



Implementieren Sie serverbasierte SMB- Services

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

- Implementieren Sie serverbasierte SMB-Services 1
 - Home Directorys managen 1
 - Konfigurieren Sie den SMB-Client-Zugriff auf symbolische UNIX-Links 14
 - Mit BranchCache werden SMB-Inhalte im Cache für die gemeinsame Nutzung an externen Standorten gespeichert. 22
 - Höhere Performance von Microsoft Remote Copy 54
 - Verkürzen Sie die Antwortzeiten von Clients durch automatische SMB-Node-Empfehlungen mit Auto Location 60
 - Bereitstellen der Ordnersicherheit für Freigaben mit Access-Based Enumeration 67

Implementieren Sie serverbasierte SMB-Services

Home Directories managen

So ermöglicht ONTAP dynamische Home Directories

Mit den ONTAP Home Directories können Sie eine SMB-Freigabe konfigurieren, die verschiedenen Verzeichnissen anhand des Benutzers, der mit ihm verbunden wird, und einer Reihe von Variablen zugeordnet wird. Anstatt separate Shares für jeden Benutzer zu erstellen, können Sie eine Freigabe mit einigen Home-Directory-Parametern konfigurieren, um die Beziehung eines Benutzers zwischen einem Eintragungspunkt (Share) und dem Home-Verzeichnis (ein Verzeichnis auf der SVM) zu definieren.

Ein Benutzer, der als Gastbenutzer angemeldet ist, verfügt nicht über ein Home-Verzeichnis und kann nicht auf die Home-Verzeichnisse anderer Benutzer zugreifen. Es gibt vier Variablen, die bestimmen, wie ein Benutzer einem Verzeichnis zugeordnet wird:

- **Name teilen**

Dies ist der Name der Freigabe, die Sie erstellen, mit der der Benutzer eine Verbindung herstellt. Sie müssen die Home-Verzeichnis-Eigenschaft für diese Freigabe festlegen.

Der Freigabename kann die folgenden dynamischen Namen verwenden:

- %w (Der Windows-Benutzername des Benutzers)
- %d (Windows-Domain-Name des Benutzers)
- %u (Der zugewiesene UNIX-Benutzername des Benutzers) um den Freigabennamen in allen Home-Verzeichnissen eindeutig zu machen, muss der Freigabename entweder den enthalten/%w Oder im %u Variabel. Der Freigaben-Name kann beides enthalten %d Und das/%w Variable (z. B. %d/%w), oder der Freigabename kann einen statischen Teil und einen variablen Teil enthalten (z. B. Home_/%w).

- **Pfad teilen**

Dies ist der relative Pfad, der durch die Freigabe definiert wird und somit mit einem der Share-Namen verknüpft ist, der an jeden Suchpfad angehängt wird, um den gesamten Home-Directory-Pfad des Benutzers aus dem Root der SVM zu generieren. Er kann statisch sein (z.B. home), dynamisch (zum Beispiel, %w) Oder eine Kombination der beiden (zum Beispiel, eng/%w).

- **Suchpfade**

Dies ist die Gruppe der absoluten Pfade aus dem Root der SVM, die Sie angeben, dass die ONTAP-Suche nach Home Directories geleitet wird. Sie können einen oder mehrere Suchpfade mithilfe des angeben vserver cifs home-directory search-path add Befehl. Wenn Sie mehrere Suchpfade angeben, versucht ONTAP sie in der angegebenen Reihenfolge, bis ein gültiger Pfad gefunden wird.

- **Verzeichnis**

Dies ist das Home-Verzeichnis des Benutzers, das Sie für den Benutzer erstellen. Der Verzeichnisname ist normalerweise der Name des Benutzers. Sie müssen das Home-Verzeichnis in einem der Verzeichnisse erstellen, die durch die Suchpfade definiert werden.

Betrachten Sie als Beispiel die folgende Einrichtung:

- Benutzer: John Smith
- Benutzerdomäne: acme
- Benutzername: Jsmith
- SVM-Name: vs1
- Home Directory share Name #1: Home_ %w - Freigabepfad: %w
- Home-Verzeichnis Freigabename #2: %w - Freigabepfad: %d/%w
- Suchpfad #1: /vol0home/home
- Suchpfad #2: /vol1home/home
- Suchpfad #3: /vol2home/home
- Home-Verzeichnis: /vol1home/home/jsmith

Szenario 1: Der Benutzer stellt eine Verbindung her `\\vs1\home_jsmith`. Dies entspricht dem ersten Home-Verzeichnis-Freigabennamen und erzeugt den relativen Pfad `jsmith`. ONTAP sucht jetzt nach einem Verzeichnis mit dem Namen `jsmith` indem Sie die einzelnen Suchpfade in der folgenden Reihenfolge überprüfen:

- `/vol0home/home/jsmith` Ist nicht vorhanden; weiter zu Suchpfad #2.
- `/vol1home/home/jsmith` Existiert; deshalb wird der Suchpfad #3 nicht überprüft; der Benutzer ist jetzt mit seinem Home-Verzeichnis verbunden.

Szenario 2: Der Benutzer stellt eine Verbindung her `\\vs1\jsmith`. Dies entspricht dem zweiten Home-Verzeichnis-Freigabennamen und erzeugt den relativen Pfad `acme/jsmith`. ONTAP sucht jetzt nach einem Verzeichnis mit dem Namen `acme/jsmith` indem Sie die einzelnen Suchpfade in der folgenden Reihenfolge überprüfen:

- `/vol0home/home/acme/jsmith` Ist nicht vorhanden; weiter zu Suchpfad #2.
- `/vol1home/home/acme/jsmith` Ist nicht vorhanden; weiter zum Suchpfad #3.
- `/vol2home/home/acme/jsmith` Ist nicht vorhanden; das Home-Verzeichnis ist nicht vorhanden; daher schlägt die Verbindung fehl.

Home Directory-Freigaben

Fügen Sie eine Home-Directory-Freigabe hinzu

Wenn Sie die SMB-Home-Verzeichnis-Funktion verwenden möchten, müssen Sie mindestens eine Freigabe mit der Eigenschaft Home Directory hinzufügen, die in den Share-Eigenschaften enthalten ist.

Über diese Aufgabe

Sie können eine Home-Directory-Freigabe zum Zeitpunkt der Erstellung der Freigabe mit erstellen `vserver cifs share create` Befehl, oder Sie können eine vorhandene Freigabe jederzeit mit dem in ein Home Directory-Share ändern `vserver cifs share modify` Befehl.

Um eine Home-Directory-Freigabe zu erstellen, müssen Sie das einschließen `homedirectory` Wert im

`-share-properties` Option, wenn Sie eine Freigabe erstellen oder ändern. Sie können den Freigabennamen und den Freigabepfad mithilfe von Variablen angeben, die dynamisch erweitert werden, wenn Benutzer eine Verbindung zu ihren Home-Verzeichnissen herstellen. Die verfügbaren Variablen, die Sie im Pfad verwenden können, sind `%w`, `%d`, und `%u`, Entsprechend dem Windows-Benutzernamen, der Domäne und dem zugeordneten UNIX-Benutzernamen.

Schritte

1. Home Directory-Freigabe hinzufügen:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties homedirectory[,...]
```

`-vserver vserver` Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

`-share-name share-name` Gibt den Freigabennamen des Home-Verzeichnisses an.

Zusätzlich zu einer der erforderlichen Variablen, wenn der Freigabename einen der wörtlichen Zeichenfolgen enthält `%w`, `%u`, Oder `%d`, Sie müssen vor dem Literal String ein `%` (Prozent) Zeichen setzen, um zu verhindern, dass ONTAP die Zeichenfolge als Variable behandelt (z. B. `%%w`).

- Der Freigabe-Name muss entweder den enthalten `%w` Oder im `%u` Variabel.
- Der Freigabe-Name kann zusätzlich das enthalten `%d` Variable (z. B. `%d/%w`) Oder einen statischen Teil im Freigabennamen (z. B. `home1_/%w`).
- Wenn die Freigabe von Administratoren verwendet wird, um eine Verbindung zu den Home-Verzeichnissen anderer Benutzer herzustellen oder um Benutzern die Verbindung zu den Home-Verzeichnissen anderer Benutzer zu ermöglichen, muss dem dynamischen Namensmuster ein Tilde (`~`) vorangestellt sein.

Der `vserver cifs home-directory modify` Wird verwendet, um diesen Zugriff durch Festlegen der zu aktivieren `-is-home-dirs-access-for-admin-enabled` Option auf `true`) Oder durch die Einstellung der erweiterten Option `-is-home-dirs-access-for-public-enabled` Bis `true`.

`-path path` Gibt den relativen Pfad zum Home-Verzeichnis an.

`-share-properties homedirectory[,...]` Gibt die Freigabeigenschaften für diese Freigabe an. Sie müssen das angeben `homedirectory` Wert: Sie können zusätzliche Freigabeigenschaften mithilfe einer kommagetrennten Liste angeben.

1. Überprüfen Sie, ob Sie die Home-Directory-Freigabe mithilfe des erfolgreich hinzugefügt haben `vserver cifs share show` Befehl.

Beispiel

Mit dem folgenden Befehl wird eine Home Directory-Freigabe mit dem Namen erstellt `%w`. Der `oplocks`, `browsable`, und `changenotify` Freigabeigenschaften werden zusätzlich zur Einstellung des festgelegt `homedirectory` Eigenschaft freigeben.



Dieses Beispiel zeigt nicht die Ausgabe für alle Freigaben auf der SVM an. Ausgabe wird abgeschnitten.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory
```

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

Vserver	Share	Path	Properties	Comment	ACL
vs1	%w	%w	oplocks	-	Everyone / Full
Control			browsable changenotify homedirectory		

Verwandte Informationen

[Hinzufügen eines Suchpfads für das Home-Verzeichnis](#)

[Anforderungen und Richtlinien für die Nutzung automatischer Node-Empfehlungen](#)

[Management des Zugriffs auf die Home Directorys von Benutzern](#)

Für Home Directory Shares sind eindeutige Benutzernamen erforderlich

Achten Sie darauf, beim Erstellen von Home-Directory-Freigaben mit dem eindeutige Benutzernamen zuzuweisen `%w` (Windows-Benutzername) oder `%u` (UNIX-Benutzername)-Variablen zur dynamischen Generierung von Freigaben Der Freigabename wird Ihrem Benutzernamen zugeordnet.

Es können zwei Probleme auftreten, wenn der Name einer statischen Freigabe und der Name eines Benutzers identisch sind:

- Wenn der Benutzer die Freigaben auf einem Cluster mit `net view` aufführt Der Befehl zeigt zwei Freigaben mit demselben Benutzernamen an.
- Wenn der Benutzer eine Verbindung zu diesem Freigabennamen herstellt, ist der Benutzer immer mit der statischen Freigabe verbunden und kann nicht auf die Home-Directory-Freigabe mit demselben Namen zugreifen.

Beispielsweise gibt es eine Freigabe mit dem Namen „Administrator“ und Sie haben einen Windows-Benutzernamen „Administrator“. Wenn Sie eine Home-Directory-Freigabe erstellen und eine Verbindung zu dieser Freigabe herstellen, werden Sie mit der statischen Freigabe „Administrator“ und nicht mit der Home-Directory-Freigabe „Administrator“ verbunden.

