Konfigurieren Sie SMB mit der CLI

ONTAP 9

NetApp
February 12, 2026

Inhalt

Konfigurieren Sie SMB mit der CLI

Erfahren Sie mehr über die SMB-Konfiguration mit der ONTAP CLI

Mit ONTAP 9 CLI-Befehlen können SMB-Client-Zugriff auf Dateien konfiguriert werden, die sich in einem neuen Volume oder qtree in einer neuen oder vorhandenen SVM befinden.

SMB (Server Message Block) bezieht sich auf moderne Dialekte des CIFS-Protokolls (Common Internet File System). Sie sehen *CIFS* immer noch in der ONTAP Befehlszeilenschnittstelle (CLI) und in OnCommand-Managementtools.

Verwenden Sie diese Verfahren, um den SMB-Zugriff auf ein Volume oder qtree folgendermaßen zu konfigurieren:

- Sie möchten SMB Version 2 oder höher verwenden.
- Es sollen nur SMB-Clients genutzt werden, keine NFS-Clients (keine Multiprotokoll-Konfiguration).
- NTFS-Dateiberechtigungen werden zum Sichern des neuen Volumes verwendet.
- Sie verfügen über Cluster-Administratorrechte, keine SVM-Administratorrechte.

  Zum Erstellen von SVMs und LIFs sind Berechtigungen für Cluster-Administratoren erforderlich. SVM-Administratorberechtigungen reichen für andere SMB-Konfigurationsaufgaben aus.

- Sie möchten die CLI verwenden, nicht System Manager oder ein automatisiertes Scripting Tool.

  Informationen zum Konfigurieren des NAS-Multiprotokollzugriffs mit System Manager finden Sie unter "Stellen Sie NAS Storage für Windows und Linux mit NFS und SMB bereit".

- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.

  Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Informationen über die verschiedenen SMB-Protokollfunktionen von ONTAP finden Sie unter "SMB-Referenzübersicht".

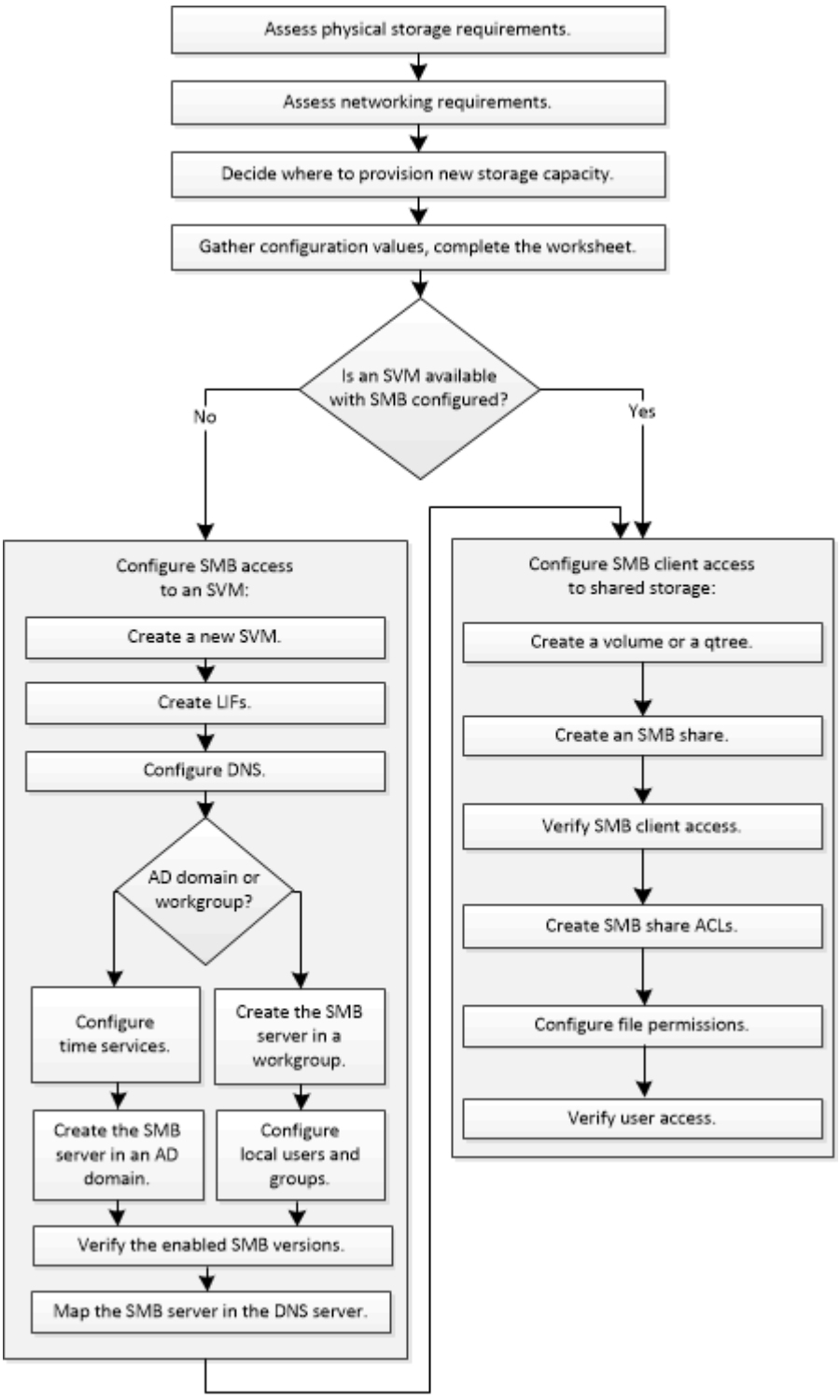
Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Stellen Sie NAS-Storage für Windows Server mithilfe von SMB bereit"
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Übersicht über die SMB-Konfiguration"

ONTAP SMB-Konfigurationsworkflow

Bei der Konfiguration von SMB müssen physische Storage- und Netzwerkanforderungen

geprüft werden, und anschließend ein spezifisch Zielworkflow ausgewählt werden, SMB-Zugriff auf eine neue oder vorhandene SVM konfiguriert oder ein Volume oder qtree zu einer vorhandenen SVM hinzugefügt werden, die bereits vollständig für SMB-Zugriff konfiguriert ist.



Vorbereitung

Anforderungen für physischen ONTAP SMB-Storage bewerten

Bevor Sie SMB-Storage für Clients bereitstellen, müssen Sie sicherstellen, dass in einem vorhandenen Aggregat für das neue Volume ausreichend Speicherplatz vorhanden ist. Ist dies nicht der Fall, können Sie einem vorhandenen Aggregat Festplatten hinzufügen oder ein neues Aggregat des gewünschten Typs erstellen.

