Regelreihenfolge wird durch die Indexnummer der Regel vorgegeben. Stimmt eine Regel mit einem Client überein, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Stimmen keine Regeln überein, wird dem Client der Zugriff verweigert.

Sie können Exportregeln konfigurieren, um Clientzugriffsberechtigungen anhand der folgenden Kriterien zu ermitteln:

- Das Dateizugriffsprotokoll, das vom Client verwendet wird, der die Anforderung sendet, z. B. NFSv4 oder SMB.
- Eine Client-ID, z. B. Hostname oder IP-Adresse.

  Die maximale Größe für die `-clientmatch` Das Feld darf 4096 Zeichen enthalten.

- Der vom Client zum Authentifizieren verwendete Sicherheitstyp, z. B. Kerberos v5, NTLM oder AUTH_SYS.

Wenn in einer Regel mehrere Kriterien angegeben sind, muss der Client alle Kriterien erfüllen, damit die Regel angewendet werden kann.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

Die Client-Zugriffsanforderung wird mithilfe des NFSv3-Protokolls versendet, 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 Clientabgleich fehl, und diese Regel gilt nicht für diesen Client.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

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

Das Client-Zugriffsprotokoll stimmt überein, und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientabgleich erfolgreich, und diese Regel gilt für diesen Client. Der Client erhält unabhängig vom Sicherheitstyp Lese-/Schreibzugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den 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 authentifiziert mit Kerberos v5.

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

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat. Client #2 erhält keinen Lese-/Schreibzugriff.

Beispiele für Exportrichtlinien, die den Zugriff über SMB einschränken oder zulassen

Die Beispiele zeigen, wie man Richtlinien für den Export erstellt, die den Zugriff auf SMB für eine SVM einschränken oder zulassen, deren Exportrichtlinien für SMB-Zugriff aktiviert sind.

Exportrichtlinien für SMB-Zugriff sind standardmäßig deaktiviert. Sie müssen Richtlinien für den Export konfigurieren, die den Zugriff über SMB einschränken oder zulassen, nur wenn Sie Exportrichtlinien für SMB-Zugriff aktiviert haben.

Exportregel nur für SMB-Zugriff

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „`vs1`“ erstellt, die die folgende

Konfiguration hat:

- Richtlinienname: Ziff1
- Indexnummer: 1
- Client Match: Entspricht nur Clients im 192.168.1.0/24 Netzwerk
- Protokoll: Nur SMB-Zugriff möglich
- Schreibgeschützter Zugriff: Auf Clients mit NTLM- oder Kerberos-Authentifizierung
- Lese-Schreib-Zugriff für Clients, die Kerberos-Authentifizierung verwenden

```
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

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „` vs1`“ erstellt, die die folgende Konfiguration hat:

- Policy Name: Cifsnfs1
- Indexnummer: 2
- Client-Match: Entspricht allen Clients
- Protokoll: SMB- und NFS-Zugriff
- Schreibgeschützter Zugriff: Für alle Clients
- Lese-Schreibzugriff: Für Clients, die Kerberos (NFS und SMB) oder NTLM-Authentifizierung (SMB) verwenden
- Zuordnung für UNIX-Benutzer-ID 0 (Null): Zugeordnet zu Benutzer-ID 65534 (die typischerweise dem Benutzernamen niemand zugeordnet ist)
- SUID und sgid Access: Ermöglicht

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Exportregel für SMB-Zugriff nur mit NTLM

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „`vs1`“ erstellt, die die folgende Konfiguration hat:

- Policy-Name: Ntlm1
- Indexnummer: 1
- Client-Match: Entspricht allen Clients
- Protokoll: Nur SMB-Zugriff möglich
- Schreibgeschützter Zugriff: Nur für Clients, die NTLM verwenden

- Lese-Schreib-Zugriff: Nur für Clients, die NTLM verwenden

> Wenn Sie die schreibgeschützte Option oder die Lese-Schreib-Option für NTLM-Only-Zugriff konfigurieren, müssen Sie IP-address-basierte Einträge in der Client-Match-Option verwenden. Andernfalls erhalten Sie `access denied` Fehler. Dies liegt daran, dass ONTAP Kerberos-Dienst-Principal-Namen (SPN) verwendet, wenn ein Hostname verwendet wird, um die Zugriffsrechte des Clients zu überprüfen. NTLM-Authentifizierung unterstützt keine SPN-Namen.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Aktivieren oder Deaktivieren von Exportrichtlinien für SMB-Zugriff

Sie können Exportrichtlinien für 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

Nachfolgend sind die Anforderungen für die Aktivierung von Exportrichtlinien für SMB aufgeführt:

- Der Client muss über einen „`PTR`“-Datensatz in DNS verfügen, bevor Sie die Exportregeln für diesen Client erstellen.
- Wenn die SVM Zugriff auf NFS-Clients bietet, ist ein zusätzlicher Satz von „`A`“- und „`PTR`“-Datensätzen erforderlich, und der Hostname, den Sie für NFS-Zugriff verwenden möchten, unterscheidet sich vom CIFS-Servernamen.

Über diese Aufgabe

Beim Einrichten eines neuen CIFS-Servers auf Ihrer SVM ist die Verwendung von Exportrichtlinien für SMB-Zugriff standardmäßig deaktiviert. Sie können Exportrichtlinien für SMB-Zugriffe aktivieren, wenn Sie den Zugriff auf Basis des Authentifizierungsprotokoll oder anhand von Client-IP-Adressen oder Host-Namen steuern möchten. Die Exportrichtlinien für SMB-Zugriff können jederzeit aktiviert oder deaktiviert werden.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `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 Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Im folgenden Beispiel können Exportrichtlinien verwendet werden, um den Zugriff von SMB-Clients auf Ressourcen von SVM vs1 zu kontrollieren:

```
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
```

Sicherer Dateizugriff über Storage-Level Access Guard

Sicherer Dateizugriff über Storage-Level Access Guard

Zusätzlich zur Sicherung des Zugriffs durch native File-Level und die Sicherheit für Export und Freigabe können Sie den Storage-Level Access Guard konfigurieren, eine dritte Sicherheitsschicht, die von ONTAP auf Volume-Ebene angewendet wird. Storage-Level Access Guard gilt für den Zugriff von allen NAS-Protokollen auf das Storage-Objekt, auf das es angewendet wird.

Es werden nur NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP auf UNIX-Benutzern Sicherheitsüberprüfungen für den Zugriff auf Daten auf Volumes durchführen kann, für die der Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der auch Eigentümer des Volumes ist, zuordnen.

Verhalten des Access Guard auf Storage-Ebene

- 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 für den Speicherlevel Access Guard unterliegen, ist keine Vererbung durch die Ausbreitung erforderlich.

- Sie können den Storage-Level Access Guard so konfigurieren, dass er nur auf Dateien, nur Verzeichnisse oder auf Dateien und Verzeichnisse innerhalb eines Volumes angewendet wird.
  - Datei- und Verzeichnissicherheit

    Gilt für jedes Verzeichnis und jede Datei im Storage-Objekt. Dies ist die Standardeinstellung.

  - Dateisicherheit

    Gilt für jede Datei im Storage-Objekt. Die Anwendung dieser Sicherheit hat keinen Einfluss auf den Zugriff oder die Prüfung von Verzeichnissen.

  - Verzeichnissicherheit

    Gilt für jedes Verzeichnis im Storage-Objekt. Die Anwendung dieser Sicherheit hat keinen Einfluss auf den Zugriff oder die Prüfung von Dateien.

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

Es wird niemals zusätzliche Zugriffsrechte geben.

- Wenn Sie die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Storage-Level Access Guard nicht angezeigt.

  Sie wird auf Storage-Objektebene angewendet und in den Metadaten gespeichert, die zur Bestimmung der effektiven Berechtigungen verwendet werden.

- Sicherheit auf Storage-Ebene kann nicht durch einen Client entzogen werden, selbst wenn ein System-Administrator (Windows oder UNIX) dies durchführt.

  Dieses Design lässt sich nur von Storage-Administratoren ändern.

- Sie können Storage-Level Access Guard auf Volumes mit NTFS oder einem gemischten Sicherheitsstil anwenden.
- Sie können Access Guard auf Storage-Ebene auf Volumes mit UNIX-Sicherheitsstil anwenden, solange für die SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist.
- Wenn Volumes unter einem Volume-Verbindungspfad gemountet werden und wenn Access Guard auf Storage-Ebene auf diesem Pfad vorhanden ist, wird sie nicht auf Volumes übertragen, die darunter angehängt sind.
- Der Sicherheitsdeskriptor für den Storage-Level Access Guard wird mit SnapMirror Datenreplizierung und SVM-Replizierung repliziert.
- Es gibt spezielle Dispensierung für Virenscanner.