Sie können das Problem durch doppelte Freigabennamen lösen, indem Sie einen der folgenden Schritte ausführen:

- Umbenennen der statischen Freigabe, sodass keine Konflikte mehr mit der Home-Directory-Freigabe des Benutzers auftreten.
- Geben Sie dem Benutzer einen neuen Benutzernamen, damit er nicht mehr mit dem statischen Freigabennamen in Konflikt steht.
- Erstellen einer CIFS-Home-Directory-Freigabe mit einem statischen Namen wie „Home“ statt mit dem `%w`

Parameter zur Vermeidung von Konflikten mit den Freigabennamen.

Was passiert mit statischen Home-Verzeichnis-Freigabennamen nach dem Upgrade

Freigabennamen für das Home-Verzeichnis müssen entweder den enthalten `%w` Oder im `%u` Dynamische Variable Sie sollten wissen, was mit bestehenden statischen Home Directory Share-Namen passiert, nachdem Sie ein Upgrade auf eine ONTAP-Version durchgeführt haben, die neue Anforderung erfordert.

Wenn die Konfiguration Ihres Home-Verzeichnisses statische Freigabennamen enthält und Sie auf ONTAP aktualisieren, werden die statischen Home-Verzeichnis-Freigabennamen nicht geändert und sind immer noch gültig. Sie können jedoch keine neuen Home-Verzeichnis-Freigaben erstellen, die keine der enthalten `%w` Oder `%u` Variabel.

Da eine dieser Variablen in den Home Directory-Freigabennamen des Benutzers enthalten ist, wird sichergestellt, dass jeder Freigabename in der Konfiguration des Home-Verzeichnisses eindeutig ist. Bei Bedarf können Sie die statischen Home-Verzeichnis-Freigabennamen in Namen ändern, die entweder den enthalten `%w` Oder `%u` Variabel.

Fügen Sie einen Suchpfad für das Home-Verzeichnis hinzu

Wenn Sie ONTAP SMB Home Directorys verwenden möchten, müssen Sie mindestens einen Suchpfad für das Home Directory hinzufügen.

Über diese Aufgabe

Sie können einen Suchpfad für das Home-Verzeichnis mit dem hinzufügen `vserver cifs home-directory search-path add` Befehl.

Der `vserver cifs home-directory search-path add` Befehl überprüft den im angegebenen Pfad `-path` Option während der Befehlsausführung. Wenn der angegebene Pfad nicht vorhanden ist, generiert der Befehl eine Meldung, in der Sie aufgefordert werden, fortzufahren. Sie entscheiden `y` Oder `n`. Wenn Sie sich entscheiden `y` Um fortzufahren, erstellt ONTAP den Suchpfad. Sie müssen jedoch die Verzeichnisstruktur erstellen, bevor Sie den Suchpfad in der Konfiguration des Home-Verzeichnisses verwenden können. Wenn Sie den Vorgang nicht fortsetzen möchten, schlägt der Befehl fehl; der Suchpfad wird nicht erstellt. Sie können dann die Struktur des Pfad-Verzeichnisses erstellen und den erneut ausführen `vserver cifs home-directory search-path add` Befehl.

Schritte

1. Hinzufügen eines Suchpfads für das Home-Verzeichnis: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Überprüfen Sie, ob Sie den Suchpfad mithilfe des erfolgreich hinzugefügt haben `vserver cifs home-directory search-path show` Befehl.

Beispiel

Im folgenden Beispiel wird der Pfad hinzugefügt `/home1` Zur Home Directory-Konfiguration auf SVM vs1.

```

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1

```

Im folgenden Beispiel wird versucht, den Pfad hinzuzufügen /home2 Zur Home Directory-Konfiguration auf SVM vs1. Der Pfad ist nicht vorhanden. Es wird die Entscheidung getroffen, nicht fortzufahren.

```

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n

```

Verwandte Informationen

[Hinzufügen einer Home-Directory-Freigabe](#)

Erstellen Sie eine Home-Verzeichnis-Konfiguration mit den Variablen %w und %d

Sie können eine Home-Verzeichnis-Konfiguration mit dem erstellen %w Und %d Variablen. Die Benutzer können sich dann mithilfe von dynamisch erstellten Shares mit ihren Home Shares verbinden.

Schritte

1. Erstellen Sie einen qtree, um die Home Directories des Benutzers zu enthalten: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Vergewissern Sie sich, dass der qtree den richtigen Sicherheitsstil verwendet: `volume qtree show`
3. Wenn der qtree nicht den gewünschten Sicherheitsstil nutzt, ändern Sie den Sicherheitsstil mithilfe von `volume qtree security` Befehl.
4. Home Directory-Freigabe hinzufügen: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

`-vserver vserver` Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

`-share-name %w` Gibt den Freigabennamen des Home-Verzeichnisses an. ONTAP erstellt den Freigabennamen dynamisch, wenn jeder Benutzer eine Verbindung zu seinem Home-Verzeichnis herstellt. Der Freigabename wird vom Formular *Windows_user_Name* sein.

`-path %d/%w` Gibt den relativen Pfad zum Home-Verzeichnis an. Der relative Pfad wird dynamisch erstellt, wenn jeder Benutzer sich mit seinem Home-Verzeichnis verbindet und aus der Form *Domain/Windows_user_Name* besteht.

`-share-properties homedirectory[,...]` + Gibt die Freigabeigenschaften für diese Freigabe an. Sie müssen das angeben `homedirectory` Wert: Sie können zusätzliche Freigabeigenschaften mithilfe einer kommagetrennten Liste angeben.

5. Stellen Sie sicher, dass die Freigabe über die gewünschte Konfiguration verfügt `vserver cifs share show` Befehl.

6. Hinzufügen eines Suchpfads für das Home-Verzeichnis: `vserver cifs home-directory search-path add -vserver vserver -path path`

`-vserver vserver-name` Gibt die SVM mit CIFS-Aktivierung an, auf der der Suchpfad hinzugefügt werden soll.

`-path path` Gibt den absoluten Verzeichnispfad zum Suchpfad an.

7. Überprüfen Sie, ob Sie den Suchpfad mithilfe des erfolgreich hinzugefügt haben `vserver cifs home-directory search-path show` Befehl.

8. Erstellen Sie bei Benutzern mit einem Home Directory ein entsprechendes Verzeichnis im qtree oder Volume, damit sie Home Directories enthalten sollen.

Wenn Sie beispielsweise einen qtree mit dem Pfad von erstellt haben `/vol/vol1/users` Und der Benutzername, dessen Verzeichnis Sie erstellen möchten, lautet `mydomain\user1`, Sie würden ein Verzeichnis mit dem folgenden Pfad erstellen: `/vol/vol1/users/mydomain/user1`.

Wenn Sie ein Volume mit dem Namen „home1“ erstellt haben, montiert bei `/home1`, Sie würden ein Verzeichnis mit dem folgenden Pfad erstellen: `/home1/mydomain/user1`.

9. Überprüfen Sie, ob ein Benutzer eine Verbindung zur Home-Share erfolgreich herstellen kann, indem Sie ein Laufwerk zuweisen oder eine Verbindung über den UNC-Pfad herstellen.

Wenn Benutzer `mydomain\user1` beispielsweise eine Verbindung zu dem in Schritt 8 erstellten Verzeichnis herstellen möchte, das sich auf SVM `vs1` befindet, würde `user1` über den UNC-Pfad verbinden `\\vs1\user1`.

Beispiel

Mit den Befehlen im folgenden Beispiel wird eine Home Directory-Konfiguration mit den folgenden Einstellungen erstellt:

- Der Freigabename ist `%w`.
- Der relative Home-Verzeichnis-Pfad lautet `%d/%w`.
- Der Suchpfad, der verwendet wird, um die Home-Verzeichnisse zu enthalten, `/home1`, ist ein Volumen, das mit NTFS-Sicherheitsstil konfiguriert ist.
- Die Konfiguration wird auf SVM `vs1` erstellt.

Sie können diese Art von Home Directory-Konfiguration verwenden, wenn Benutzer von Windows-Hosts auf ihre Home-Verzeichnisse zugreifen. Sie können diese Art der Konfiguration auch verwenden, wenn Benutzer über Windows- und UNIX-Hosts auf ihre Home Directories zugreifen, und der Dateisystemadministrator verwendet Windows-basierte Benutzer und Gruppen, um den Zugriff auf das Dateisystem zu steuern.

```

cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vsriver cifs share show -vsriver vs1 -share-name %w

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %d/%w
    Share Properties: oplocks
                    browsable
                    changenotify
                    homedirectory
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
        Volume Name: -
        Offline Files: manual
    Vscan File-Operations Profile: standard

cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1

cluster::> vsriver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1

```

Verwandte Informationen

[Konfigurieren von Home-Verzeichnissen mit der %U-Variablen](#)

[Zusätzliche Home Directory-Konfigurationen](#)

[Anzeigen von Informationen über den Home-Directory-Pfad eines SMB-Benutzers](#)

Konfigurieren Sie Home-Verzeichnisse mit der %U-Variablen

Sie können eine Home-Verzeichnis-Konfiguration erstellen, in der Sie den Freigabennamen mithilfe der angeben `%w` Variable, aber Sie verwenden die `%u` Variable zur Angabe des relativen Pfads zur Home-Directory-Freigabe. Die Benutzer können sich dann mithilfe von dynamisch mit ihrem Windows-Benutzernamen erstellten Shares mit ihren Home-Shares verbinden, ohne den tatsächlichen Namen oder Pfad des Home-Verzeichnisses kennen zu müssen.

Schritte

1. Erstellen Sie einen qtree, um die Home Directorys des Benutzers zu enthalten: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Vergewissern Sie sich, dass der qtree den richtigen Sicherheitsstil verwendet: `volume qtree show`
3. Wenn der qtree nicht den gewünschten Sicherheitsstil nutzt, ändern Sie den Sicherheitsstil mithilfe von `volume qtree security` Befehl.
4. Home Directory-Freigabe hinzufügen: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

`-vserver vserver` Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

`-share-name %w` Gibt den Freigabennamen des Home-Verzeichnisses an. Der Freigabename wird dynamisch erstellt, wenn jeder Benutzer eine Verbindung zu seinem Home-Verzeichnis herstellt und von der Form *Windows_user_Name* ist.



Sie können auch die verwenden `%u` Variable für das `-share-name` Option. Dadurch wird ein relativer Freigabepfad erstellt, der den zugeordneten UNIX-Benutzernamen verwendet.

`-path %u` Gibt den relativen Pfad zum Home-Verzeichnis an. Der relative Pfad wird dynamisch erstellt, wenn jeder Benutzer eine Verbindung zu seinem Home-Verzeichnis herstellt und von der Form *Mapping_UNIX_user_Name* ist.



Der Wert für diese Option kann auch statische Elemente enthalten. Beispiel: `eng/%u`.

`-share-properties homedirectory\[, ...\]` Gibt die Freigabeigenschaften für diese Freigabe an. Sie müssen das angeben `homedirectory` Wert: Sie können zusätzliche Freigabeigenschaften mithilfe einer kommagetrennten Liste angeben.