Schritte

1. Verfügbaren Speicherplatz in vorhandenen Aggregaten anzeigen: `storage aggregate show`

   Wenn es ein Aggregat mit ausreichend Speicherplatz gibt, tragen Sie seinen Namen in das Arbeitsblatt ein.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                         normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                         normal
6 entries were displayed.
```

2. Falls keine Aggregate mit ausreichend Speicherplatz vorhanden sind, fügen Sie mit dem `storage aggregate add-disks` Befehl Festplatten zu einem vorhandenen Aggregat hinzu oder erstellen Sie mithilfe des `storage aggregate create` Befehls ein neues Aggregat.

Verwandte Informationen

- "Speicheraggregat-Add-Disks"
- "Speicheraggregat erstellen"

ONTAP SMB-Netzwerkanforderungen bewerten

Bevor Sie Clients SMB Storage zur Verfügung stellen, müssen Sie überprüfen, ob das Netzwerk ordnungsgemäß konfiguriert ist, um die SMB-Bereitstellungsanforderungen zu erfüllen.

Bevor Sie beginnen

Die folgenden Cluster-Netzwerkobjekte müssen konfiguriert werden:

- Physische und logische Ports

- Broadcast-Domänen
- Subnetze (falls erforderlich)
- IPspaces (nach Bedarf zusätzlich zum Standard-IPspace)
- Failover-Gruppen (falls erforderlich, zusätzlich zur Standard-Failover-Gruppe für jede Broadcast-Domäne)
- Externe Firewalls

Schritte

1. Zeigt die verfügbaren physischen und virtuellen Ports an: `network port show`
   - Wenn möglich, sollten Sie den Port mit der höchsten Geschwindigkeit für das Datennetzwerk verwenden.
   - Für optimale Performance müssen alle Komponenten im Datennetzwerk dieselbe MTU-Einstellung aufweisen.

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

2. Wenn Sie planen, einen Subnetznamen zum Zuweisen der IP-Adresse und des Netzwerkmaskenwerts für eine LIF zu verwenden, überprüfen Sie, ob das Subnetz vorhanden ist und genügend Adressen verfügbar sind: `network subnet show`

   Erfahren Sie mehr über `network subnet show` in der "ONTAP-Befehlsreferenz".

   Subnetze enthalten einen Pool mit IP-Adressen, die zum selben Layer-3-Subnetz gehören. Subnetze werden mit dem `network subnet create` Befehl erstellt.

   Erfahren Sie mehr über `network subnet create` in der "ONTAP-Befehlsreferenz".

3. Verfügbare IPspaces anzeigen: `network ipspace show`

   Sie können den Standard-IPspace oder einen benutzerdefinierten IPspace verwenden.

   Erfahren Sie mehr über `network ipspace show` in der "ONTAP-Befehlsreferenz".

4. Wenn Sie IPv6-Adressen verwenden möchten, überprüfen Sie, ob IPv6 auf dem Cluster aktiviert ist: `network options ipv6 show`

   Falls erforderlich, können Sie IPv6 mit dem `network options ipv6 modify` Befehl aktivieren.

   Erfahren Sie mehr über `network options ipv6 show` und `network options ipv6 modify` in der "ONTAP-Befehlsreferenz".

Erfahren Sie mehr über die Kapazitätsbereitstellung für SMB-Storage von ONTAP

Bevor Sie ein neues SMB Volume oder einen neuen qtree erstellen, müssen Sie entscheiden, ob dieser in eine neue oder vorhandene SVM platziert werden soll und wie viel Konfiguration die SVM benötigt. Diese Entscheidung bestimmt Ihren Workflow.

Wahlmöglichkeiten

- Wenn Sie ein Volume oder qtree auf einer neuen SVM oder auf einer vorhandenen SVM mit SMB-Aktivierung, aber nicht Konfiguration bereitstellen möchten, führen Sie die Schritte sowohl unter

„Konfigurieren des SMB-Zugriffs auf eine SVM“ als auch „Hinzufügen von Storage-Kapazität zu einer SMB-fähigen SVM“ aus.

Konfigurieren des SMB-Zugriffs auf eine SVM

Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

Sie können eine neue SVM erstellen, wenn eine der folgenden Optionen zutrifft:

- Sie aktivieren SMB auf einem Cluster zum ersten Mal.
- Sie verfügen über vorhandene SVMs in einem Cluster, in dem die SMB-Unterstützung nicht aktiviert werden soll.
- In einem Cluster gibt es mindestens eine SMB-fähige SVMs mit einer der folgenden Verbindungen:
  - Zu einer anderen Active Directory-Gesamtstruktur oder -Arbeitsgruppe.
  - Für einen SMB-Server in einem isolierten Namespace (Szenario mit Mandantenfähigkeit). Wählen Sie diese Option auch, um Storage auf einer vorhandenen SVM mit SMB-Aktivierung, jedoch nicht konfiguriert, bereitzustellen. Dies wäre unter Umständen der Fall, wenn Sie die SVM für SAN-Zugriff erstellt haben oder wenn beim Erstellen der SVM keine Protokolle aktiviert wurden.

Nachdem Sie SMB auf der SVM aktiviert haben, fahren Sie mit der Bereitstellung eines Volume oder qtree fort.

- Wenn Sie ein Volume oder einen qtree auf einer vorhandenen SVM bereitstellen möchten, die vollständig für SMB-Zugriff konfiguriert ist, führen Sie die Schritte unter „Hinzufügen von Storage-Kapazität zu einer SMB-fähigen SVM“ aus.

  Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

ONTAP SMB-Konfigurationsarbeitsblatt

Über das SMB-Konfigurationsarbeitsblatt können Sie die erforderlichen Informationen für die Einrichtung des SMB-Zugriffs für Clients sammeln.

Je nach Ihrer Entscheidung über den Speicherort sollten Sie einen oder beide Abschnitte des Arbeitsblatts ausfüllen:

- Wenn Sie SMB-Zugriff auf eine SVM konfigurieren, sollten Sie beide Abschnitte abschließen.

  Konfigurieren des SMB-Zugriffs auf eine SVM

  Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

- Wenn Sie einer SMB-fähigen SVM Storage-Kapazität hinzufügen, sollten Sie nur den zweiten Abschnitt ausfüllen.

  Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

Erfahren Sie mehr über die Parameter im "ONTAP-Befehlsreferenz".

Konfigurieren des SMB-Zugriffs auf eine SVM

Parameter zum Erstellen einer SVM

Sie geben diese Werte mit dem `vserver create` Befehl an, wenn Sie eine neue SVM erstellen. Erfahren Sie mehr über `vserver create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Einen Namen, den Sie für die neue SVM angeben, der entweder ein vollständig qualifizierter Domain-Name (FQDN) ist, oder der einer anderen Konvention folgt, die eindeutige SVM-Namen in einem Cluster durchsetzt.	
`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichend Speicherplatz für neue SMB-Storage-Kapazität.	
`-rootvolume`	Ein eindeutiger Name für das SVM-Root-Volume.	
`-rootvolume-security-style`	Verwenden Sie den NTFS-Sicherheitsstil für die SVM.	`ntfs`
`-language`	Verwenden Sie die Standardeinstellung für die Sprache in diesem Workflow.	`C.UTF-8`
`ipspace`	Optional: IPspaces sind unterschiedliche IP-Adressbereiche, in denen SVMs sich befinden.	

Parameter zur Erstellung eines LIF

Sie geben diese Werte `network interface create` beim Erstellen von LIFs mit dem Befehl an. Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-lif`	Einen Namen, den Sie für das neue LIF angeben.	
`-role`	Verwenden Sie die LIF-Rolle der Daten in diesem Workflow.	`data`
`-data-protocol`	Verwenden Sie in diesem Workflow nur das SMB-Protokoll.	`cifs`

Feld	Beschreibung	Ihr Wert
`-home-node`	Der Node, zu dem das LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird. Erfahren Sie mehr über `network interface revert` in der "ONTAP-Befehlsreferenz".	
`-home-port`	Der Port oder die Schnittstellengruppe, zu dem das LIF zurückgegeben wird, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.	
`-address`	Die IPv4- oder IPv6-Adresse auf dem Cluster, die für den Datenzugriff durch die neue LIF verwendet wird.	
`-netmask`	Netzwerkmaske und Gateway für LIF.	
`-subnet`	Ein Pool mit IP-Adressen. Wird anstelle von `-address` und verwendet `-netmask`, um Adressen und Netzmasken automatisch zuzuweisen.	
`-firewall-policy`	Verwenden Sie in diesem Workflow die standardmäßige Richtlinie für die Daten-Firewall.	`data`
`-auto-revert`	Optional: Gibt an, ob eine Daten-LIF automatisch auf ihren Home-Node beim Start oder unter anderen Umständen zurückgesetzt wird. Die Standardeinstellung ist `false`.	

Parameter für DNS Host Name Auflösung

Sie geben diese Werte mit dem `vserver services name-service dns create` Befehl an, wenn Sie DNS konfigurieren. Erfahren Sie mehr über `vserver services name-service dns create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-domains`	Bis zu fünf DNS-Domain-Namen	
`-name-servers`	Bis zu drei IP-Adressen für jeden DNS-Namenserver.	

Einrichten eines SMB-Servers in einer Active Directory-Domäne

Parameter für die Konfiguration des Zeitdienstes

Sie geben diese Werte mit dem `cluster time-service ntp server create` Befehl an, wenn Sie Zeitdienste konfigurieren. Erfahren Sie mehr über `cluster time-service ntp server create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-server`	Der Hostname oder die IP-Adresse des NTP-Servers für die Active Directory-Domäne.	

Parameter zum Erstellen eines SMB-Servers in einer Active Directory-Domäne

Sie geben diese Werte mit dem `vserver cifs create` Befehl an, wenn Sie einen neuen SMB-Server erstellen und Domäneninformationen angeben. Erfahren Sie mehr über `vserver cifs create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der der SMB-Server erstellt werden soll.	
`-cifs-server`	Der Name des SMB-Servers (bis zu 15 Zeichen).	
`-domain`	Der vollständig qualifizierte Domänenname (FQDN) der Active Directory-Domäne, der mit dem SMB-Server verknüpft werden soll.	
`-ou`	Optional: Die Organisationseinheit innerhalb der Active Directory-Domäne, die mit dem SMB-Server verknüpft werden soll. Standardmäßig ist dieser Parameter auf CN=Computer eingestellt.	

Feld	Beschreibung	Ihr Wert
`-netbios-aliases`	Optional: Eine Liste von NetBIOS-Aliasen, bei denen es sich um alternative Namen zum SMB-Servernamen handelt.	
`-comment`	Optional: Ein Textkommentar für den Server. Windows-Clients können diese SMB-Serverbeschreibung beim Durchsuchen von Servern im Netzwerk sehen.	

Einrichten eines SMB-Servers in einer Arbeitsgruppe

Parameter zum Erstellen eines SMB-Servers in einer Arbeitsgruppe

Sie geben diese Werte mit dem `vserver cifs create` Befehl an, wenn Sie einen neuen SMB-Server erstellen und unterstützte SMB-Versionen angeben. Erfahren Sie mehr über `vserver cifs create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der der SMB-Server erstellt werden soll.	
`-cifs-server`	Der Name des SMB-Servers (bis zu 15 Zeichen).	
`-workgroup`	Der Name der Arbeitsgruppe (bis zu 15 Zeichen).	