  Der Zugriff auf diese Server ist auf die Anzeige von Dateien und Verzeichnissen gestattet, selbst wenn der Access Guard auf Storage-Ebene den Zugriff auf das Objekt verweigert.

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

Reihenfolge der Zugriffskontrollen

Der Zugriff auf eine Datei oder ein Verzeichnis wird durch den kombinierten Effekt der Export- oder Freigabeberechtigungen, der auf Volumes festgelegten Zugriffsschutz auf Storage-Ebene und der nativen Dateiberechtigungen auf Dateien und/oder Verzeichnisse bestimmt. Alle Sicherheitsstufen werden ausgewertet, um festzustellen, welche effektiven Berechtigungen eine Datei oder ein Verzeichnis besitzt. Die Sicherheitszugriffskontrollen werden in folgender Reihenfolge durchgeführt:

1. SMB-Freigabe- oder NFS-Berechtigungen für den Export
2. Storage-Level Access Guard
3. NTFS-Datei-/Ordnerzugangskontrolllisten (ACLs), NFSv4-ACLs oder UNIX-Modus-Bits

Anwendungsfälle für die Verwendung von Storage-Level Access Guard

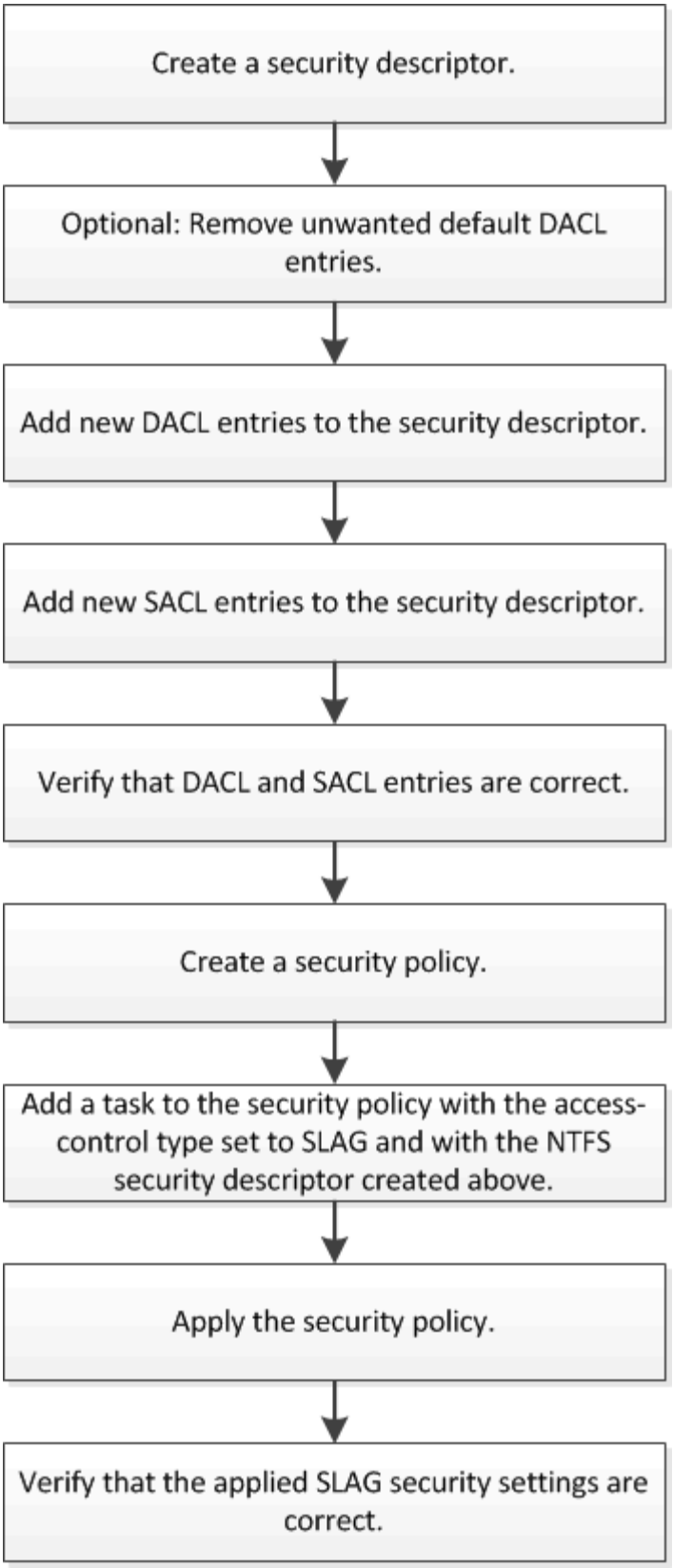
Storage-Level Access Guard bietet zusätzliche Sicherheit auf Storage-Ebene, die nicht von Client-Seite sichtbar ist. Daher kann diese Sicherheit nicht von Benutzern oder Administratoren mit ihren Desktops entzogen werden. In bestimmten Anwendungsfällen ist die Zugriffskontrolle auf Storage-Ebene von Vorteil.

Zu den typischen Anwendungsfällen für diese Funktion zählen folgende Szenarien:

- Schutz geistigen Eigentums durch Auditing und Controlling aller Benutzer` Zugriff auf Storage-Ebene
- Storage für Finanzdienstleister einschließlich Bank- und Handelskonzerne
- Öffentlicher Dienst mit separatem File Storage für einzelne Abteilungen
- Universitäten schützen alle Studentendateien

Workflow zum Konfigurieren der Zugriffsschutz auf Storage-Ebene

Der Workflow zum Konfigurieren von Storage-Level Access Guard (SCHLACKE) verwendet dieselben ONTAP-CLI-Befehle, mit denen Sie NTFS-Dateiberechtigungen und Audit-Richtlinien konfigurieren. Anstatt Datei- und Verzeichniszugriff auf einem festgelegten Ziel zu konfigurieren, konfigurieren Sie LAG auf dem zugewiesenen SVM-Volume (Storage Virtual Machine).



Verwandte Informationen

Konfigurieren Des Zugriffsschutzes Auf Storage-Ebene

Konfigurieren Sie Den Storage-Level Access Guard

Zur Konfiguration des Storage-Level Access Guard auf einem Volume oder qtree müssen Sie verschiedene Schritte befolgen. Access Guard auf Storage-Ebene bietet eine Zugriffssicherheit, die auf Storage-Ebene festgelegt ist. Das Tool bietet Sicherheit, die für alle Zugriffe aus allen NAS-Protokollen auf das Storage-Objekt gilt, auf das es angewendet wurde.

Schritte

1. Erstellen Sie mithilfe des einen Sicherheitsdeskriptor `vserver security file-directory ntfs create` Befehl.