5. Stellen Sie sicher, dass die Freigabe über die gewünschte Konfiguration verfügt `vserver cifs share show` Befehl.
6. Hinzufügen eines Suchpfads für das Home-Verzeichnis: `vserver cifs home-directory search-path add -vserver vserver -path path`
`-vserver vserver` Gibt die SVM mit CIFS-Aktivierung an, auf der der Suchpfad hinzugefügt werden soll.
`-path path` Gibt den absoluten Verzeichnispfad zum Suchpfad an.
7. Überprüfen Sie, ob Sie den Suchpfad mithilfe des erfolgreich hinzugefügt haben `vserver cifs home-directory search-path show` Befehl.
8. Wenn der UNIX-Benutzer nicht vorhanden ist, erstellen Sie den UNIX-Benutzer mit der `vserver services unix-user create` Befehl.



Der UNIX-Benutzername, dem Sie den Windows-Benutzernamen zuordnen, muss vorhanden sein, bevor Sie den Benutzer zuordnen.

9. Erstellen Sie mit dem folgenden Befehl eine Namenszuweisung für den Windows-Benutzer für den UNIX-Benutzer: `vserver name-mapping create -vserver vserver_name -direction win-unix`

`-priority integer -pattern windows_user_name -replacement unix_user_name`



Wenn bereits Namenszuordnungen vorhanden sind, die Windows-Benutzer UNIX-Benutzern zuordnen, müssen Sie den Zuordnungsschritt nicht durchführen.

Der Windows-Benutzername wird dem entsprechenden UNIX-Benutzernamen zugeordnet. Wenn der Windows-Benutzer eine Verbindung zu seiner Home Directory-Freigabe herstellt, stellen sie eine Verbindung zu einem dynamisch erstellten Home-Verzeichnis her, das einen Share-Namen hat, der ihrem Windows-Benutzernamen entspricht, ohne zu wissen, dass der Verzeichnisname dem UNIX-Benutzernamen entspricht.

10. Erstellen Sie bei Benutzern mit einem Home Directory ein entsprechendes Verzeichnis im qtree oder Volume, damit sie Home Directories enthalten sollen.

Wenn Sie beispielsweise einen qtree mit dem Pfad von erstellt haben `/vol/voll/users` Und der zugeordnete UNIX-Benutzername des Benutzers, dessen Verzeichnis Sie erstellen möchten, ist „unixuser1“, würden Sie ein Verzeichnis mit dem folgenden Pfad erstellen:
`/vol/voll/users/unixuser1`.

Wenn Sie ein Volume mit dem Namen „home1“ erstellt haben, montiert bei `/home1`, Sie würden ein Verzeichnis mit dem folgenden Pfad erstellen: `/home1/unixuser1`.

11. Überprüfen Sie, ob ein Benutzer eine Verbindung zur Home-Share erfolgreich herstellen kann, indem Sie ein Laufwerk zuweisen oder eine Verbindung über den UNC-Pfad herstellen.

Beispiel: Wenn Benutzer `mydomain\user1` UNIX-Benutzer `unixuser1` zuordnet und eine Verbindung zu dem in Schritt 10 erstellten Verzeichnis herstellen möchte, das sich auf SVM `vs1` befindet, würde `user1` über den UNC-Pfad verbinden `\\vs1\user1`.

Beispiel

Mit den Befehlen im folgenden Beispiel wird eine Home Directory-Konfiguration mit den folgenden Einstellungen erstellt:

- Der Freigabename ist `%w`.
- Der relative Home-Verzeichnis-Pfad ist `%u`.
- Der Suchpfad, der verwendet wird, um die Home-Verzeichnisse zu enthalten, `/home1`, Ist ein Volume, das mit UNIX-Sicherheitsstil konfiguriert ist.
- Die Konfiguration wird auf SVM `vs1` erstellt.

Sie können diese Art der Home Directory-Konfiguration verwenden, wenn Benutzer von Windows-Hosts oder Windows- und UNIX-Hosts auf ihre Home Directories zugreifen. Der Dateisystemadministrator verwendet UNIX-basierte Benutzer und Gruppen, um den Zugriff auf das Dateisystem zu steuern.

```

cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

          Vserver: vs1
          Share: %w
CIFS Server NetBIOS Name: VS1
          Path: %u
    Share Properties: oplocks
                    browsable
                    changenotify
                    homedirectory
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver      Position Path
-----
vs1          1      /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver      Direction Position
-----
vs1          win-unix  5      Pattern: user1
                    Replacement: unixuser1

```

Verwandte Informationen

[Erstellen einer Home-Verzeichnis-Konfiguration unter Verwendung der Variablen %w und %d](#)

[Zusätzliche Home Directory-Konfigurationen](#)

[Anzeigen von Informationen über den Home-Directory-Pfad eines SMB-Benutzers](#)

Zusätzliche Home Directory-Konfigurationen

Mit dem können Sie zusätzliche Home-Verzeichnis-Konfigurationen erstellen `%w`, `%d`, und `%u` Variablen, mit denen Sie die Konfiguration des Home-Verzeichnisses an Ihre Anforderungen anpassen können.

Sie können in den Freigabenamen und Suchpfaden eine Reihe von Home-Verzeichnis-Konfigurationen erstellen, indem Sie Variablen und statische Zeichenfolgen kombinieren. Die folgende Tabelle enthält einige Beispiele zur Erstellung verschiedener Home Directory-Konfigurationen:

Pfade, die beim Erstellen von sind /voll/user Enthält Home Directories...	Freigabbefehl...
Um einen Freigabepfad zu erstellen \\vs1\~win_username Das führt den Benutzer an /voll/user/win_username	<code>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory</code>
Um einen Freigabepfad zu erstellen \\vs1\win_username Das führt den Benutzer an /voll/user/domain/win_username	<code>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory</code>
Um einen Freigabepfad zu erstellen \\vs1\win_username Das führt den Benutzer an /voll/user/unix_username	<code>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>
Um einen Freigabepfad zu erstellen \\vs1\unix_username Das führt den Benutzer an /voll/user/unix_username	<code>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>

Befehle zum Verwalten von Suchpfaden

Es gibt bestimmte ONTAP-Befehle zum Managen von Suchpfaden für SMB Home Directory-Konfigurationen. Beispielsweise gibt es Befehle zum Hinzufügen, Entfernen und Anzeigen von Informationen zu Suchpfaden. Es gibt auch einen Befehl zum Ändern der Suchpfadreihenfolge.

Ihr Ziel ist	Befehl
Fügen Sie einen Suchpfad hinzu	<code>vserver cifs home-directory search-path add</code>
Suchpfade anzeigen	<code>vserver cifs home-directory search-path show</code>

Ihr Ziel ist	Befehl
Ändern Sie die Suchpfadreihenfolge	<code>vserver cifs home-directory search-path reorder</code>
Suchpfad entfernen	<code>vserver cifs home-directory search-path remove</code>

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

Zeigt Informationen zum Home-Verzeichnis-Pfad eines SMB-Benutzers an

Auf der Storage Virtual Machine (SVM) kann der Home Directory-Pfad eines SMB-Benutzers angezeigt werden. Dieser kann verwendet werden, wenn mehrere CIFS-Home-Verzeichnis-Pfade konfiguriert sind und Sie sehen möchten, welcher Pfad das Home Directory des Benutzers enthält.

Schritt

1. Zeigen Sie den Pfad des Home-Verzeichnisses mit dem `vserver cifs home-directory show-user` Befehl.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

Vserver	User	Home Dir Path
-----	-----	-----
vs1	user1	/home/user1

Verwandte Informationen

[Management des Zugriffs auf die Home Directories von Benutzern](#)

Managen des Zugriffs auf die Home Directories von Benutzern

Standardmäßig kann nur von diesem Benutzer auf das Home-Verzeichnis eines Benutzers zugegriffen werden. Für Freigaben, für die der dynamische Name der Freigabe mit einem Tilde (~) vorangestellt ist, können Sie den Zugriff auf die Home-Verzeichnisse von Windows-Administratoren oder von jedem anderen Benutzer (öffentlicher Zugriff) aktivieren oder deaktivieren.

Bevor Sie beginnen

Die Home Directory-Freigaben auf der Storage Virtual Machine (SVM) müssen mit dynamischen Freigabennamen konfiguriert werden, denen ein Tilde (~) vorangestellt ist. In den folgenden Fällen werden die Anforderungen für die Benennung von Freigaben dargestellt:

Freigabename für das Home-Verzeichnis	Beispiel für Befehl zur Verbindung mit der Freigabe
~%d~%w	net use * \\IPAddress\~domain~user/u:credentials
~%w	net use * \\IPAddress\~user/u:credentials
~abc~%w	net use * \\IPAddress\abc~user/u:credentials

Schritt

1. Führen Sie die entsprechende Aktion aus:

Wenn Sie den Zugriff auf die Home Directories von Benutzern aktivieren oder deaktivieren möchten,	Geben Sie Folgendes ein...
Windows Administratoren	vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true false}`Die Standardeinstellung lautet `true.
Alle Benutzer (öffentlicher Zugriff)	<ol style="list-style-type: none"> a. Stellen Sie die Berechtigungsebene auf Erweitert: + ein set -privilege advanced b. Zugriff aktivieren oder deaktivieren: `vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-public-enabled {true

Das folgende Beispiel ermöglicht den öffentlichen Zugriff auf die Home Directories von Benutzern:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Verwandte Informationen

[Anzeigen von Informationen über den Home-Directory-Pfad eines SMB-Benutzers](#)

Konfigurieren Sie den SMB-Client-Zugriff auf symbolische UNIX-Links

Wie ONTAP Ihnen ermöglicht, symbolischen UNIX-Links SMB-Client-Zugriff bereitzustellen

Ein symbolischer Link ist eine Datei, die in einer UNIX-Umgebung erstellt wird, die einen

Verweis auf eine andere Datei oder ein anderes Verzeichnis enthält. Wenn ein Client auf eine symbolische Verbindung zugreift, wird der Client an die Zieldatei oder das Verzeichnis weitergeleitet, auf die sich der symbolische Link bezieht. ONTAP unterstützt relative und absolute symbolische Links, einschließlich widelinks (absolute Links mit Zielen außerhalb des lokalen Filesystems).

Mit ONTAP können SMB-Clients symbolische UNIX-Links verfolgen, die auf der SVM konfiguriert sind. Diese Funktion ist optional, und Sie können sie über das pro-Share konfigurieren `-symlink-properties` Option des `vserver cifs share create` Befehl, mit einer der folgenden Einstellungen:

- Aktiviert mit Lese-/Schreibzugriff
- Mit schreibgeschütztem Zugriff aktiviert
- Deaktiviert, indem symbolische Links von SMB-Clients ausgeblendet werden
- Deaktiviert ohne Zugriff auf symbolische Links von SMB-Clients

Wenn Sie symbolische Links auf einer Freigabe aktivieren, funktionieren relative symbolische Links ohne weitere Konfiguration.

Wenn Sie symbolische Links auf einer Share aktivieren, funktionieren absolute symbolische Links nicht sofort. Sie müssen zuerst eine Zuordnung zwischen dem UNIX-Pfad der symbolischen Verbindung zum Ziel-SMB-Pfad erstellen. Beim Erstellen der absoluten symbolischen Link-Zuordnungen können Sie angeben, ob es ein lokaler Link oder ein *widelinks* ist; *widelinks* kann zu Dateisystemen auf anderen Speichergeräten oder Links zu Dateisystemen sein, die in separaten SVMs auf demselben ONTAP-System gehostet werden. Wenn Sie eine *widelink* erstellen, muss sie die Informationen enthalten, denen der Client folgen kann; das heißt, Sie erstellen einen Analysepunkt für den Client, um den Verzeichnispunkt zu ermitteln. Wenn Sie einen absoluten symbolischen Link zu einer Datei oder einem Verzeichnis außerhalb der lokalen Freigabe erstellen, aber die Lokalität auf lokal setzen, lässt ONTAP den Zugriff auf das Ziel nicht zu.