`-comment`	Optional: Ein Textkommentar für den Server. Windows-Clients können diese SMB-Serverbeschreibung beim Durchsuchen von Servern im Netzwerk sehen.	

Parameter zum Erstellen von lokalen Benutzern

Sie geben diese Werte ein, wenn Sie lokale Benutzer mit dem `vserver cifs users-and-groups local-user create` Befehl erstellen. Sie sind für SMB-Server in Arbeitsgruppen und optional in AD-Domänen erforderlich. Erfahren Sie mehr über `vserver cifs users-and-groups local-user create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der der lokale Benutzer erstellt werden soll.	
`-user-name`	Der Name des lokalen Benutzers (bis zu 20 Zeichen).	
`-full-name`	Optional: Der vollständige Name des Benutzers. Wenn der vollständige Name ein Leerzeichen enthält, setzen Sie den vollständigen Namen in doppelte Anführungszeichen.	
`-description`	Optional: Eine Beschreibung für den lokalen Benutzer. Wenn die Beschreibung ein Leerzeichen enthält, setzen Sie den Parameter in Anführungszeichen.	
`-is-account-disabled`	Optional: Gibt an, ob das Benutzerkonto aktiviert oder deaktiviert ist. Wenn dieser Parameter nicht angegeben wird, ist die Standardeinstellung, das Benutzerkonto zu aktivieren.	

Parameter zum Erstellen von lokalen Gruppen

Sie geben diese Werte ein, wenn Sie lokale Gruppen mit dem `vserver cifs users-and-groups local-group create` Befehl erstellen. Sie sind optional für SMB Server in AD-Domänen und Arbeitsgruppen. Erfahren Sie mehr über `vserver cifs users-and-groups local-group create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der die lokale Gruppe erstellt werden soll.	
`-group-name`	Der Name der lokalen Gruppe (bis zu 256 Zeichen).	
`-description`	Optional: Eine Beschreibung für die lokale Gruppe. Wenn die Beschreibung ein Leerzeichen enthält, setzen Sie den Parameter in Anführungszeichen.	

Hinzufügen von Storage-Kapazität zu einer SMB-fähigen SVM

Parameter für die Erstellung eines Volumens

Sie geben diese Werte mit dem `volume create` Befehl an, wenn Sie ein Volume anstelle eines qtree erstellen. Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name einer neuen oder vorhandenen SVM, die das neue Volume hosten wird.	
`-volume`	Ein eindeutiger beschreibende Name, den Sie für das neue Volume angeben.	
`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichend Platz für das neue SMB Volume.	
`-size`	Eine Ganzzahl, die Sie für die Größe des neuen Datenträgers festlegen.	
`-security-style`	Verwenden Sie den NTFS-Sicherheitsstil für diesen Workflow.	`ntfs`
`-junction-path`	Ort unter root (/), wo das neue Volume gemountet werden soll.	

Parameter zur Erstellung eines qtree

Sie geben diese Werte mit dem `volume qtree create` Befehl an, wenn Sie einen qtree anstelle eines Volumes erstellen. Erfahren Sie mehr über `volume qtree create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der sich das Volume mit dem qtree befindet.	
`-volume`	Der Name des Volume, das den neuen qtree enthalten soll.	
`-qtree`	Einen eindeutigen beschreibenden Namen, den Sie für den neuen qtree bereitstellen, mindestens 64 Zeichen.	

Feld	Beschreibung	Ihr Wert
`-qtree-path`	Das qtree-Pfad-Argument im Format `/vol/volume_name/qtree_name\>` kann angegeben werden, anstatt das Volume und qtree als separate Argumente anzugeben.	

Parameter zum Erstellen von SMB-Shares

Sie geben diese Werte mit dem `vserver cifs share create` Befehl ein. Erfahren Sie mehr über `vserver cifs share create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der die SMB-Freigabe erstellt werden soll.	
`-share-name`	Der Name der zu erstellenden SMB-Freigabe (bis zu 256 Zeichen).	
`-path`	Der Name des Pfads zur SMB-Freigabe (bis zu 256 Zeichen). Dieser Pfad muss in einem Volume vorhanden sein, bevor die Freigabe erstellt wird.	
`-share-properties`	Optional: Eine Liste der Freigabegenschaften. Die Standardeinstellungen sind `oplocks`, , `browsable changenotify` und `show-previous-versions`.	
`-comment`	Optional: Ein Textkommentar für den Server (bis zu 256 Zeichen). Windows-Clients können diese SMB-Share-Beschreibung beim Durchsuchen im Netzwerk sehen.	

Parameter zum Erstellen von SMB-Share-Zugriffssteuerungslisten (ACLs)

Sie geben diese Werte mit dem `vserver cifs share access-control create` Befehl ein. Erfahren Sie mehr über `vserver cifs share access-control create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der die SMB-ACL erstellt werden soll.	
`-share`	Der Name der SMB-Freigabe, auf der erstellt werden soll.	
`-user-group-type`	Der Typ des Benutzers oder der Gruppe, der zur ACL der Freigabe hinzugefügt werden soll. Der Standardtyp ist `windows`	`windows`
`-user-or-group`	Der Benutzer oder die Gruppe, der zur ACL der Freigabe hinzugefügt werden soll. Wenn Sie den Benutzernamen angeben, müssen Sie die Domäne des Benutzers im Format „`domain\username`“ angeben.	
`-permission`	Gibt die Berechtigungen für den Benutzer oder die Gruppe an.	`[No_access
Read	Change	Full_Control]`

Konfigurieren des SMB-Zugriffs auf eine SVM

SMB-Zugriff auf ONTAP SVMs konfigurieren

Wenn Sie noch keine SVM für den SMB-Client-Zugriff konfiguriert haben, müssen Sie entweder eine neue SVM erstellen und konfigurieren oder eine vorhandene SVM konfigurieren. Zum Konfigurieren von SMB werden der Root-Volume-Zugriff auf SVM, die Erstellung eines SMB-Servers, die Erstellung einer logischen Schnittstelle, die Aktivierung der Hostnamenauflösung, die Konfiguration von Name Services und, falls gewünscht, ermöglicht. Aktivieren der Kerberos-Sicherheit.

Erstellen Sie ONTAP SVMs, um den SMB-Datenzugriff zu gewährleisten

Wenn nicht bereits mindestens eine SVM in einem Cluster vorhanden ist, um den Datenzugriff für SMB-Clients zu ermöglichen, muss eine SVM erstellt werden.

Bevor Sie beginnen

- Ab ONTAP 9.13.1 können Sie die maximale Kapazität für eine Storage-VM festlegen. Sie können außerdem Warnmeldungen konfigurieren, wenn sich die SVM einem Kapazitätsschwellenwert nähert. Weitere Informationen finden Sie unter Management der SVM-Kapazität.

Schritte

1. SVM erstellen: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
   - Verwenden Sie die NTFS-Einstellung für die `-rootvolume-security-style` Option.
   - Verwenden Sie die Standardoption C.UTF-8 `-language`.
   - Die `ipspace` Einstellung ist optional.
2. Konfiguration und Status der neu erstellten SVM überprüfen: `vserver show -vserver vserver_name`

   Das `Allowed Protocols` Feld muss CIFS enthalten. Sie können diese Liste später bearbeiten.

   Das `Vserver Operational State` Feld muss den `running` Status anzeigen. Wenn auf der Statusanzeige der `initializing` Status angezeigt wird, ist ein Zwischenvorgang wie das Erstellen des Root-Volumes fehlgeschlagen, und Sie müssen die SVM löschen und neu erstellen.

Beispiele

Mit dem folgenden Befehl wird eine SVM für den Datenzugriff im IPspace erstellt `ipspaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

Mit dem folgenden Befehl wird angezeigt, dass eine SVM mit einem 1-GB-Root-Volume erstellt wurde und dieses automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine standardmäßige Exportrichtlinie, die keine Regeln enthält, sodass das Root-Volume bei der Erstellung nicht exportiert wird.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

Ab ONTAP 9.13.1 können Sie eine Vorlage für anpassungsfähige QoS-Richtliniengruppen festlegen und dabei eine Durchsatzgrenze sowie eine Obergrenze für die Volumes in der SVM festlegen. Sie können diese Richtlinie nur anwenden, nachdem Sie die SVM erstellt haben. Weitere Informationen zu diesem Prozess finden Sie unter Legen Sie eine Vorlage für adaptive Richtliniengruppen fest.

Vergewissern Sie sich, dass das SMB-Protokoll auf der ONTAP SVM aktiviert ist

Bevor Sie SMB auf SVMs konfigurieren und verwenden können, müssen Sie sicherstellen, dass das Protokoll aktiviert ist.

Über diese Aufgabe

Dies geschieht normalerweise während des SVM Setups. Wenn Sie das Protokoll jedoch während des Setups nicht aktiviert haben, können Sie es später über den `vserver add-protocols` Befehl aktivieren.

Sobald ein Protokoll erstellt wurde, können Sie es nicht mehr zu einem LIF hinzufügen oder daraus entfernen.

Sie können auch Protokolle für SVMs mit dem `vserver remove-protocols` Befehl deaktivieren.

Schritte

1. Prüfen Sie, welche Protokolle derzeit für die SVM aktiviert und deaktiviert sind: `vserver show -vserver vserver_name -protocols`

   Außerdem können Sie mit dem `vserver show-protocols` Befehl die derzeit aktivierten Protokolle auf allen SVMs im Cluster anzeigen.

2. Aktivieren oder deaktivieren Sie gegebenenfalls ein Protokoll:
   - So aktivieren Sie das SMB-Protokoll: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - So deaktivieren Sie ein Protokoll: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Stellen Sie sicher, dass die aktivierten und deaktivierten Protokolle korrekt aktualisiert wurden: `vserver show -vserver vserver_name -protocols`

Beispiel

Mit dem folgenden Befehl werden auf der SVM namens vs1 angezeigt, welche Protokolle derzeit aktiviert bzw. deaktiviert (zulässig und nicht zulässig) sind:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

Mit dem folgenden Befehl wird `cifs` der Zugriff über SMB ermöglicht, indem zu der Liste der aktivierten Protokolle auf der SVM mit dem Namen vs1 hinzugefügt wird:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Öffnen Sie die SMB-Exportrichtlinie des ONTAP SVM Root-Volumes

Die standardmäßige Exportrichtlinie für das SVM-Root-Volume muss eine Regel enthalten, um allen Clients einen offenen Zugriff über SMB zu ermöglichen. Ohne diese Regel erhält jeder SMB-Client Zugriff auf die SVM und ihre Volumes.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine standardmäßige Exportrichtlinie (Standard) für das Root-Volume der SVM erstellt. Sie müssen eine oder mehrere Regeln für die Standard-Exportrichtlinie erstellen, bevor Clients auf Daten auf der SVM zugreifen können.

Sie sollten überprüfen, ob der gesamte SMB-Zugriff in der Standard-Exportrichtlinie geöffnet ist, und den Zugriff später auf einzelne Volumes einschränken, indem Sie benutzerdefinierte Exportrichtlinien für einzelne Volumes oder qtrees erstellen.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, überprüfen Sie die Standardexportrichtlinie des Root-