   `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-Zugriffssteuerungseinträgen (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 die Standardeinträge bei der Konfiguration des Speicher-Level Access Guard nicht verwenden möchten, können Sie sie vor dem Erstellen und Hinzufügen eigener Asse zum Sicherheitsdeskriptor entfernen.

2. Entfernen Sie eine der Standard-DACL-Aces aus dem Sicherheitsdeskriptor, den Sie nicht mit der Sicherheit für den Speicherlevel Access Guard konfigurieren möchten:

   a. Entfernen Sie alle unerwünschten DACL-Asse mithilfe des `vserver security file-directory ntfs dacl remove` Befehl.

      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. Stellen Sie sicher, dass die DACL-Aces, die Sie nicht für die Sicherheit des Speicherzugriffsschutzes verwenden möchten, mit dem aus dem Sicherheitsdeskriptor entfernt werden `vserver security file-directory ntfs dacl show` Befehl.

      In diesem Beispiel überprüft die Ausgabe des Befehls, ob drei Standard-DACL-Aces aus dem Sicherheitsdeskriptor entfernt wurden und nur der NT AUTHORITY\SYSTEM Standard-DACL ACE-Eintrag hinterlassen wurde:

      ```
      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. Fügen Sie einen oder mehrere DACL-Einträge zu einem Sicherheitsdeskriptor hinzu, indem Sie das verwenden `vserver security file-directory ntfs dacl add` Befehl.

   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. Fügen Sie einen oder mehrere SACL-Einträge zu einem Sicherheitsdeskriptor hinzu, indem Sie die verwenden `vserver security file-directory ntfs sacl add` Befehl.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei SACL-Asse 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. Überprüfen Sie mithilfe des, ob die DACL- und SACL-Asse richtig konfiguriert sind `vserver security file-directory ntfs dacl show` Und `vserver security file-directory ntfs sacl show` Befehle.

   In diesem Beispiel zeigt der folgende Befehl Informationen über DACL-Einträge für 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 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. Erstellen Sie eine Sicherheitsrichtlinie mithilfe von `vserver security file-directory policy create` Befehl.

   Im folgenden Beispiel wird eine Richtlinie mit dem Namen „`policy1`“ erstellt:

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

7. Überprüfen Sie mithilfe des, ob die Richtlinie richtig konfiguriert ist `vserver security file-directory policy show` Befehl.

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

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

8. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor hinzu, indem Sie die verwenden `vserver security file-directory policy task add` Befehl mit dem `-access-control` Parameter auf gesetzt `slag`.

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

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

   ```
   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. Überprüfen Sie mithilfe des, ob die Aufgabe richtig konfiguriert ist `vserver security file-directory policy task show` Befehl.