Wenn ein Client versucht, einen lokalen symbolischen Link zu löschen (absolut oder relativ), wird nur der symbolische Link gelöscht, nicht die Zieldatei oder das Zielverzeichnis. Wenn ein Kunde jedoch versucht, eine *widelink* zu löschen, kann die tatsächliche Zieldatei oder das Verzeichnis, auf das sich der *widelink* bezieht, gelöscht werden. ONTAP hat keine Kontrolle darüber, da der Client die Zieldatei oder das Zielverzeichnis außerhalb der SVM explizit öffnen und löschen kann.

• Reparse-Punkte und ONTAP-Dateisystemdienste

Ein *Analysepunkt* ist ein NTFS-Dateisystem-Objekt, das optional zusammen mit einer Datei auf dem Volumen gespeichert werden kann. Durch die Analysepunkte können SMB-Clients bei der Arbeit mit NTFS-Style-Volumen erweiterte oder erweiterte Dateisystemservices erhalten. Die Analysepunkte bestehen aus Standard-Tags, die den Typ des Analysepunkts identifizieren und den Inhalt des Reparse-Punkts, der von SMB-Clients zur weiteren Verarbeitung durch den Client abgerufen werden kann. Von den Objekttypen, die für erweiterte Dateisystemfunktionen verfügbar sind, implementiert ONTAP die Unterstützung für NTFS-symbolische Links und Verzeichnispunkte mithilfe von Reparse Point-Tags. SMB-Clients, die den Inhalt eines Analysepunkts nicht verstehen können, ignorieren ihn einfach und geben den erweiterten Dateisystem-Service nicht an, den der Analysepunkt möglicherweise aktiviert.

• Directory-Verbindungspunkte und ONTAP-Unterstützung für symbolische Links

Verzeichnis-Verbindungspunkte sind Standorte innerhalb einer Dateisystemverzeichnisstruktur, die sich auf alternative Speicherorte beziehen kann, entweder auf einem anderen Pfad (symbolische Links) oder auf ein separates Speichergerät (*widelinks*). ONTAP SMB Server stellen für Windows-Clients

Verbindungspunkte als Analysepunkte bereit, sodass Clients bei einem Umfahren eines Verzeichnispunkts Inhalte von ONTAP neu analysieren können. Sie können dadurch navigieren und eine Verbindung zu verschiedenen Pfaden oder Speichergeräten herstellen, als wären sie Teil des gleichen Dateisystems.

- **Aktivierung der widelink-Unterstützung mit den Optionen für das Analysieren von Punkten**


Der `-is-use-junctions-as-reparse-points-enabled` Die Option ist standardmäßig in ONTAP 9 aktiviert. Nicht alle SMB-Clients unterstützen widelinks, sodass die Informationen per Protokoll-Version konfigurierbar sind, so dass Administratoren sowohl unterstützte als auch nicht unterstützte SMB-Clients nutzen können. In ONTAP 9.2 und neueren Versionen müssen Sie die Option aktivieren `-widelink-as-reparse-point-versions` Für jedes Client-Protokoll, das mit widelinks auf die Freigabe zugreift; der Standard ist SMB1. In früheren Versionen wurden nur widelinks berichtet, auf die mit dem Standard SMB1 zugegriffen wurde, und Systeme mit SMB2 oder SMB3 konnten nicht auf die widelinks zugreifen.

Weitere Informationen finden Sie in der Microsoft NTFS-Dokumentation.

["Microsoft Dokumentation: Parsen Von Punkten"](#)

Einschränkungen bei der Konfiguration von symbolischen UNIX-Links für SMB-Zugriff

Beim Konfigurieren von symbolischen UNIX-Links für SMB-Zugriff müssen Sie sich über bestimmte Einschränkungen im Klaren sein.

Grenze	Beschreibung
45	<p>Maximale Länge des CIFS-Servernamens, den Sie angeben können, wenn Sie einen FQDN für den CIFS-Servernamen verwenden.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-left: 20px;">  Alternativ können Sie den CIFS-Servernamen als NetBIOS-Name angeben, der auf 15 Zeichen beschränkt ist. </div>
80	Maximale Länge des Freigabennamens.
256	<p>Maximale Länge des UNIX-Pfads, den Sie beim Erstellen eines symbolischen Links oder beim Ändern des UNIX-Pfads eines vorhandenen symbolischen Links angeben können. Der UNIX-Pfad muss mit einem "/" beginnen und mit einem "/" enden. Sowohl der Anfang als auch der letzte Schrägstrich zählen als Teil des 256-stelligen Limits.</p>

Grenze	Beschreibung
256	Maximale Länge des CIFS-Pfads, den Sie beim Erstellen eines symbolischen Links oder beim Ändern des CIFS-Pfads einer vorhandenen symbolischen Verbindung angeben können. Der CIFS-Pfad muss mit einem "/" beginnen und mit "/" enden. Sowohl der Anfang als auch der letzte Schrägstrich zählen als Teil des 256-stelligen Limits.

Verwandte Informationen

[Erstellen von symbolischen Link-Zuordnungen für SMB-Freigaben](#)

Steuerung der automatischen DFS-Anzeigen in ONTAP mit einer CIFS-Serveroption

Über eine CIFS-Serveroption wird festgelegt, wie DFS-Funktionen bei der Verbindung zu Freigaben an SMB-Clients weitergegeben werden. Da ONTAP DFS-Empfehlungen verwendet, wenn Clients auf symbolische Links über SMB zugreifen, sollten Sie sich bewusst sein, welche Auswirkungen bei der Deaktivierung oder Aktivierung dieser Option haben.

Über eine CIFS-Serveroption wird festgelegt, ob die CIFS-Server automatisch angeben, dass sie für SMB-Clients DFS-fähig sind. Standardmäßig ist diese Option aktiviert, und der CIFS-Server gibt immer an, dass es DFS-fähig ist für SMB-Clients (auch wenn die Verbindung zu Freigaben deaktiviert ist, wenn der Zugriff auf symbolische Links deaktiviert ist). Wenn Sie möchten, dass der CIFS-Server anwirbt, dass er für Clients nur dann geeignet ist, wenn sie eine Verbindung zu Freigaben herstellen, in denen der Zugriff auf symbolische Links aktiviert ist, können Sie diese Option deaktivieren.

Beachten Sie, was passiert, wenn diese Option deaktiviert ist:

- Die Share-Konfigurationen für symbolische Links bleiben unverändert.
- Wenn der Freigabeparameter den symbolischen Link-Zugriff zulässt (entweder Lese-/Schreibzugriff oder schreibgeschützter Zugriff), gibt der CIFS-Server DFS-Funktionen für Clients an, die eine Verbindung zu dieser Freigabe herstellen.

Client-Verbindungen und Zugang zu symbolischen Links werden ohne Unterbrechung fortgesetzt.

- Wenn der Share-Parameter auf keinen symbolischen Link-Zugriff (entweder durch Deaktivieren des Zugriffs oder wenn der Wert für den Share-Parameter Null ist) eingestellt ist, gibt der CIFS-Server DFS-Funktionen nicht an Clients weiter, die eine Verbindung zu dieser Freigabe herstellen.

Da Clients Informationen im Cache haben, die der CIFS-Server DFS-fähig ist und es nicht mehr Werbung für diese ist, können Clients, die mit Shares verbunden sind, bei denen der symbolische Link-Zugriff deaktiviert ist, möglicherweise nicht auf diese Freigaben zugreifen, nachdem die CIFS-Server-Option deaktiviert ist. Nachdem die Option deaktiviert ist, müssen Sie möglicherweise Clients neu starten, die mit diesen Freigaben verbunden sind. Dadurch werden die zwischengespeicherten Informationen gelöscht.

Diese Änderungen gelten nicht für SMB 1.0-Verbindungen.

Konfigurieren Sie die Unterstützung für symbolische UNIX-Links auf SMB-Freigaben

Sie können die Unterstützung für symbolische UNIX-Links auf SMB-Freigaben konfigurieren, indem Sie beim Erstellen von SMB-Freigaben oder jederzeit durch Ändern vorhandener SMB-Freigaben eine Einstellung für die symbolische Link-Freigabe angeben. Die Unterstützung für symbolische UNIX-Links ist standardmäßig aktiviert. Sie können auch die Unterstützung für symbolische UNIX-Links auf einer Freigabe deaktivieren.

Über diese Aufgabe

Wenn Sie UNIX-Unterstützung für symbolische Links für SMB-Freigaben konfigurieren, können Sie eine der folgenden Einstellungen wählen:

Einstellung	Beschreibung
<code>enable</code> (VERALTET*)	Gibt an, dass symbolische Links für den Lese-Schreib-Zugriff aktiviert sind.
<code>read_only</code> (VERALTET*)	Gibt an, dass Symlinks für schreibgeschützten Zugriff aktiviert sind. Diese Einstellung gilt nicht für widelinks. Widelink-Zugriff ist immer schreibgeschützt.
<code>hide</code> (VERALTET*)	Gibt an, dass SMB-Clients Symlinks nicht sehen können.
<code>no-strict-security</code>	Gibt an, dass Clients außerhalb der Freigabegrenzen Symlinks verfolgen.
<code>symlinks</code>	Gibt an, dass Symlinks lokal für Lese-/Schreibzugriff aktiviert werden. Die DFS-Werbeanzeigen werden nicht erzeugt, auch wenn die CIFS-Option verwendet wird <code>is-advertise-dfs-enabled</code> Ist auf festgelegt <code>true</code> . Dies ist die Standardeinstellung.
<code>symlinks-and-widelinks</code>	Gibt an, dass sowohl lokale Symlinks als auch widelinks für den Lese-Schreib-Zugriff sind. Die DFS-Anzeigen werden sowohl für lokale Symlink- als auch für widelinks erzeugt, auch wenn die CIFS-Option ist <code>is-advertise-dfs-enabled</code> Ist auf festgelegt <code>false</code> .
<code>disable</code>	Gibt an, dass <code>symlinks</code> und <code>widelinks</code> deaktiviert sind. Die DFS-Werbeanzeigen werden nicht erzeugt, auch wenn die CIFS-Option verwendet wird <code>is-advertise-dfs-enabled</code> Ist auf festgelegt <code>true</code> .
<code>""</code> (Null, nicht gesetzt)	Deaktiviert symbolische Verknüpfungen auf der Freigabe.

Einstellung	Beschreibung
- (Nicht eingestellt)	Deaktiviert symbolische Verknüpfungen auf der Freigabe.



*Die Parameter *enable*, *hide* und *read-only* sind veraltet und können in einer zukünftigen Version von ONTAP entfernt werden.