Volumes: `vserver export-policy rule show`

Die Befehlsausgabe sollte wie die folgenden sein:

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

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Wenn eine solche Regel vorhanden ist, die einen offenen Zugriff ermöglicht, ist diese Aufgabe abgeschlossen. Falls nicht, fahren Sie mit dem nächsten Schritt fort.

2. Exportregel für das SVM-Root-Volume erstellen: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Überprüfen Sie die Regelerstellung mit dem `vserver export-policy rule show` Befehl.

Ergebnisse

Jeder SMB-Client kann jetzt auf alle Volumes oder qtree zugreifen, die auf der SVM erstellt wurden.

Erstellung von ONTAP SMB LIFs

Ein LIF ist eine IP-Adresse, die einem physischen oder logischen Port zugewiesen ist. Falls eine Komponente ausfällt, kann ein LIF ein Failover auf einen anderen physischen Port durchführen oder zu einem anderen migrieren, sodass weiterhin mit dem Netzwerk kommunizieren wird.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss im Administratorstatus konfiguriert worden `up` sein. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.

  Subnetze enthalten einen Pool mit IP-Adressen, die zum selben Layer-3-Subnetz gehören. Sie werden mit dem `network subnet create` Befehl erstellt.

  Erfahren Sie mehr über `network subnet create` in der "ONTAP-Befehlsreferenz".

- Der Mechanismus zur Angabe der von einem LIF bearbeiteten Traffic-Art ist geändert. Für ONTAP 9.5 und früher verwendeten LIFs Rollen, um den Typ des Datenverkehrs anzugeben, den er verarbeiten würde. Ab ONTAP 9.6 verwenden LIFs Service-Richtlinien, um den Typ des Datenverkehrs anzugeben, den es verarbeiten würde.

Über diese Aufgabe

- Sie können am gleichen Netzwerkport IPv4- und IPv6-LIFs erstellen.
- Wenn Sie im Cluster eine große Anzahl von LIFs enthalten sind, können Sie die auf dem Cluster unterstützte LIF- `network interface capacity show`Kapazität überprüfen. Verwenden Sie dazu den Befehl und die auf jedem Node unterstützte LIF-Kapazität. Hierzu können Sie mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene) nachprüfen.

  Erfahren Sie mehr über `network interface` in der "ONTAP-Befehlsreferenz".

- Wenn bereits ab ONTAP 9.7 andere LIFs für die SVM im selben Subnetz vorhanden sind, müssen Sie den Home Port der LIF nicht angeben. ONTAP wählt automatisch einen zufälligen Port auf dem angegebenen Home-Node in derselben Broadcast-Domäne wie die anderen LIFs, die bereits im selben Subnetz konfiguriert sind.

Schritte

1. LIF erstellen:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask IP_address | -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

ONTAP 9.5 und früher
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

ONTAP 9.6 und höher
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

   - Der `-role` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Service-Richtlinie erstellt wird (beginnend mit ONTAP 9.6).
   - Der `-data-protocol` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Service-Richtlinie erstellt wird (beginnend mit ONTAP 9.6). Bei Verwendung von ONTAP 9 5 und früher `-data -protocol` muss der Parameter bei der Erstellung der LIF angegeben werden und kann später nicht mehr verändert werden, ohne die Daten-LIF zu zerstören und neu zu erstellen.

- `-home-node` Ist der Node, zu dem das LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

  Sie können außerdem angeben, ob die LIF mithilfe der `-auto-revert` Option automatisch zum Home Node und Home Port zurückgesetzt werden soll.

- `-home-port` Ist der physische oder logische Port, zu dem die LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
- Sie können eine IP-Adresse mit den `-address -netmask` Optionen und angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option aktivieren.
- Wenn Sie zur Versorgung der IP-Adresse und Netzwerkmaske ein Subnetz verwenden, wird bei einem Gateway automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt, wenn mithilfe dieses Subnetzes eine LIF erstellt wird.
- Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänen-Controller in einem anderen IP-Subnetz vorhanden sind. Weitere Informationen zum `network route create` Erstellen einer statischen Route innerhalb einer SVM finden Sie im "ONTAP-Befehlsreferenz".
- `-firewall-policy`Verwenden Sie für die Option denselben Standard `data` wie die LIF-Rolle.

  Sie können bei Bedarf später eine benutzerdefinierte Firewallrichtlinie erstellen und hinzufügen.

  > Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

- `-auto-revert` Ermöglicht Ihnen die Angabe, ob eine Daten-LIF automatisch auf ihren Home Node zurückgesetzt wird, wenn beispielsweise ein Start erfolgt, Änderungen am Status der Managementdatenbank oder die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`, Sie können sie jedoch `false` abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf festlegen.

2. Überprüfen Sie, ob das LIF erfolgreich erstellt wurde:

   ```
   network interface show
   ```

3. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Beispiele

Mit dem folgenden Befehl wird eine LIF erstellt und die Werte der IP-Adresse und Netzwerkmaske anhand der `-address -netmask` Parameter und angegeben:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

Mit dem folgenden Befehl wird eine LIF erstellt und dem angegebenen Subnetz (namens client1_sub) IP-Adresse und Netzwerkmaskenwerte zugewiesen:

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

Mit dem folgenden Befehl werden alle LIFs in Cluster-1 angezeigt. Datenschnittstellen Datenschnittstellen Datenverbund Daten3 werden mit IPv4-Adressen konfiguriert und Daten3 wird mit einer IPv6-Adresse konfiguriert:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Der folgende Befehl zeigt, wie eine NAS-Daten-LIF erstellt wird, die der `default-data-files` Service-Richtlinie zugewiesen ist:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Verwandte Informationen

- "Netzwerk-Ping"
- "Wiederherstellung der Netzwerkschnittstelle"

Aktivieren Sie DNS für die ONTAP-SMB-Hostnamenauflösung

Sie können mit dem `vserver services name-service dns` Befehl DNS auf einer SVM aktivieren und für die Verwendung von DNS für die Auflösung von Host-Namen konfigurieren. Host-Namen werden mithilfe externer DNS-Server aufgelöst. Erfahren Sie mehr über `vserver services name-service dns` in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Ein standortweiter DNS-Server muss für die Suche nach Hostnamen verfügbar sein.

Sie sollten mehrere DNS-Server konfigurieren, um Single Point of Failure zu vermeiden. `vserver services name-service dns create`Wenn Sie nur einen DNS-Servernamen eingeben, gibt der Befehl eine Warnung aus. Erfahren Sie mehr über `vserver services name-service dns create` in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Erfahren Sie mehr über "Dynamisches DNS auf der SVM konfigurieren".

Schritte

1. DNS auf der SVM aktivieren: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   Mit dem folgenden Befehl werden externe DNS-Server auf der SVM vs1 aktiviert:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > ⓘ Der `vserver services name-service dns create` Befehl führt eine automatische Konfigurationsprüfung durch und meldet eine Fehlermeldung, wenn ONTAP den Name Server nicht kontaktieren kann.

2. Zeigen Sie die DNS-Domänenkonfigurationen mit dem `vserver services name-service dns show` Befehl an.

   Mit dem folgenden Befehl werden die DNS-Konfigurationen für alle SVMs im Cluster angezeigt:

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   Mit dem folgenden Befehl werden detaillierte DNS-Konfigurationsinformationen für SVM vs1 angezeigt:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Überprüfen Sie den Status der Namensserver mit dem `vserver services name-service dns check` Befehl.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
---------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Richten Sie einen SMB-Server in einer Active Directory-Domäne ein

Konfiguration der ONTAP Time Services für SMB-Server

Bevor Sie einen SMB-Server in einem Active Domain-Controller erstellen, müssen Sie sicherstellen, dass die Clusterzeit und die Zeit auf den Domänencontrollern der Domäne, zu der der SMB-Server gehört, innerhalb von fünf Minuten übereinstimmen.

Über diese Aufgabe

Sie sollten die Cluster-NTP-Dienste so konfigurieren, dass sie für die Synchronisierung dieselben NTP-Server verwenden, die auch die Active Directory-Domäne nutzt.

Ab ONTAP 9.5 können Sie Ihren NTP-Server mit symmetrischer Authentifizierung einrichten.

Schritte

1. Konfigurieren Sie Zeitdienste mit dem `cluster time-service ntp server create` Befehl.
   - Geben Sie den folgenden Befehl ein, um Time Services ohne symmetrische Authentifizierung zu konfigurieren: `cluster time-service ntp server create -server server_ip_address`
   - Geben Sie den folgenden Befehl ein, um Zeitdienste mit symmetrischer Authentifizierung zu konfigurieren: `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. Überprüfen Sie mit dem `cluster time-service ntp server show` Befehl, ob die Zeitdienste ordnungsgemäß eingerichtet wurden.

   `cluster time-service ntp server show`

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

Verwandte Informationen

- "Cluster Time Service ntp"

ONTAP-Befehle zum Managen der symmetrischen Authentifizierung auf NTP-Servern

Ab ONTAP 9.5 wird das Network Time Protocol (NTP) Version 3 unterstützt. NTPv3 bietet eine symmetrische Authentifizierung mit SHA-1-Schlüsseln, die die Netzwerksicherheit erhöht.

Hier…	Befehl
Konfigurieren Sie einen NTP-Server ohne symmetrische Authentifizierung	`cluster time-service ntp server create -server server_name`
Konfigurieren Sie einen NTP-Server mit symmetrischer Authentifizierung	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Symmetrische Authentifizierung für einen vorhandenen NTP-Server aktivieren ein vorhandener NTP-Server kann angepasst werden, um die Authentifizierung durch Hinzufügen der erforderlichen Schlüssel-ID zu ermöglichen	`cluster time-service ntp server modify -server server_name -key-id key_id`