   `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. Wenden Sie die Sicherheitsrichtlinie für den Storage-Level Access Guard mithilfe des an `vserver security file-directory apply` Befehl.

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

    Der Auftrag zur Anwendung der Sicherheitsrichtlinie ist geplant.

11. Überprüfen Sie, ob die verwendeten Sicherheitseinstellungen für den Zugriffschutz auf Storage-Ebene mit dem korrekt sind `vserver security file-directory show` Befehl.

    In diesem Beispiel zeigt die Ausgabe des Befehls, dass der Zugriffschutz auf Storage-Ebene auf das NTFS-Volume angewendet wurde `/datavol1`. Obwohl die Standard-DACL, die die volle Kontrolle für alle zulässt, bleibt, schränkt die Sicherheit auf Storage-Ebene den Zugriff auf die in den Einstellungen für den Speicher-Level Access Guard definierten Gruppen ein (und prüft).

    `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

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

Workflow zum Konfigurieren der Zugriffsschutz auf Storage-Ebene

Anzeigen von Informationen zum Speicher-Level Access Guard

Entfernen Des Zugriffsschutzes Auf Storage-Ebene

Effektive SCHLACKE-Matrix

SIE können LAG auf einem Volume oder einem qtree oder beiden konfigurieren. Die SCHLACKE-Matrix definiert, auf welchem Volume oder qtree die SCHLACKE-Konfiguration ist. Sie wird unter verschiedenen in der Tabelle aufgeführten Szenarien angewendet.

	Volumen-SCHLACKE in einem AFS	Volume-LAG IN einer Snapshot Kopie	Qtree SCHLACKE in einem AFS	Qtree LAG IN einer Snapshot Kopie
Volume-Zugriff in einem Access File System (AFS)	JA	NEIN	1. A.	1. A.
Zugriff auf das Volume in einer Snapshot Kopie	JA	NEIN	1. A.	1. A.
Qtree-Zugriff in einem AFS (wenn IM qtree SCHLACKE vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in einem AFS (wenn LAG nicht im qtree vorhanden ist)	JA	NEIN	NEIN	NEIN
Qtree-Zugriff in der Snapshot-Kopie (wenn IM qtree AFS EIN SCHLACKE vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in der Snapshot-Kopie (wenn SCHLACKE nicht im qtree AFS vorhanden ist)	JA	NEIN	NEIN	NEIN

Zeigen Sie Informationen zum Storage-Level Access Guard an

Storage-Level Access Guard ist eine dritte Sicherheitsschicht, die auf einem Volume oder qtree angewendet wird. Die Einstellungen für den Zugriffschutz auf Speicherebene können nicht über das Fenster „Windows-Eigenschaften“ angezeigt werden. Sie müssen die ONTAP-CLI verwenden, um Informationen zur Sicherheit des Zugriffschutzes auf Storage-Ebene anzuzeigen, mit der Sie die Konfiguration validieren oder Probleme beim

Dateizugriff beheben können.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zum Volume oder qtree angeben, dessen Sicherheitsinformationen auf Storage-Level Access Guard angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

Schritt

1. Die Sicherheitseinstellungen der Speicherebene für den Access Guard mit der gewünschten Detailebene anzeigen:

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

Beispiele

Im folgenden Beispiel werden Sicherheitsinformationen auf Speicherebene für das NTFS-Sicherheitsvolumen mit dem Pfad angezeigt `/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
```

Im folgenden Beispiel werden die Informationen der Storage-Level Access Guard zum Volume mit gemischtem Sicherheitsstil auf dem Pfad angezeigt `/datavol5` In SVM vs1. Die oberste Ebene dieses Volumens besitzt effektive UNIX-Sicherheit. Das Volume verfügt über Sicherheit auf Storage-Ebene beim Access Guard.

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

Entfernen Sie Den Storage-Level Access Guard

Sie können Storage-Level Access Guard auf einem Volume oder qtree entfernen, wenn Sie nicht mehr die Zugriffssicherheit auf Storage-Ebene festlegen möchten. Das Entfernen von Speicherebene Access Guard ändert oder entfernt die normale NTFS-Datei- und Verzeichnissicherheit nicht.

Schritte

1. Überprüfen Sie, ob auf dem Volume oder qtree der Storage Level Access Guard konfiguriert ist `vserver security file-directory show` Befehl.

   ```
   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. Entfernen Sie den Storage-Level Access Guard, indem Sie den verwenden `vserver security file-directory remove-slag` Befehl.

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

3. Überprüfen Sie, ob der Storage-Level Access Guard mithilfe des vom Volume oder qtree entfernt wurde `vserver security file-directory show` Befehl.

   ```
   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
```