Schritte

1. Konfigurieren oder Deaktivieren der Unterstützung für symbolische Links:

Falls es so ist...	Eingeben...
Ein neuer SMB-Share	<code>`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable</code>
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},...]+`	Ein vorhandener SMB-Share
<code>`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable</code>	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},...]+`

2. Vergewissern Sie sich, dass die Konfiguration der SMB-Freigabe korrekt ist: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Beispiel

Mit dem folgenden Befehl wird eine SMB-Freigabe mit dem Namen „data1“ erstellt, bei der die UNIX-Konfiguration als symbolischer Link festgelegt ist `enable`:

```

cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                Vserver: vs1
                Share: data1
CIFS Server NetBIOS Name: VS1
                Path: /data1
                Share Properties: oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
                File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
                Vscan File-Operations Profile: standard
                Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -

```

Verwandte Informationen

[Erstellen von symbolischen Link-Zuordnungen für SMB-Freigaben](#)

Erstellen Sie symbolische Link-Zuordnungen für SMB-Freigaben

Sie können Zuordnungen von UNIX-symbolischen Links für SMB-Freigaben erstellen. Sie können entweder einen relativen symbolischen Link erstellen, der sich auf die Datei oder den Ordner bezogen auf den übergeordneten Ordner bezieht, oder Sie können einen absoluten symbolischen Link erstellen, der sich auf die Datei oder den Ordner mit einem absoluten Pfad bezieht.

Über diese Aufgabe

Auf Widelinks kann von Mac OS X-Clients nicht zugegriffen werden, wenn Sie SMB 2.x verwenden. Wenn ein Benutzer versucht, eine Verbindung zu einer Freigabe mit widelinks von einem Mac OS X Client herzustellen, schlägt der Versuch fehl. Sie können jedoch widelinks mit Mac OS X Clients verwenden, wenn Sie SMB 1 nutzen.

Schritte

1. So erstellen Sie symbolische Link-Zuordnungen für SMB-Freigaben: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-`

```
directory {true|false}}
```

`-vserver virtual_server_name` Gibt den Namen der Storage Virtual Machine (SVM) an.

`-unix-path path` Gibt den UNIX-Pfad an. Der UNIX-Pfad muss mit einem Schrägstrich beginnen (/) Und muss mit einem Schrägstrich enden (/).

`-share-name share_name` Gibt den Namen der zu mappenden SMB-Freigabe an.

`-cifs-path path` Gibt den CIFS-Pfad an. Der CIFS-Pfad muss mit einem Schrägstrich beginnen (/) Und muss mit einem Schrägstrich enden (/).

`-cifs-server server_name` Gibt den Namen des CIFS-Servers an. Der CIFS-Servername kann als DNS-Name (z. B. mynetwork.cifs.server.com), IP-Adresse oder NetBIOS-Name angegeben werden. Der NetBIOS-Name kann mithilfe des ermittelten `vserver cifs show` Befehl. Wenn dieser optionale Parameter nicht angegeben wird, ist der Standardwert der NetBIOS-Name des lokalen CIFS-Servers.

`-locality local|free|widelink` Gibt an, ob ein lokaler Link, ein freier Link oder ein breiter symbolischer Link erstellt werden soll. Ein lokaler symbolischer Link ordnet der lokalen SMB-Freigabe zu. Ein kostenloser symbolischer Link kann überall auf dem lokalen SMB-Server zugeordnet werden. Ein großer symbolischer Link ordnet jede SMB-Freigabe im Netzwerk zu. Wenn Sie diesen optionalen Parameter nicht angeben, wird der Standardwert verwendet `local`.

`-home-directory true false` Gibt an, ob es sich bei der Zielfreigabe um ein Home-Verzeichnis handelt. Obwohl dieser Parameter optional ist, müssen Sie diesen Parameter auf festlegen `true` Wenn die Zielfreigabe als Home-Verzeichnis konfiguriert ist. Die Standardeinstellung lautet `false`.

Beispiel

Mit dem folgenden Befehl wird eine symbolische Link-Zuordnung auf der SVM mit dem Namen `vs1` erstellt. Es gibt den UNIX Pfad `/src/`, Der SMB-Share-Name „SOURCE“, der CIFS-Pfad `/mycompany/source/`, Und die CIFS-Server IP-Adresse `123.123.123.123`, und es ist ein `widelink`.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Verwandte Informationen

[Konfiguration der Unterstützung für symbolische UNIX-Links auf SMB-Freigaben](#)

Befehle zum Verwalten von symbolischen Link-Zuordnungen

Es gibt bestimmte ONTAP-Befehle zum Verwalten von symbolischen Link-Zuordnungen.

Ihr Ziel ist	Befehl
Erstellen Sie eine symbolische Link-Zuordnung	<code>vserver cifs symlink create</code>
Informationen zu symbolischen Link-Zuordnungen anzeigen	<code>vserver cifs symlink show</code>

Ihr Ziel ist	Befehl
Ändern Sie eine symbolische Verbindungszuordnung	<code>vserver cifs symlink modify</code>
Löschen Sie eine symbolische Link-Zuordnung	<code>vserver cifs symlink delete</code>

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

Mit BranchCache werden SMB-Inhalte im Cache für die gemeinsame Nutzung an externen Standorten gespeichert

Verwenden Sie BranchCache, um SMB-Inhalte im Cache zu speichern, um Inhalte gemeinsam in Zweigstellen zu nutzen

BranchCache wurde von Microsoft entwickelt, um die lokale Cache-Speicherung von Inhalten auf Computern für die Anforderung von Clients zu ermöglichen. ONTAP Implementierung von BranchCache senkt die WAN-Auslastung (Wide Area Network) und sorgt für bessere Zugriffszeiten, wenn Benutzer in Zweigstellen mithilfe von SMB auf Inhalte zugreifen, die auf Storage Virtual Machines (SVMs) gespeichert sind.

Wenn Sie BranchCache konfigurieren, werden Inhalte von Windows BranchCache Clients zuerst von der SVM abgerufen und dann der Inhalt auf einem Computer innerhalb der Zweigstelle zwischengespeichert. Falls ein anderer mit BranchCache aktivierter Client in der Zweigstelle denselben Inhalt anfordert, authentifiziert die SVM zunächst und autorisiert den gewünschten Benutzer. Die SVM bestimmt dann, ob der gecachte Inhalt noch immer aktuell ist und sendet die Client-Metadaten zum zwischengespeicherten Inhalt. Der Client verwendet dann die Metadaten, um Inhalte direkt aus dem lokalen Cache abzurufen.

Verwandte Informationen

[Verwendung von Offline-Dateien, um das Caching von Dateien für die Offline-Verwendung zu ermöglichen](#)

Anforderungen und Richtlinien

Unterstützung der BranchCache-Version

Beachten Sie, welche BranchCache-Versionen ONTAP unterstützen.

ONTAP unterstützt BranchCache 1 und den erweiterten BranchCache 2:

- Wenn Sie BranchCache auf dem SMB-Server für die Storage Virtual Machine (SVM) konfigurieren, können Sie BranchCache 1, BranchCache 2 oder alle Versionen aktivieren.

Standardmäßig sind alle Versionen aktiviert.

- Wenn Sie nur BranchCache 2 aktivieren, müssen die Windows-Client-Rechner an Remote-Standorten BranchCache 2 unterstützen.

Nur SMB 3.0 oder höher unterstützt BranchCache 2.

Weitere Informationen zu BranchCache-Versionen finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Anforderungen an die Unterstützung des Netzwerkprotokolls

Sie müssen die Netzwerkprotokollanforderungen für die Implementierung von ONTAP BranchCache kennen.

Die ONTAP BranchCache Funktion lässt sich über IPv4- und IPv6-Netzwerke mit SMB 2.1 oder höher implementieren.

Alle CIFS-Server und Zweigstellenmaschinen, die an der BranchCache-Implementierung beteiligt sind, müssen das SMB 2.1- oder höher-Protokoll aktivieren. SMB 2.1 verfügt über Protokollerweiterungen, mit denen Kunden an einer BranchCache Umgebung teilnehmen können. Dies ist die SMB-Mindestprotokollversion, die Unterstützung von BranchCache bietet. SMB 2.1 unterstützt Version BranchCache Version 1.

Wenn Sie BranchCache Version 2 verwenden möchten, ist SMB 3.0 die minimal unterstützte Version. Alle CIFS-Server und Maschinen in Zweigstellen, die an einer BranchCache 2-Implementierung beteiligt sind, müssen SMB 3.0 oder höher aktivieren.

Wenn Kunden über Remote-Standorte verfügen, wo einige Clients nur SMB 2.1 unterstützen, und einige der Clients zudem SMB 3.0 unterstützen, können sie eine BranchCache-Konfiguration auf dem CIFS-Server implementieren, die Caching-Unterstützung über BranchCache 1 und BranchCache 2 bietet.



Obwohl die Microsoft BranchCache Funktion sowohl die HTTP-/HTTPS- als auch SMB-Protokolle als Dateizugriffsprotokolle unterstützt, unterstützt ONTAP BranchCache nur die Verwendung von SMB.

Versionsanforderungen für ONTAP und Windows Hosts

ONTAP und Windows-Hosts in Zweigstellen müssen bestimmte Versionsanforderungen erfüllen, bevor BranchCache konfiguriert werden kann.

Bevor Sie BranchCache konfigurieren, müssen Sie sicherstellen, dass die ONTAP Version auf dem Cluster und die teilnehmenden Zweigstellen-Clients SMB 2.1 oder höher unterstützen und die BranchCache Funktion unterstützen. Wenn Sie den Hosted Cache-Modus konfigurieren, müssen Sie außerdem sicherstellen, dass Sie einen unterstützten Host für den Cache-Server verwenden.

BranchCache 1 wird auf den folgenden ONTAP-Versionen und Windows-Hosts unterstützt:

- Content Server: Storage Virtual Machine (SVM) mit ONTAP
- Cache Server: Windows Server 2008 R2 oder Windows Server 2012 oder höher
- Peer oder Client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 oder Windows Server 2012 oder höher

BranchCache 2 wird auf den folgenden ONTAP-Versionen und Windows-Hosts unterstützt:

- Content Server: SVM mit ONTAP
- Cache-Server: Windows Server 2012 oder höher
- Peer oder Client: Windows 8 oder Windows Server 2012 oder höher

Aktuelle Informationen dazu, welche Windows Clients BranchCache unterstützen, finden Sie in der Interoperabilitäts-Matrix.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

Gründe, warum ONTAP BranchCache Hash-Werte für ungültig erklärt

Wenn Sie Ihre BranchCache-Konfiguration planen, sollten Sie die Gründe verstehen, warum ONTAP-Hash-Funktionen als ungültig erklärt werden. Es hilft Ihnen bei der Entscheidung, welchen Betriebsmodus Sie konfigurieren sollten, und unterstützt Sie bei der Auswahl, auf welchen Freigaben BranchCache aktiviert werden soll.

ONTAP muss die Hash-Werte von BranchCache managen, um die Gültigkeit von Hashes zu gewährleisten. Wenn ein Hash nicht gültig ist, ungültig ONTAP den Hash und berechnet bei der nächsten Anforderung einen neuen Hash. Dabei wird davon ausgegangen, dass BranchCache weiterhin aktiviert ist.

ONTAP erklärt Hashes aus den folgenden Gründen für ungültig:

- Der Serverschlüssel wird geändert.

Wenn der Serverschlüssel geändert wird, setzt ONTAP alle Hashes im Hash-Speicher ungültig.