Konfigurieren Sie einen freigegebenen NTP-Schlüssel	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Freigegebene Schlüssel werden durch eine ID bezeichnet. Die ID, der Typ und der Wert müssen auf dem Node und dem NTP-Server identisch sein
Konfigurieren Sie einen NTP-Server mit einer unbekannten Schlüssel-ID	`cluster time-service ntp server create -server server_name -key-id key_id`

Hier…	Befehl
Konfigurieren Sie einen Server mit einer Schlüssel-ID, die nicht auf dem NTP-Server konfiguriert ist.	`cluster time-service ntp server create -server server_name -key-id key_id` Die Schlüssel-ID, der Typ und der Wert müssen identisch mit der auf dem NTP-Server konfigurierten Schlüssel-ID, dem Typ und dem Wert sein.
Deaktivieren Sie die symmetrische Authentifizierung	`cluster time-service ntp server modify -server server_name -authentication disabled`

Verwandte Informationen

- "Cluster Time Service ntp"

Erstellen Sie SMB-Server in einer ONTAP Active Directory-Domäne

Sie können mit dem `vserver cifs create` Befehl einen SMB-Server auf der SVM erstellen und die Active Directory (AD)-Domäne angeben, zu der sie gehört.

Bevor Sie beginnen

Die SVM und die LIFs, die Sie zur Bedienung von Daten verwenden, müssen konfiguriert worden sein, um das SMB-Protokoll zu unterstützen. Die LIFs müssen in der Lage sein, eine Verbindung zu den DNS-Servern herzustellen, die auf der SVM konfiguriert sind, und zu einem AD-Domänencontroller der Domäne, mit dem Sie dem SMB-Server beitreten möchten.

Jeder Benutzer, der zum Erstellen von Computerkonten in der AD-Domäne autorisiert ist, zu der Sie dem SMB-Server beitreten, kann den SMB-Server auf der SVM erstellen. Dies kann auch Benutzer aus anderen Domänen umfassen.

Ab ONTAP 9.7 kann Ihr AD-Administrator Ihnen einen URI zu einer Keytab-Datei als Alternative zur Bereitstellung eines Namens und Kennworts für ein privilegiertes Windows-Konto zur Verfügung stellen. Wenn Sie den URI erhalten, geben Sie ihn in den `-keytab-uri` Parameter mit den `vserver cifs` Befehlen an.

Über diese Aufgabe

Beim Erstellen eines SMB-Servers in einer Activity Directory-Domäne:

- Sie müssen den vollständig qualifizierten Domänennamen (FQDN) verwenden, wenn Sie die Domäne angeben.
- Die Standardeinstellung besteht darin, das SMB-Serverrechnerkonto dem Objekt Active Directory CN=Computer hinzuzufügen.
- Mit der `-ou` Option können Sie den SMB-Server einer anderen Organisationseinheit (Organisationseinheit) hinzufügen.
- Sie können optional eine kommagetrennte Liste mit einem oder mehreren NetBIOS-Aliasen (bis zu 200) für den SMB-Server hinzufügen.

  Das Konfigurieren von NetBIOS-Aliase für einen SMB-Server kann nützlich sein, wenn Sie Daten von anderen Dateiservern auf den SMB-Server konsolidieren und den SMB-Server auf die Namen der

ursprünglichen Server reagieren möchten.

Erfahren Sie mehr über `vserver cifs` und optionale Parameter und Benennungsanforderungen im "ONTAP-Befehlsreferenz".

Ab ONTAP 9.8 können Sie festlegen, dass Verbindungen zu Domänencontrollern verschlüsselt werden. ONTAP erfordert Verschlüsselung für die Kommunikation mit dem Domänencontroller, wenn die `-encryption-required-for-dc-connection` Option auf eingestellt ist `true`; der Standardwert ist `false`. Wenn die Option eingestellt ist, wird nur das SMB3-Protokoll für ONTAP-DC-Verbindungen verwendet, da Verschlüsselung nur von SMB3 unterstützt wird. .

"SMB-Management" Enthält weitere Informationen zu Konfigurationsoptionen für SMB-Server.

Schritte

1. Überprüfen Sie, ob SMB auf Ihrem Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist im Lieferumfang enthalten"ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

   Eine CIFS-Lizenz ist nicht erforderlich, wenn der SMB-Server nur zur Authentifizierung verwendet wird.

2. SMB-Server in einer AD-Domäne erstellen: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Beim Beitritt zu einer Domäne kann dieser Befehl einige Minuten dauern.

   Mit dem folgenden Befehl wird der SMB-Server „`smb_server01`“ in der Domäne „`example.com`“:“ erstellt

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   Der folgende Befehl erstellt den SMB-Server „`smb_Server02`“ in der Domäne „`mydomain.com`““ und authentifiziert den ONTAP-Administrator mit einer Keytab-Datei:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Überprüfen Sie die SMB-Serverkonfiguration mit dem `vserver cifs show` Befehl.

   In diesem Beispiel zeigt die Befehlsausgabe an, dass ein SMB-Server mit dem Namen „`SMB_SERVER01`“ auf SVM vs1.example.com erstellt und der Domäne „`example.com`““ hinzugefügt wurde.

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

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. Aktivieren Sie auf Wunsch die verschlüsselte Kommunikation mit dem Domänencontroller (ONTAP 9.8 und höher): `vserver cifs security modify -vserver svm_name -encryption-required-for -dc-connection true`

Beispiele

Mit dem folgenden Befehl wird ein SMB-Server mit dem Namen „`smb_server02`“ auf SVM vs2.example.com in der Domäne „`example.com`"“ erstellt. Das Maschinenkonto wird im Container „`OU=eng,OU=corp,DC=example,DC=com`“ erstellt. Dem SMB-Server wird ein NetBIOS-Alias zugewiesen.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

Mit dem folgenden Befehl kann ein Benutzer aus einer anderen Domäne, in diesem Fall ein Administrator einer vertrauenswürdigen Domäne, einen SMB-Server mit dem Namen „`smb_server03`“ auf SVM vs3.example.com erstellen. Die `-domain` Option gibt den Namen der Home-Domain (angegeben in der DNS-Konfiguration) an, in der Sie den SMB-Server erstellen möchten. Die `username` Option gibt den Administrator der vertrauenswürdigen Domäne an.

- Home Domain: example.com
- Vertrauenswürdige Domäne: trust.lab.com
- Benutzername für die vertrauenswürdige Domäne: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Erstellen Sie Keytab-Dateien für die ONTAP-SMB-Authentifizierung

Ab ONTAP 9.7 unterstützt ONTAP die SVM-Authentifizierung mit Active Directory (AD) Servern unter Verwendung von Keytab-Dateien. AD-Administratoren generieren eine Keytab-Datei und stellen sie ONTAP-Administratoren als einheitliche Ressourcenkennung (URI) zur Verfügung, die bereitgestellt wird, wenn `vserver cifs` Befehle eine Kerberos-Authentifizierung mit der AD-Domäne erfordern.

AD-Administratoren können die Keytab-Dateien mit dem Standardbefehl Windows Server erstellen `ktpass`. Der Befehl sollte in der primären Domäne ausgeführt werden, in der eine Authentifizierung erforderlich ist. Der `ktpass` Befehl kann verwendet werden, um Keytab-Dateien nur für primäre Domänenbenutzer zu generieren; Schlüssel, die mit vertrauenswürdigen Domänenbenutzern generiert werden, werden nicht unterstützt.

Keytab-Dateien werden für bestimmte ONTAP Admin-Benutzer generiert. Solange sich das Passwort des Admin-Benutzers nicht ändert, ändern sich die für den jeweiligen Verschlüsselungstyp und die Domäne generierten Schlüssel nicht. Daher ist immer dann eine neue Keytab-Datei erforderlich, wenn das Passwort des Admin-Benutzers geändert wird.

Folgende Verschlüsselungstypen werden unterstützt:

- AES256-SHA1
- DES-CBC-MD5

  ⓘ ONTAP unterstützt den Verschlüsselungstyp DES-CBC-CRC nicht.

- RC4-HMAC

AES256 ist der höchste Verschlüsselungstyp und sollte verwendet werden, wenn diese auf dem ONTAP-System aktiviert ist.

Keytab-Dateien können entweder durch Angabe des Admin-Passworts oder durch die Verwendung eines zufällig generierten Passworts generiert werden. Allerdings kann zu einem bestimmten Zeitpunkt nur eine Kennwortoption verwendet werden, da ein privater Schlüssel, der für den Admin-Benutzer spezifisch ist, auf dem AD-Server zum Entschlüsseln der Schlüssel in der Keytab-Datei benötigt wird. Jede Änderung des privaten Schlüssels für einen bestimmten Administrator wird die Keytab-Datei ungültig.

Richten Sie einen SMB-Server in einer Arbeitsgruppe ein

Erfahren Sie mehr über die Konfiguration von SMB-Servern in ONTAP-Arbeitsgruppen

Die Einrichtung eines SMB-Servers als Mitglied in einer Arbeitsgruppe besteht darin, den SMB-Server zu erstellen und dann lokale Benutzer und Gruppen zu erstellen.

Sie können einen SMB-Server in einer Arbeitsgruppe konfigurieren, wenn die Microsoft Active Directory-Domäneninfrastruktur nicht verfügbar ist.

Ein SMB-Server im Workgroup-Modus unterstützt nur NTLM-Authentifizierung und unterstützt keine Kerberos-Authentifizierung.

Erstellen Sie SMB Server auf der ONTAP SVM mit angegebenen Arbeitsgruppen

Mit dem `vserver cifs create` Befehl können Sie einen SMB-Server auf der SVM erstellen und die Arbeitsgruppe angeben, zu der er gehört.

Bevor Sie beginnen

Die SVM und die LIFs, die Sie zur Bedienung von Daten verwenden, müssen konfiguriert worden sein, um das SMB-Protokoll zu unterstützen. Die LIFs müssen in der Lage sein, eine Verbindung zu den auf der SVM konfigurierten DNS-Servern herzustellen.

Über diese Aufgabe

SMB-Server im Workgroup-Modus unterstützen die folgenden SMB-Funktionen nicht:

- SMB B3 Witness Protokoll
- SMB3 CA-Freigaben
- SQL über SMB
- Ordnerumleitung
- Roaming-Profile
- Gruppenrichtlinienobjekt (GPO)
- Volume Snapshot Service (VSS)

Weitere Informationen zu `vserver cifs` und optionalen Konfigurationsparametern und Benennungsanforderungen finden Sie im "ONTAP-Befehlsreferenz".

Schritte

1. Überprüfen Sie, ob SMB auf Ihrem Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist im Lieferumfang enthalten"ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

   Eine CIFS-Lizenz ist nicht erforderlich, wenn der SMB-Server nur zur Authentifizierung verwendet wird.

2. Erstellen Sie den SMB-Server in einer Arbeitsgruppe: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   Mit dem folgenden Befehl wird der SMB-Server „`smb_server01`“ in der Arbeitsgruppe „`workgroup01`“ erstellt:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Überprüfen Sie die SMB-Serverkonfiguration mit dem `vserver cifs show` Befehl.

   Im folgenden Beispiel zeigt die Befehlsausgabe an, dass auf SVM vs1.example.com in der Arbeitsgruppe „`workgroup01`“ ein SMB-Server mit dem Namen „`smb_server01`“ erstellt wurde:

```
cluster1::> vserver cifs show -vserver vs0

                                        Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Nachdem Sie fertig sind

Für einen CIFS-Server in einer Arbeitsgruppe müssen lokale Benutzer und optional lokale Gruppen auf der SVM erstellt werden.

Verwandte Informationen

"SMB-Management"

Erstellen Sie lokale ONTAP SMB-Benutzerkonten

Sie können ein lokales Benutzerkonto erstellen, das über eine SMB-Verbindung für den Zugriff auf die in der SVM enthaltenen Daten verwendet werden kann. Sie können auch lokale Benutzerkonten zur Authentifizierung verwenden, wenn Sie eine SMB-Sitzung erstellen.

Über diese Aufgabe

Beim Erstellen der SVM ist die lokale Benutzerfunktion standardmäßig aktiviert.

Beim Erstellen eines lokalen Benutzerkontos müssen Sie einen Benutzernamen angeben. Zudem müssen Sie die SVM angeben, der das Konto zugeordnet werden soll.

Erfahren Sie mehr über `vserver cifs users-and-groups local-user` und optionale Parameter und Benennungsanforderungen im "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen Sie den lokalen Benutzer: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Die folgenden optionalen Parameter könnten hilfreich sein:

- `-full-name`

  Der vollständige Name des Benutzers.

- `-description`

  Eine Beschreibung für den lokalen Benutzer.

- `-is-account-disabled {true|false}`

  Gibt an, ob das Benutzerkonto aktiviert oder deaktiviert ist. Wenn dieser Parameter nicht angegeben wird, ist die Standardeinstellung, das Benutzerkonto zu aktivieren.

Der Befehl fordert das Kennwort des lokalen Benutzers auf.

2. Geben Sie ein Kennwort für den lokalen Benutzer ein, und bestätigen Sie anschließend das Passwort.
3. Überprüfen Sie, ob der Benutzer erfolgreich erstellt wurde: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird ein lokaler Benutzer „`SMB_SERVER01\sue`“ mit dem vollständigen Namen „`Sue Chang`“ erstellt, der SVM vs1.example.com zugeordnet ist:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

Erstellen Sie lokale ONTAP SMB-Gruppen

Lokale Gruppen können zur Autorisierung des Zugriffs auf Daten, die der SVM zugeordnet sind, über eine SMB-Verbindung erstellt werden. Sie können auch Berechtigungen zuweisen, die definieren, welche Benutzerrechte oder Funktionen ein Mitglied der Gruppe hat.

Über diese Aufgabe

Bei der Erstellung der SVM ist die Funktion der lokalen Gruppe standardmäßig aktiviert.

Beim Erstellen einer lokalen Gruppe müssen Sie einen Namen für die Gruppe angeben. Sie müssen die SVM angeben, der die Gruppe zugeordnet werden soll. Sie können einen Gruppennamen mit oder ohne lokalen Domänennamen angeben und optional eine Beschreibung für die lokale Gruppe angeben. Sie können einer

anderen lokalen Gruppe keine lokale Gruppe hinzufügen.

Erfahren Sie mehr über `vserver cifs users-and-groups local-group` und optionale Parameter und Benennungsanforderungen im "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen Sie die lokale Gruppe: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   Der folgende optionale Parameter könnte hilfreich sein:

   - `-description`

     Eine Beschreibung für die lokale Gruppe.

2. Überprüfen Sie, ob die Gruppe erfolgreich erstellt wurde: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird eine lokale Gruppe „`SMB_SERVER01\Engineering`“ erstellt, die zu SVM vs1 gehört:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                     Description
---------------- ------------------------------ ----------------------------
vs1.example.com  BUILTIN\Administrators         Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators       Backup Operators group
vs1.example.com  BUILTIN\Power Users            Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                  All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

Nachdem Sie fertig sind

Sie müssen der neuen Gruppe Mitglieder hinzufügen.

Lokale ONTAP SMB-Gruppenmitgliedschaft verwalten

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

Über diese Aufgabe

Wenn Sie nicht mehr möchten, dass ein lokaler Benutzer, ein Domänenbenutzer oder eine Domänengruppe aufgrund einer Mitgliedschaft in einer Gruppe Zugriffsrechte oder Berechtigungen besitzen soll, können Sie das Mitglied aus der Gruppe entfernen.

Beim Hinzufügen von Mitgliedern zu einer lokalen Gruppe müssen Sie Folgendes beachten:

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

Beim Entfernen von Mitgliedern aus einer lokalen Gruppe müssen Sie Folgendes beachten:

- Sie können keine Mitglieder aus der speziellen *everyone*-Gruppe entfernen.
- Um ein Mitglied aus einer lokalen Gruppe zu entfernen, muss ONTAP in der Lage sein, seinen Namen zu einer SID aufzulösen.

Schritte

1. Fügen Sie ein Mitglied zu einer Gruppe hinzu oder entfernen Sie ein Mitglied aus einer Gruppe.
   - Mitglied hinzufügen: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Sie können eine kommagetrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die der angegebenen lokalen Gruppe hinzugefügt werden sollen.
   - Entfernen eines Mitglieds: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Sie können eine durch Komma getrennte Liste der lokalen Benutzer, Domänenbenutzer oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden sollen.

Beispiele

Im folgenden Beispiel wird der lokalen Gruppe „`SMB_SERVER01\sue`“ auf SVM vs1.example.com ein lokaler Benutzer „`SMB_SERVER01\Engineering`“ hinzugefügt:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

Im folgenden Beispiel werden die lokalen Benutzer „`SMB_SERVER01\sue`“ und „`SMB_SERVER01\james`“ aus der lokalen Gruppe „`SMB_SERVER01\Engineering`“ auf SVM vs1.example.com entfernt:

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

Überprüfen Sie aktivierte ONTAP SMB-Versionen

Ihre ONTAP Version 9 legt fest, welche SMB-Versionen standardmäßig für Verbindungen mit Clients und Domänen-Controllern aktiviert sind. Überprüfen Sie, ob der SMB-Server die in Ihrer Umgebung erforderlichen Clients und Funktionen unterstützt.

Über diese Aufgabe

Für Verbindungen mit Clients und Domänen-Controllern sollten Sie SMB 2.0 und höher aktivieren, sofern möglich. Aus Sicherheitsgründen sollten Sie die Verwendung von SMB 1.0 vermeiden. Sie sollten diese deaktivieren, wenn Sie bestätigt haben, dass dies in Ihrer Umgebung nicht erforderlich ist.

Ab ONTAP 9.3 ist die Funktion bei neuen SVMs standardmäßig deaktiviert.

> Wenn `-smb1-enabled-for-dc-connections` auf festgelegt `false` `-smb1-enabled` ist, während auf festgelegt ist `true`, verweigert ONTAP SMB 1.0-Verbindungen als Client, akzeptiert jedoch weiterhin eingehende SMB 1.0-Verbindungen als Server.

"SMB-Management" Enthält Details zu unterstützten SMB-Versionen und -Funktionen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Vergewissern Sie sich, welche SMB-Versionen aktiviert sind:

```
vserver cifs options show
```

Sie können in der Liste nach unten blättern, um die für Client-Verbindungen aktivierten SMB-Versionen anzuzeigen, und wenn Sie einen SMB-Server in einer AD-Domäne konfigurieren, für AD-Domänenverbindungen.