- Ein Hash wird aus dem Cache entfernt, da die maximale Größe des BranchCache-Hash-Speichers erreicht wurde.

Dieser Parameter ist abstimmbar und kann entsprechend Ihren geschäftlichen Anforderungen angepasst werden.

- Eine Datei wird entweder über SMB- oder NFS-Zugriff geändert.
- Eine Datei, für die es berechnete Hashes gibt, wird mit dem wiederhergestellt `snap restore` Befehl.
- Ein Volume mit SMB-Freigaben, die für BranchCache aktiviert sind, wird mithilfe der wiederhergestellt `snap restore` Befehl.

Richtlinien für die Auswahl des Hash-Speicherorts

Bei der Konfiguration von BranchCache legen Sie fest, wo Hashes gespeichert werden sollen und welche Größe der Hash-Speicher sein soll. Wenn Sie die Richtlinien bei der Auswahl des Hash-Speicherorts und der Größe kennen, können Sie Ihre BranchCache-Konfiguration auf einer CIFS-fähigen SVM planen.

- Sie sollten den Hash-Speicher auf einem Volume suchen, in dem `atime-Updates` zulässig sind.

Die Zugriffszeit einer Hash-Datei wird verwendet, um häufig verwendete Dateien im Hash-Speicher zu speichern. Wenn `atime-Updates` deaktiviert sind, wird die Erstellungszeit für diesen Zweck verwendet. Es ist vorzuziehen, Zeit zu verwenden, um häufig verwendete Dateien zu verfolgen.

- Es können keine Hash-Werte auf schreibgeschützte Dateisysteme wie SnapMirror Ziele und SnapLock Volumes gespeichert werden.
- Wenn die maximale Größe des Hash-Speichers erreicht ist, werden ältere Hashes gespült, um Platz für neue Hashes zu schaffen.

Sie können die maximale Größe des Hash-Speichers erhöhen, um die Menge an Hashes zu reduzieren,

die aus dem Cache gespült werden.

- Wenn das Volume, auf dem Sie Hashes speichern, nicht verfügbar oder vollständig ist oder wenn es zu Problemen mit der Cluster-internen Kommunikation kommt, bei der der BranchCache-Dienst keine Hash-Informationen abrufen kann, stehen die BranchCache-Services nicht zur Verfügung.

Das Volume ist möglicherweise nicht verfügbar, da es offline ist oder weil der Storage-Administrator einen neuen Speicherort für den Hash-Speicher angegeben hat.

Dies verursacht keine Probleme mit dem Dateizugriff. Wenn der Zugriff auf den Hash-Speicher behindert wird, gibt ONTAP dem Client einen Microsoft-definierten Fehler zurück, der dazu führt, dass der Client die Datei mithilfe der normalen SMB-Leseanforderung anfordert.

Verwandte Informationen

[Konfigurieren Sie BranchCache auf dem SMB-Server](#)

[Ändern der BranchCache-Konfiguration](#)

Empfehlungen für BranchCache

Bevor Sie BranchCache konfigurieren, sollten Sie bestimmte Empfehlungen bei der Entscheidung, welche SMB-Freigaben Sie BranchCache Caching aktivieren möchten, im Hinterkopf behalten.

Bei der Entscheidung, welchen Betriebsmodus Sie verwenden möchten, und bei welchen SMB-Freigaben BranchCache aktiviert werden soll, sollten Sie die folgenden Empfehlungen beachten:

- BranchCache bringt Vorteile, wenn die Daten häufiger Remote-Cache-Änderungen gespeichert werden.
- BranchCache Services profitieren von Freigaben, die Dateiinhalte enthalten, die von mehreren Remote-Clients wiederverwendet oder durch Dateiinhalte verwendet werden, auf die ein einzelner Remote-Benutzer wiederholt Zugriff hat.
- Erwägen Sie die Aktivierung von Caching für schreibgeschützte Inhalte, wie z. B. Daten in Snapshot Kopien und SnapMirror Zielen.

Konfigurieren Sie BranchCache

BranchCache Übersicht konfigurieren

Sie konfigurieren BranchCache auf Ihrem SMB-Server mithilfe von ONTAP-Befehlen. Zur Implementierung von BranchCache müssen Sie auch Ihre Clients und optional die gehosteten Cache-Server in den Zweigstellen konfigurieren, an denen Inhalte zwischengespeichert werden sollen.

Wenn Sie BranchCache so konfigurieren, dass Caching auf Share-by-Share-Basis aktiviert wird, müssen Sie BranchCache auf den SMB-Freigaben aktivieren, für die BranchCache Caching-Services bereitgestellt werden sollen.

Anforderungen für die Konfiguration von BranchCache

Nachdem Sie einige Voraussetzungen erfüllt haben, können Sie BranchCache einrichten.

Vor der Konfiguration von BranchCache auf dem CIFS-Server für die SVM müssen die folgenden Anforderungen erfüllt werden:

- ONTAP muss auf allen Nodes im Cluster installiert sein.
- CIFS muss lizenziert sein und ein CIFS-Server konfiguriert sein.
- IPv4- oder IPv6-Netzwerkonnktivität muss konfiguriert sein.
- Für BranchCache 1 muss SMB 2.1 oder höher aktiviert sein.
- Für BranchCache 2 muss SMB 3.0 aktiviert sein, und die Remote-Windows-Clients müssen BranchCache 2 unterstützen.

Konfigurieren Sie BranchCache auf dem SMB-Server

BranchCache lässt sich so konfigurieren, dass BranchCache-Services pro Freigabe bereitgestellt werden. Alternativ können Sie BranchCache so konfigurieren, dass das Caching automatisch auf allen SMB-Freigaben aktiviert wird.

Über diese Aufgabe

BranchCache auf SVMs lassen sich konfigurieren.

- Sie können eine Konfiguration mit ausschließlich Freigaben für BranchCache erstellen, wenn sie Caching-Services für alle Inhalte anbieten möchten, die in allen SMB-Freigaben auf dem CIFS-Server enthalten sind.
- Sie können eine Konfiguration für BranchCache pro Freigabe erstellen, wenn Sie Caching-Services für Inhalte anbieten möchten, die in ausgewählten SMB-Freigaben auf dem CIFS-Server enthalten sind.

Beim Konfigurieren von BranchCache müssen Sie die folgenden Parameter angeben:

Erforderliche Parameter	Beschreibung
<i>SVM Name</i>	BranchCache wird auf SVM-Basis konfiguriert. Sie müssen angeben, auf welcher SVM mit CIFS-Aktivierung der BranchCache-Service konfiguriert werden soll.

Erforderliche Parameter	Beschreibung
<i>Pfad zu Hash-Speicher</i>	<p>BranchCache-Hashes werden in normalen Dateien auf dem SVM Volume gespeichert. Sie müssen den Pfad zu einem vorhandenen Verzeichnis angeben, in dem ONTAP die Hash-Daten speichern soll. Der BranchCache-Hash-Pfad muss schreibgeschützt sein. Schreibgeschützte Pfade, wie beispielsweise Snapshot Verzeichnisse, sind nicht zulässig. Sie können Hash-Daten in einem Volume speichern, das andere Daten enthält, oder Sie können ein separates Volume zum Speichern von Hash-Daten erstellen.</p> <p>Wenn die SVM eine SVM Disaster-Recovery-Quelle ist, kann sich der Hash-Pfad nicht auf dem Root-Volume befinden. Das liegt daran, dass das Root-Volume nicht zum Disaster-Recovery-Ziel repliziert wird.</p> <p>Der Hash-Pfad kann Leerzeichen und gültige Dateinamenzeichen enthalten.</p>

Sie können optional die folgenden Parameter angeben:

Optionale Parameter	Beschreibung
<i>Unterstützte Versionen</i>	<p>ONTAP unterstützt BranchCache 1 und 2. Sie können Version 1, Version 2 oder beide Versionen aktivieren. Standardmäßig werden beide Versionen aktiviert.</p>
<i>Maximale Größe des Hash-Speichers</i>	<p>Sie können die Größe angeben, die für den Hash-Datenspeicher verwendet werden soll. Wenn die Hash-Daten diesen Wert überschreiten, löscht ONTAP ältere Hashes, um Platz für neuere Hash-Werte zu schaffen. Die Standardgröße für den Hash-Speicher beträgt 1 GB. BranchCache arbeitet effizienter, wenn Hashes nicht übermäßig aggressiv verworfen werden. Wenn Sie feststellen, dass Hashes häufig verworfen werden, weil der Hash-Speicher voll ist, können Sie die Hash-Speichergröße erhöhen, indem Sie die BranchCache-Konfiguration ändern.</p>

Optionale Parameter	Beschreibung
<i>Serverschlüssel</i>	<p>Sie können einen Serverschlüssel angeben, den der BranchCache-Dienst verwendet, um zu verhindern, dass Clients den BranchCache-Server imitieren. Wenn Sie keinen Serverschlüssel angeben, wird der nach dem Zufallsprinzip generiert, wenn Sie die BranchCache-Konfiguration erstellen. Sie können den Server-Schlüssel auf einen bestimmten Wert legen, sodass Clients Hash-Funktionen von jedem Server verwenden können, wenn mehrere Server BranchCache-Daten für die gleichen Dateien bereitstellen. Wenn der Serverschlüssel Leerzeichen enthält, müssen Sie den Serverschlüssel in Anführungszeichen einschließen.</p>
<i>Betriebsmodus</i>	<p>Standardmäßig wird BranchCache auf Share-Basis aktiviert.</p> <ul style="list-style-type: none"> • Um eine BranchCache-Konfiguration zu erstellen, bei der Sie BranchCache auf Freigabebasis aktivieren, können Sie diesen optionalen Parameter entweder nicht angeben oder angeben <code>per-share</code>. • Damit BranchCache automatisch auf allen Freigaben aktiviert werden kann, müssen Sie den Betriebsmodus auf einstellen <code>all-shares</code>.

Schritte

1. SMB 2.1 und 3.0 nach Bedarf aktivieren:

- a. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
- b. Überprüfen Sie die konfigurierten SVM-SMB-Einstellungen, um zu ermitteln, ob alle erforderlichen SMB-Versionen aktiviert sind: `vserver cifs options show -vserver vserver_name`
- c. Gegebenenfalls SMB 2.1 aktivieren: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

Mit dem Befehl werden sowohl SMB 2.0 als auch SMB 2.1 aktiviert.

- d. Gegebenenfalls SMB 3.0 aktivieren: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
- e. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

2. BranchCache konfigurieren: `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all}] [-server-key text] -operating-mode {per-share|all-shares}`

Der angegebene Hash-Storage-Pfad muss vorhanden sein und sich auf einem Volume befinden, das von der SVM verwaltet wird. Der Pfad muss sich auch auf einem schreibbaren Volume befinden. Der Befehl schlägt fehl, wenn der Pfad schreibgeschützt ist oder nicht vorhanden ist.

Wenn Sie denselben Serverschlüssel für zusätzliche SVM-BranchCache-Konfigurationen verwenden möchten, notieren Sie den für den Serverschlüssel eingegebenen Wert. Der Serverschlüssel wird nicht angezeigt, wenn Sie Informationen über die BranchCache-Konfiguration anzeigen.

3. Vergewissern Sie sich, dass die BranchCache-Konfiguration korrekt ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiele

Die folgenden Befehle überprüfen, ob SMB 2.1 und 3.0 aktiviert sind, und konfigurieren Sie BranchCache so, dass das Caching auf allen SMB-Freigaben auf SVM vs1 automatisch aktiviert wird:

```
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 show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true          true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
                                CIFS BranchCache Operating Modes: all_shares
```

Mit den folgenden Befehlen wird sichergestellt, dass sowohl SMB 2.1 als auch 3.0 aktiviert sind; BranchCache konfigurieren, um die Cache-Speicherung auf Basis der SVM vs1 zu ermöglichen. Außerdem wird die Konfiguration mit BranchCache geprüft:

```

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 show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share

```

Verwandte Informationen

[Anforderungen und Richtlinien: Unterstützung der BranchCache-Version](#)

[Wo Informationen zur Konfiguration von BranchCache an der Remote-Zweigstelle zu finden sind](#)

[Erstellen einer SMB-Freigabe mit BranchCache-Aktivierung](#)

[Aktivieren Sie BranchCache auf einer vorhandenen SMB-Freigabe](#)

[Ändern der BranchCache-Konfiguration](#)

[Übersicht: BranchCache auf SMB-Freigaben deaktivieren](#)

[Löschen Sie die BranchCache-Konfiguration auf SVMs](#)

Wo Informationen zur Konfiguration von BranchCache an der Remote-Zweigstelle zu finden sind

Nach der Konfiguration von BranchCache auf dem SMB-Server müssen Sie BranchCache auf Client-Computern und optional auf den Caching-Servern an Ihrem Remote-Standort installieren und konfigurieren. Microsoft bietet Anweisungen zur Konfiguration von BranchCache an Remote-Standorten.

Anweisungen zur Konfiguration der Clients in Remote-Standorten und, optional, zur Cache-Speicherung von Servern zur Verwendung von BranchCache befinden sich auf der Microsoft BranchCache Website.

["Microsoft BranchCache Docs: Was ist neu"](#)

Konfigurieren Sie SMB-Freigaben mit BranchCache-Aktivierung

Übersicht über BranchCache-fähige SMB-Freigaben konfigurieren

Nachdem Sie BranchCache auf dem SMB-Server und in der Zweigstelle konfiguriert haben, können Sie BranchCache auf SMB-Freigaben aktivieren, die Inhalte enthalten, die Clients an Zweigstellen den Cache erlauben möchten.

BranchCache Caching kann auf allen SMB-Freigaben auf dem SMB-Server oder auf Share-by-Share-Basis aktiviert werden.

- Wenn Sie BranchCache auf Share-by-Share-Basis aktivieren, können Sie BranchCache bei der Erstellung der Freigabe oder durch Ändern vorhandener Freigaben aktivieren.

Wenn Sie das Caching für eine bestehende SMB-Freigabe aktivieren, beginnt ONTAP mit der Verarbeitung von Hash-Funktionen und dem Versand von Metadaten an Clients, die Inhalte anfordern, sobald Sie BranchCache auf dieser Freigabe aktivieren.

- Alle Clients, auf denen eine SMB-Verbindung zu einer Freigabe besteht, erhalten keine BranchCache-Unterstützung, wenn BranchCache anschließend für diese Freigabe aktiviert wird.

ONTAP wirbt mit BranchCache-Unterstützung für eine Freigabe zum Zeitpunkt der Einrichtung der SMB-Sitzung. Clients, auf denen bereits Sitzungen eingerichtet wurden, wenn BranchCache aktiviert ist, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.



Wenn BranchCache auf einer SMB-Freigabe anschließend deaktiviert wird, stoppt ONTAP das Senden von Metadaten an den Client, der die Anfrage anfordert. Ein Client, der Daten benötigt, ruft diese direkt vom Content Server ab (SMB Server).

Erstellen einer SMB-Freigabe mit BranchCache-Aktivierung

Sie können BranchCache auf einer SMB-Freigabe aktivieren, wenn Sie die Freigabe erstellen, indem Sie die festlegen `branchcache` Eigenschaft freigeben.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Konfiguration der Offline-Dateien auf manuelle Cache-Speicherung festgelegt sein.

Dies ist die Standardeinstellung, wenn Sie eine Freigabe erstellen.

- Sie können auch zusätzliche optionale Freigabeparameter festlegen, wenn Sie die BranchCache-fähige Freigabe erstellen.
- Sie können die einstellen `branchcache` Eigenschaft auf einer Freigabe, auch wenn BranchCache nicht konfiguriert und auf der Storage Virtual Machine (SVM) aktiviert ist.

Um jedoch gecachte Inhalte bereitstellen zu können, müssen BranchCache auf der SVM konfiguriert und

aktiviert werden.

- Da bei Verwendung des keine Standardeigenschaften für die Freigabe vorhanden sind `-share -properties` Parameter: Sie müssen alle anderen Freigabeeigenschaften angeben, die zusätzlich zum auf die Freigabe angewendet werden sollen `branchcache` Teilen Sie die Eigenschaft mithilfe einer durch Komma getrennten Liste.
- Weitere Informationen finden Sie auf der man-Page für das `vserver cifs share create` Befehl.

Schritt

1. BranchCache-fähige SMB-Freigabe erstellen:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,...]
```

2. Überprüfen Sie, ob die Eigenschaft BranchCache-Freigabe auf der SMB-Freigabe mithilfe des festgelegt ist `vserver cifs share show` Befehl.

Beispiel

Mit dem folgenden Befehl wird eine SMB-Freigabe mit BranchCache-Aktivierung mit dem Namen „data“ mit dem Pfad von erstellt `/data` Auf SVM vs1. Standardmäßig ist die Einstellung Offline-Dateien auf festgelegt `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path /data -share-properties branchcache,oplocks,browsable,notify
cluster1::> vserver cifs share show -vserver vs1 -share-name data
      Vserver: vs1
      Share: data
CIFS Server NetBIOS Name: VS1
      Path: /data
      Share Properties: branchcache
                       oplocks
                       browsable
                       notify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: data
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

Verwandte Informationen

[Deaktivieren von BranchCache auf einer einzelnen SMB-Freigabe](#)

Aktivieren Sie BranchCache auf einer vorhandenen SMB-Freigabe

Sie können BranchCache auf einer vorhandenen SMB-Freigabe aktivieren, indem Sie die hinzufügen `branchcache` Eigenschaft für die vorhandene Liste der Freigabegenschaften freigeben.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Konfiguration der Offline-Dateien auf manuelle Cache-Speicherung festgelegt sein.

Wenn die Einstellung der Offline-Dateien der vorhandenen Freigabe nicht auf manuelles Caching eingestellt ist, müssen Sie sie durch Ändern der Freigabe konfigurieren.

- Sie können die einstellen `branchcache` Eigenschaft auf einer Freigabe, auch wenn BranchCache nicht konfiguriert und auf der Storage Virtual Machine (SVM) aktiviert ist.

Um jedoch gecachte Inhalte bereitstellen zu können, müssen BranchCache auf der SVM konfiguriert und aktiviert werden.

- Wenn Sie die hinzufügen `branchcache` Freigabegenschaft für die Freigabe, bestehende Freigabeneinstellungen und Freigabegenschaften bleiben erhalten.

Die Eigenschaft BranchCache-Freigabe wird zur bestehenden Liste der Freigabeneigenschaften hinzugefügt. Weitere Informationen zur Verwendung des `vserver cifs share properties add` Befehl, siehe die man-Pages.

Schritte

1. Konfigurieren Sie bei Bedarf die Einstellung Offline-Dateifreigabe für manuelles Caching:
 - a. Legen Sie fest, welche Einstellungen für die Offline-Dateifreigabe verwendet werden `vserver cifs share show` Befehl.
 - b. Wenn die Einstellung Offline-Dateifreigabe nicht auf manuell eingestellt ist, ändern Sie sie in den gewünschten Wert: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. BranchCache auf einer vorhandenen SMB-Freigabe aktivieren: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Vergewissern Sie sich, dass die Eigenschaft BranchCache-Freigabe auf der SMB-Freigabe festgelegt ist: `vserver cifs share show -vserver vserver_name -share-name share_name`

Beispiel

Mit dem folgenden Befehl wird BranchCache auf einer vorhandenen SMB-Freigabe mit dem Namen „data2“ mit dem Pfad von aktiviert `/data2` Auf SVM vs1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
    Share Properties: oplocks
                    browsable
                    changenotify
                    showsnapshot
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
    Share Properties: oplocks
                    browsable
                    showsnapshot
                    changenotify
                    branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard
```

Verwandte Informationen

Management und Monitoring der BranchCache Konfiguration

Ändern Sie BranchCache-Konfigurationen

Sie können die Konfiguration des BranchCache-Service auf SVMs ändern, einschließlich des Hash-Speicherverzeichnispfads, der maximalen Verzeichnisgröße des Hash-Speichers, des Betriebsmodus und der unterstützten BranchCache-Versionen. Sie können auch die Größe des Volumens erhöhen, das den Hash-Speicher enthält.

Schritte

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Geben Sie Folgendes ein...
Ändern Sie die Verzeichnisgröße des Hash-Speichers	<code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB</code>
MB	GB
TB	PB]}`
Erhöhen Sie die Größe des Volumens, das den Hash-Speicher enthält	<code>`volume size -vserver vserver_name -volume volume_name -new-size new_size[k</code>
m	g
t]` Wenn sich das Volume mit dem Hash-Speicher füllt, können Sie die Volume-Größe möglicherweise erhöhen. Sie können die neue Volume-Größe als Zahl festlegen, gefolgt von einer Einheitenbezeichnung.	Ändern Sie den Verzeichnispfad für den Hash-Speicher
Weitere Informationen zu " Verwalten von FlexVol Volumes "	

Ihr Ziel ist	Geben Sie Folgendes ein...
<pre>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</pre>	<p>false}` Wenn die SVM eine SVM Disaster-Recovery-Quelle ist, kann sich der Hash-Pfad nicht auf dem Root-Volume befinden. Das liegt daran, dass das Root-Volume nicht zum Disaster-Recovery-Ziel repliziert wird.</p> <p>Der Hash-Pfad für BranchCache kann Leerzeichen und gültige Dateinamenzeichen enthalten.</p> <p>Wenn Sie den Hash-Pfad ändern, <code>-flush-hashes</code> ist ein erforderlicher Parameter, der angibt, ob ONTAP die Hash-Werte vom ursprünglichen Hash-Speicherort spülen soll. Sie können die folgenden Werte für das festlegen <code>-flush-hashes</code> Parameter:</p> <p>Wenn Sie angeben <code>true</code>, ONTAP löscht die Hash-Werte am ursprünglichen Standort und erstellt neue Hash-Werte am neuen Standort, sobald neue Anfragen von den branchCache-fähigen Clients gestellt werden. Wenn Sie angeben <code>false</code>, Die Hashes werden nicht gespült. + In diesem Fall können Sie die bestehenden Hashes später wieder verwenden, indem Sie den Hash-Speicherpfad zurück zur ursprünglichen Position ändern.</p>
Den Betriebsmodus ändern	<pre>`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share</pre>
all-shares	<pre>disable}`</pre> <p>Beim Ändern des Betriebsmodus sollten Sie Folgendes beachten:</p> <p>ONTAP wirbt mit BranchCache-Unterstützung für eine Freigabe, wenn die SMB-Sitzung eingerichtet ist. Clients, auf denen bereits Sitzungen eingerichtet wurden, wenn BranchCache aktiviert ist, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.</p>
Ändern Sie die Unterstützung der BranchCache-Version	<pre>`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable</pre>
v2-enable	<pre>enable-all}`</pre>

2. Überprüfen Sie die Konfigurationsänderungen mit der `vserver cifs branchcache show` Befehl.