3. Aktivieren oder Deaktivieren des SMB-Protokolls für Client-Verbindungen nach Bedarf:
   - So aktivieren Sie eine SMB-Version:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

Mögliche Werte für `smb_version`:

- `-smb1-enabled`
- `-smb2-enabled`
- `-smb3-enabled`
- `-smb31-enabled`

Mit dem folgenden Befehl wird SMB 3.1 auf SVM vs1.example.com aktiviert: `cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true`

- So deaktivieren Sie eine SMB-Version:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. Wenn sich Ihr SMB-Server in einer Active Directory-Domäne befindet, aktivieren oder deaktivieren Sie das SMB-Protokoll für DC-Verbindungen nach Bedarf:
   - So aktivieren Sie eine SMB-Version:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   - So deaktivieren Sie eine SMB-Version:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Ordnen Sie ONTAP SMB-Server auf dem DNS-Server zu

Der DNS-Server Ihres Standorts muss über einen Eintrag verfügen, der den SMB-Servernamen und alle NetBIOS-Aliase auf die IP-Adresse der Daten-LIF verweist, damit Windows-Benutzer ein Laufwerk dem SMB-Servernamen zuordnen können.

Bevor Sie beginnen

Sie müssen über Administratorzugriff auf den DNS-Server Ihres Standorts verfügen. Wenn Sie keinen Administratorzugriff haben, müssen Sie den DNS-Administrator bitten, diese Aufgabe auszuführen.

Über diese Aufgabe

Wenn Sie NetBIOS Aliase für den SMB-Servernamen verwenden, ist es eine Best Practice, DNS-Server-Einstiegspunkte für jeden Alias zu erstellen.

Schritte

1. Melden Sie sich beim DNS-Server an.
2. Erstellen Sie Einträge zum Forward (A - Address Record) und Reverse (PTR - Zeigerdatensatz), um den Namen des SMB-Servers der IP-Adresse der Daten-LIF zuzuordnen.
3. Wenn Sie NetBIOS-Aliase verwenden, erstellen Sie einen Alias Canonical Name (CNAME Resource

Record)-Sucheintrag, um jeden Alias der IP-Adresse der Daten-LIF des SMB-Servers zuzuordnen.

Ergebnisse

Nachdem das Mapping über das Netzwerk verbreitet wurde, können Windows-Benutzer ein Laufwerk dem SMB-Servernamen oder seinen NetBIOS-Aliasen zuordnen.

Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

Konfigurieren Sie den SMB-Client-Zugriff auf Shared-ONTAP-Storage

Um SMB-Client-Zugriff auf Shared Storage auf einer SVM zu ermöglichen, müssen Sie ein Volume oder einen qtree erstellen, um einen Storage-Container bereitzustellen, und anschließend eine Freigabe für diesen Container erstellen oder ändern. Anschließend können Sie Freigaben- und Dateiberechtigungen konfigurieren und den Zugriff von Client-Systemen testen.

Bevor Sie beginnen

- SMB muss vollständig auf der SVM eingerichtet sein.
- Alle Aktualisierungen Ihrer Namensdienstkonfiguration müssen abgeschlossen sein.
- Alle Erweiterungen oder Änderungen an einer Active Directory-Domäne oder einer Workgroup-Konfiguration müssen abgeschlossen sein.

Erstellung eines Volume oder qtree Storage-Containers

Erstellen Sie ONTAP SMB Volumes

Sie können ein Volume erstellen und seinen Verbindungspunkt sowie andere Eigenschaften mit dem `volume create` Befehl angeben.

Über diese Aufgabe

Ein Volume muss einen Verbindungspfad_ enthalten, damit seine Daten den Clients zur Verfügung gestellt werden können. Sie können den Verbindungspfad angeben, wenn Sie ein neues Volume erstellen. Wenn Sie ein Volume erstellen, ohne einen Verbindungspfad anzugeben, müssen Sie das Volume mit dem `volume mount` Befehl im SVM Namespace *mounten*.

Bevor Sie beginnen

- SMB sollte eingerichtet und ausgeführt werden.
- Der SVM-Sicherheitsstil muss NTFS sein.
- Ab ONTAP 9.13.1 können Sie Volumes mit aktivierten Kapazitätsanalysen und Aktivitätsverfolgung erstellen. Um die Kapazitäts- oder Aktivitätsüberwachung zu aktivieren, geben Sie den `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on`ein.

  Weitere Informationen über Kapazitätsanalysen und Aktivitätsverfolgung finden Sie unter "Dateisystemanalyse Aktivieren". Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen Sie das Volume mit einem Verbindungspunkt: `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path]`

   ```
   `-junction-path`Folgende Optionen stehen zur Auswahl:
   ```

   - Direkt unter root, zum Beispiel `/new_vol`

     Sie können ein neues Volume erstellen und festlegen, dass es direkt in das SVM Root-Volume eingebunden wird.

   - Unter einem vorhandenen Verzeichnis, z. B. `/existing_dir/new_vol`

     Sie können ein neues Volume erstellen und angeben, dass es in ein vorhandenes Volume (in einer vorhandenen Hierarchie) eingebunden wird, das als Verzeichnis angegeben wird.

   Wenn Sie beispielsweise ein Volume in einem neuen Verzeichnis (in einer neuen Hierarchie unter einem neuen Volume) `/new_dir/new_vol` erstellen möchten, müssen Sie zunächst ein neues übergeordnetes Volume erstellen, das mit dem SVM-Root-Volume verbunden wird. Anschließend würde das neue untergeordnete Volume im Verbindungspfad des neuen übergeordneten Volume (neues Verzeichnis) erstellt.

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

Beispiele

Mit dem folgenden Befehl wird ein neues Volume mit dem Namen „user1“ auf der SVM vs1.example.com und auf dem Aggregat aggr1 erstellt. Der neue Band ist verfügbar unter `/users`. Das Volume ist 750 GB groß und seine Volumengarantie ist vom Typ Volume (standardmäßig).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- -------  -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

Mit dem folgenden Befehl wird ein neues Volume mit dem Namen „`home4`“ auf der SVM“`vs1.example.com`**"** und das Aggregat „`aggr1`“ erstellt. Das Verzeichnis `/eng/` ist bereits im Namespace für die vs1 SVM vorhanden, und das neue Volume `/eng/home` wird unter, zur Verfügung gestellt `/eng/`, welches das Home-Verzeichnis für den Namespace wird. Das Volumen ist 750 GB groß, und seine Volumengarantie ist vom Typ `volume` (standardmäßig).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

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

Erstellen von ONTAP SMB qtrees

Sie können einen qtree mit Ihren Daten erstellen und seine Eigenschaften mit dem `volume qtree create` Befehl angeben.

Bevor Sie beginnen

- Es muss bereits die SVM und das Volume, das den neuen qtree enthalten soll, vorhanden sein.
- Der SVM-Sicherheitsstil muss NTFS enthalten und SMB sollte eingerichtet und ausgeführt werden.

Schritte

1. Erstellen des qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   Sie können den Volume und qtree als separate Argumente angeben oder das qtree Pfad-Argument im Format angeben `/vol/volume_name/_qtree_name`.

2. Vergewissern Sie sich, dass der qtree mit dem gewünschten Verbindungspfad erstellt wurde: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Beispiel

Im folgenden Beispiel wird ein qtree mit dem Namen qt01 auf SVM vs1.example.com erstellt, der einen Verbindungspfad hat `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: ntfs
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Anforderungen und Überlegungen beim Erstellen von ONTAP SMB-Freigaben

Vor dem Erstellen einer SMB-Freigabe müssen Sie die Anforderungen an Freigabungspfade und Share-Eigenschaften kennen, insbesondere für Home Directorys.

Beim Erstellen einer SMB-Freigabe muss eine Verzeichnispfadstruktur angegeben werden (mit der `-path` Option im `vserver cifs share create` Befehl), auf die Clients zugreifen. Der Verzeichnispfad entspricht dem Verbindungspfad für ein Volume oder qtree, den Sie im SVM Namespace erstellt haben. Der Verzeichnispfad und der entsprechende Verbindungspfad müssen vorhanden sein, bevor Sie Ihre Freigabe erstellen.

Freigabpfade haben die folgenden Anforderungen:

- Der Name eines Verzeichnispfads kann bis zu 255 Zeichen lang sein.
- Wenn ein Leerzeichen im Pfadnamen vorhanden ist, muss der gesamte String in Anführungszeichen gesetzt werden (z.B. `"/new volume/mount here"`).
- Wenn der UNC-Pfad (`\\servername\sharename\filepath`) der Freigabe mehr als 256 Zeichen enthält (mit Ausnahme des anfänglichen “\\” im UNC-Pfad), ist die Registerkarte **Sicherheit** im Windows-Eigenschaften-Feld 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.

Die Standardeinstellungen für die Freigabeeigenschaft können geändert werden:

- Die Standard-Anfangseigenschaften für alle Shares sind `oplocks`, , `browsable` `changenotify` und `show-previous-versions`.
- Beim Erstellen einer Freigabe können Sie die Freigabegenschaften festlegen.

Wenn Sie beim Erstellen der Freigabe jedoch Freigabeeigenschaften angeben, werden die Standardeinstellungen nicht verwendet. Wenn Sie den `-share-properties` Parameter beim Erstellen einer Freigabe verwenden, müssen Sie alle Freigabeeigenschaften angeben, die Sie auf die Freigabe anwenden möchten, indem Sie eine kommagetrennte Liste verwenden.

- Verwenden Sie die `homedirectory` Eigenschaft, um eine Home-Directory-Freigabe festzulegen.

  Mit dieser Funktion können Sie eine Freigabe konfigurieren, die verschiedenen Verzeichnissen zugeordnet wird, basierend auf dem Benutzer, der eine Verbindung zu ihr herstellt, und einem Satz von Variablen. Anstatt separate Shares für jeden Benutzer zu erstellen, können Sie eine einzelne Freigabe mit einigen Home-Directory-Parametern konfigurieren, um die Beziehung eines Benutzers zwischen einem Einstiegspunkt (Share) und seinem Home-Verzeichnis (einem Verzeichnis auf der SVM) zu definieren.

  Sie können diese Eigenschaft nach dem Erstellen der Freigabe nicht hinzufügen oder entfernen.

Home Directory-Shares haben die folgenden Anforderungen:

- Bevor Sie SMB-Home-Verzeichnisse erstellen, müssen Sie mit dem `vserver cifs home-directory search-path add` Befehl mindestens einen Suchpfad für das Home-Verzeichnis hinzufügen.
- `homedirectory -share-properties`Die mit dem Wert von auf angegebenen Home-Verzeichnis-Shares müssen die `%w` dynamische Variable (Windows-Benutzername) in den Freigabenamen enthalten.

  Der Freigabename kann zusätzlich die `%d` dynamische Variable (Domänenname) (z. B. `%d/%w`) oder einen statischen Teil im Freigabenamen (z. B. `home1_%w`) enthalten.

- Wenn die Freigabe von Administratoren oder Benutzern verwendet wird, um sich mit den Home-Verzeichnissen anderer Benutzer zu verbinden (mit den Optionen für den `vserver cifs home-directory modify` Befehl), muss dem dynamischen Share-Namensmuster eine Tilde vorangestellt werden (~).

Erfahren Sie mehr über `vserver cifs share` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "SMB-Management"

Erstellen von ONTAP SMB-Freigaben

Sie müssen eine SMB-Freigabe erstellen, bevor Sie Daten von einem SMB-Server für SMB-Clients freigeben können. Wenn Sie eine Freigabe erstellen, können Sie Freigabegenschaften festlegen, wie z. B. die Freigabe als Home-Verzeichnis zu bezeichnen. Sie können die Freigabe auch anpassen, indem Sie optionale Einstellungen konfigurieren.

Bevor Sie beginnen

Der Verzeichnispfad für Volume oder qtree muss im SVM-Namespace vorhanden sein, bevor die Freigabe erstellt wird.

Über diese Aufgabe

Wenn Sie eine Freigabe erstellen, lautet die Standard-Freigabe-ACL (Standard-Freigabeberechtigungen) `Everyone / Full Control`. Nachdem Sie den Zugriff auf die Freigabe getestet haben, sollten Sie die Standard-Share-ACL entfernen und sie durch eine sicherere Alternative ersetzen.

Schritte

1. Erstellen Sie bei Bedarf die Verzeichnispfadstruktur für die Freigabe.

   Der `vserver cifs share create` Befehl überprüft den in der `-path` Option während der Erstellung von Freigaben angegebenen Pfad. Wenn der angegebene Pfad nicht vorhanden ist, schlägt der Befehl fehl.

2. Mit der angegebenen SVM verbundene SMB-Freigabe erstellen: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Überprüfen Sie, ob die Freigabe erstellt wurde:`vserver cifs share show -share-name share_name`

Beispiele

Mit dem folgenden Befehl wird eine SMB-Freigabe namens „`SHARE1`“ auf SVM erstellt `vs1.example.com`. Sein Verzeichnispfad ist `/users`, und er wird mit Standardeigenschaften erstellt.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                    browsable
                                    changenotify
                                    show-previous-versions
```

Überprüfen Sie den ONTAP SMB-Client-Zugriff

Sie sollten überprüfen, ob SMB richtig konfiguriert wurde, indem Sie auf die Freigabe zugreifen und Daten schreiben. Sie sollten den Zugriff mithilfe des SMB-Servernamens und aller NetBIOS-Aliase testen.

Schritte

1. Melden Sie sich bei einem Windows-Client an.
2. Testen des Zugriffs mithilfe des SMB-Servernamens:

   a. Ordnen Sie in Windows Explorer der Freigabe ein Laufwerk im folgenden Format zu: `\\SMB_Server_Name\Share_Name`

      Wenn die Zuordnung nicht erfolgreich ist, kann es sein, dass das DNS-Mapping noch nicht im

gesamten Netzwerk verbreitet wurde. Sie müssen den Zugriff später mithilfe des SMB-Servernamens testen.

Wenn der SMB-Server den Namen vs1.example.com hat und die Freigabe den Namen SHARE1 hat, müssen Sie Folgendes eingeben: `\\vs0.example.com\SHARE1`

b. Erstellen Sie auf dem neu erstellten Laufwerk eine Testdatei, und löschen Sie dann die Datei.

Sie haben mithilfe des SMB-Servernamens den Schreibzugriff auf die Freigabe überprüft.

3. Wiederholen Sie Schritt 2 für alle NetBIOS-Aliase.

Erstellen von Zugriffssteuerungslisten der ONTAP SMB-Freigabe

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.

Bevor Sie beginnen

Sie müssen entschieden haben, welche Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.

Über diese Aufgabe

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

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

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_group_name -permission access_right`

3. Überprüfen Sie mit dem `vserver cifs share access-control show` Befehl, ob die auf die

Freigabe angewendete ACL korrekt ist.

Beispiel

Mit dem folgenden Befehl erhalten `Change` Sie Berechtigungen für die Windows-Gruppe „`Sales Team`“ für die Freigabe „`sales`“ auf „`vs1.example.com`"SVM:“

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

cluster1::> vserver cifs share access-control show
                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
```

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

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

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

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

Konfigurieren Sie NTFS-Dateiberechtigungen in ONTAP SMB-Freigaben

Um den Dateizugriff für die Benutzer oder Gruppen zu aktivieren, die Zugriff auf eine Freigabe haben, müssen Sie NTFS-Dateiberechtigungen für Dateien und Verzeichnisse in dieser Freigabe von einem Windows-Client aus konfigurieren.

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

"SMB-Management" Und Ihre Windows-Dokumentation enthält Informationen zum Festlegen von Standard- und erweiterten NTFS-Berechtigungen.

Schritte

1. Melden Sie sich als Administrator bei einem Windows-Client an.
2. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
3. Füllen Sie die Box * Map Network Drive* aus:

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

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

      Wenn Ihr SMB-SERVERNAME SMB_SERVER01 lautet und Ihre Freigabe „`SHARE1`“ heißt, geben Sie ein `\\SMB_SERVER01\SHARE1`.

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

4. Wählen Sie die Datei oder das Verzeichnis aus, für die Sie NTFS-Dateiberechtigungen festlegen möchten.
5. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis, und wählen Sie dann **Eigenschaften** aus.
6. 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 <Objekt> wird eine Liste mit Berechtigungen für den ausgewählten Benutzer oder die ausgewählte Gruppe angezeigt.

7. Klicken Sie Auf **Bearbeiten**.

   Das Feld Berechtigungen für <Objekt> wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie… wollen	Gehen Sie wie folgt vor…
Legen Sie die Standard-NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe fest	a. Klicken Sie Auf **Hinzufügen**. Das Fenster Benutzer, Computer, Servicekonten oder Gruppen auswählen wird geöffnet. b. Geben Sie im Feld **Geben Sie die Objektnamen ein, die Sie auswählen möchten**, den Namen des Benutzers oder der Gruppe ein, auf der Sie NTFS-Berechtigung hinzufügen möchten. c. Klicken Sie auf **OK**.
Ändern oder entfernen Sie standardmäßige NTFS-Berechtigungen von einem Benutzer oder einer Gruppe	Wählen Sie im Feld **Gruppe oder Benutzernamen** den Benutzer oder die Gruppe aus, die Sie ändern oder entfernen möchten.

9. Führen Sie die gewünschten Aktionen aus:

Ihr Ziel ist	Gehen Sie wie folgt vor
Legen Sie die Standard-NTFS-Berechtigungen für einen neuen oder vorhandenen Benutzer oder eine vorhandene Gruppe fest	Wählen Sie im Feld **Berechtigungen für <Objekt>** die Felder **Zulassen** oder **Deny** für den Zugriffstyp aus, den Sie dem ausgewählten Benutzer oder der ausgewählten Gruppe erlauben oder nicht zulassen möchten.
Entfernen Sie einen Benutzer oder eine Gruppe	Klicken Sie Auf **Entfernen**.

Wenn einige oder alle Standardberechtigungsfelder nicht ausgewählt werden können, liegt dies daran, dass die Berechtigungen vom übergeordneten Objekt übernommen werden. Die Box * Special Permissions* ist nicht wählbar. Wenn diese Option ausgewählt ist, bedeutet dies, dass für den ausgewählten Benutzer oder die ausgewählte Gruppe mindestens eine der erweiterten granularen Rechte festgelegt wurde.

10. Klicken Sie nach dem Hinzufügen, Entfernen oder Bearbeiten von NTFS-Berechtigungen für dieses Objekt auf **OK**.

Überprüfen Sie den Zugriff der ONTAP SMB-Benutzerfreigabe

Sie sollten testen, dass die von Ihnen konfigurierten Benutzer auf die SMB-Freigabe und die darin enthaltenen Dateien zugreifen können.

Schritte

1. Melden Sie sich auf einem Windows-Client als einer der Benutzer an, der nun Zugriff auf die Freigabe hat.
2. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
3. Füllen Sie die Box * Map Network Drive* aus:

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

b. Geben Sie im Feld **Ordner** den Freigabenamen ein, den Sie Benutzern zur Verfügung stellen möchten.

   Wenn Ihr SMB-SERVERNAME SMB_SERVER01 lautet und Ihre Freigabe „`SHARE1`“ heißt, geben Sie ein `\\SMB_SERVER01\share1`.

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.

4. Erstellen Sie eine Testdatei, überprüfen Sie, ob sie vorhanden ist, schreiben Sie Text in die Datei und entfernen Sie dann die Testdatei.