Zeigt Informationen zu BranchCache-Konfigurationen an

Sie können Informationen zu BranchCache-Konfigurationen auf Storage Virtual Machines (SVMs) anzeigen. Diese Informationen lassen sich zur Überprüfung der Konfiguration oder zum Bestimmen aktueller Einstellungen vor dem Ändern der Konfiguration verwenden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Sie möchten Folgendes anzeigen:	Diesen Befehl eingeben...
Zusammenfassende Informationen zu BranchCache-Konfigurationen auf allen SVMs	<code>vserver cifs branchcache show</code>
Detaillierte Informationen zur Konfiguration auf einer bestimmten SVM	<code>vserver cifs branchcache show -vserver <i>vserver_name</i></code>

Beispiel

Im folgenden Beispiel werden Informationen zur BranchCache-Konfiguration auf der SVM vs1 angezeigt:

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

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

Ändern des BranchCache-Serverschlüssels

Sie können den BranchCache-Serverschlüssel ändern, indem Sie die BranchCache-Konfiguration auf der Storage Virtual Machine (SVM) ändern und einen anderen Serverschlüssel angeben.

Über diese Aufgabe

Sie können den Server-Schlüssel auf einen bestimmten Wert legen, sodass Clients Hash-Funktionen von jedem Server verwenden können, wenn mehrere Server BranchCache-Daten für die gleichen Dateien bereitstellen.

Wenn Sie den Serverschlüssel ändern, müssen Sie auch den Hash-Cache leeren. Nach der Hash-Funktion erstellt ONTAP neue Hash-Funktionen, wenn neue Anforderungen von Clients mit BranchCache-Aktivierung gestellt werden.

Schritte

1. Ändern Sie den Serverschlüssel mit dem folgenden Befehl: `vserver cifs branchcache modify`

```
-vserver vserver_name -server-key text -flush-hashes true
```

Beim Konfigurieren eines neuen Serverschlüssels müssen Sie ebenfalls angeben `-flush-hashes` Und setzen Sie den Wert auf `true`.

2. Überprüfen Sie mithilfe des, ob die BranchCache-Konfiguration korrekt ist `vserver cifs branchcache show` Befehl.

Beispiel

Im folgenden Beispiel wird ein neuer Serverschlüssel festgelegt, der Leerzeichen enthält und den Hash-Cache auf SVM vs1 schreibt:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

Verwandte Informationen

[Gründe, warum ONTAP BranchCache Hash-Werte für ungültig erklärt](#)

BranchCache wird vor der Berechnung auf festgelegten Pfaden hashes ausgeführt

Sie können den BranchCache-Service so konfigurieren, dass Hashes für eine einzelne Datei, für ein Verzeichnis oder für alle Dateien in einer Verzeichnisstruktur vorab berechnet werden. Dies ist unter Umständen hilfreich, wenn Hash-Daten in einer mit BranchCache kompatiblen Freigabe während Off-Zeiten ohne Spitzenauslastung berechnet werden.

Über diese Aufgabe

Wenn Sie eine Datenprobe erfassen möchten, bevor Sie Hash-Statistiken anzeigen, müssen Sie den verwenden `statistics start` Und optional `statistics stop` Befehle.

- Sie müssen Storage Virtual Machine (SVM) und Pfad angeben, auf dem Sie Hash-Werte vorab berechnen möchten.
- Sie müssen auch angeben, ob Hashes rekursiv berechnet werden sollen.
- Wenn Hashes rekursiv berechnet werden sollen, durchquert der BranchCache-Dienst die gesamte Verzeichnisstruktur unter dem angegebenen Pfad und berechnet die Hash-Werte für jedes berechnete Objekt.

Schritte

1. Hashes nach Wunsch vorberechnen:

Wenn Sie Hashes vorberechnen wollen...	Geben Sie den Befehl ein...
Einer einzelnen Datei oder einem Verzeichnis	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</pre>
Rekursiv auf allen Dateien in einer Verzeichnisstruktur	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true</pre>

2. Stellen Sie sicher, dass Hashes mit dem berechneten `statistics` Befehl:

- a. Zeigen Sie Statistiken für das `hashd` Objekt auf der gewünschten SVM-Instanz:

```
statistics show -object hashd -instance vserver_name
```
- b. Überprüfen Sie, ob die Anzahl der erstellten Hash-Werte durch Wiederholung des Befehls erhöht wird.

Beispiele

Das folgende Beispiel erzeugt Hashes auf dem Pfad `/data` und unter allen enthaltenen Dateien und Unterverzeichnissen in SVM `vs1`:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

```
Object: hashd
```

```
Instance: vs1
```

```
Start-time: 9/6/2012 19:09:54
```

```
End-time: 9/6/2012 19:11:15
```

```
Cluster: cluster1
```

Counter	Value
-----	-----
branchcache_hash_created	85
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

```
cluster1::> statistics show -object hashd -instance vs1
```

```
Object: hashd
```

```
Instance: vs1
```

```
Start-time: 9/6/2012 19:09:54
```

```
End-time: 9/6/2012 19:11:15
```

```
Cluster: cluster1
```

Counter	Value
-----	-----
branchcache_hash_created	92
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

Verwandte Informationen

["Einrichtung der Performance-Überwachung"](#)

Hash-Speicher von SVM-BranchCache

Sie können alle Hash-Speicher des BranchCache auf der Storage Virtual Machine (SVM) spülen, die im Cache gespeichert sind. Dies kann nützlich sein, wenn Sie die Konfiguration von BranchCache in der Zweigstelle geändert haben. Wenn Sie beispielsweise den Caching-Modus vor kurzem vom verteilten Caching- zum gehosteten Caching-Modus neu konfigurieren, sollten Sie den Hash-Speicher spülen.

Über diese Aufgabe

Nach der Hash-Funktion erstellt ONTAP neue Hash-Funktionen, wenn neue Anforderungen von Clients mit BranchCache-Aktivierung gestellt werden.

Schritt

1. Spülen Sie die Hash-Werte aus dem BranchCache-Hash-Speicher: `vserver cifs branchcache hash-flush -vserver vserver_name`

`vserver cifs branchcache hash-flush -vserver vs1`

Zeigt BranchCache-Statistiken an

Sie können BranchCache-Statistiken anzeigen, um unter anderem die optimale Cache-Speicherung zu ermitteln, ob Ihre Konfiguration den Clients zwischengespeicherte Inhalte bereitstellt, und bestimmen, ob Hash-Dateien gelöscht wurden, um Platz für aktuellere Hash-Daten zu schaffen.

Über diese Aufgabe

Der `hashd` Statistikobjekt enthält Zähler, die statistische Informationen über BranchCache-Hash-Werte liefern. Der `cifs` Das Statistikobjekt enthält Zähler, die statistische Informationen über branchCache-bezogene Aktivitäten liefern. Sie können auf der erweiterten Berechtigungsebene Informationen über diese Objekte erfassen und anzeigen.

Schritte

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

```
cluster1::> set -privilege advanced
```

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

2. Zeigen Sie die mit BranchCache verbundenen Zähler mithilfe des `an statistics catalog counter show` Befehl.

Weitere Informationen zu Statistikzählern finden Sie auf der man-Page für diesen Befehl.

```
cluster1::*> statistics catalog counter show -object hashd
```

Object: hashd

Counter	Description
branchcache_hash_created	Number of times a request to generate BranchCache hash for a file succeeded.
branchcache_hash_files_replaced	Number of times a BranchCache hash file was deleted to make room for more recent hash data. This happens if the hash store size is exceeded.
branchcache_hash_rejected	Number of times a request to generate BranchCache hash data failed.
branchcache_hash_store_bytes	Total number of bytes used to store hash data.
branchcache_hash_store_size	Total space used to store BranchCache hash data for the Vserver.
instance_name	Instance Name
instance_uuid	Instance UUID
node_name	System node name
node_uuid	System node id

9 entries were displayed.

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

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
avg_junction_depth	Average number of junctions crossed by SMB and SMB2 path-based commands
branchcache_hash_fetch_fail	Total number of times a request to fetch hash

```

It
data
branchcache_hash_fetch_ok
hash
branchcache_hash_sent_bytes
branchcache_missing_hash_bytes
to be
that
....Output truncated....
data failed. These are failures when
attempting to read existing hash data.
does not include attempts to fetch hash
that has not yet been generated.
Total number of times a request to fetch
data succeeded.
Total number of bytes sent to clients
requesting hashes.
Total number of bytes of data that had
read by the client because the hash for
content was not available on the server.

```

3. Sammeln Sie Statistiken zu BranchCache, indem Sie die verwenden `statistics start` Und `statistics stop` Befehle.

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. Zeigen Sie die gesammelten BranchCache-Statistiken mithilfe der `an statistics show` Befehl.

```
cluster1::*> statistics show -object cifs -counter  
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0

```
cluster1::*> statistics show -object cifs -counter  
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0

5. Zurück zur Administratorberechtigungsebene: set -privilege admin

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

Verwandte Informationen

[Anzeigen von Statistiken](#)

["Einrichtung der Performance-Überwachung"](#)

Unterstützung für Richtlinienobjekte der BranchCache-Gruppe

ONTAP BranchCache unterstützt Gruppenrichtlinienobjekte (GPOs) von BranchCache,

die ein zentralisiertes Management bestimmter Konfigurationsparameter von BranchCache erlauben. Es gibt zwei Gruppenrichtlinienobjekte für BranchCache, die Hash Publication for BranchCache GPO und das Gruppenrichtlinienobjekt Hash-Version-Unterstützung für BranchCache.

- **Hash-Publikation für BranchCache GPO**

Die Hash Publication for BranchCache GPO entspricht dem `-operating-mode` Parameter. Bei Gruppenupdates wird dieser Wert auf SVM-Objekte (Storage Virtual Machine) angewendet, die sich in der Organisationseinheit (OU) befinden, auf die die Gruppenrichtlinie gilt.

- **Hash-Version Unterstützung für BranchCache GPO**

Das Gruppenrichtlinienobjekt Hash Version Support für BranchCache entspricht dem `-versions` Parameter. Wenn GPO-Aktualisierungen erfolgen, wird dieser Wert auf SVM-Objekte angewendet, die sich in der Organisationseinheit befinden, auf die die Gruppenrichtlinie gilt.

Verwandte Informationen

[Werden Gruppenrichtlinienobjekte auf CIFS-Server angewendet](#)

Informationen zu den Gruppenrichtlinienobjekten von BranchCache anzeigen

Sie können Informationen zur Konfiguration des Gruppenrichtlinienobjekts (Group Policy Object, GPO) des CIFS-Servers anzeigen, um zu bestimmen, ob BranchCache-GPOs für die Domäne definiert sind, zu der der CIFS-Server gehört, und falls ja, welche Einstellungen zulässig sind. Sie bestimmen auch, ob BranchCache GPO-Einstellungen auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Obwohl in der Domäne, zu der der CIFS-Server gehört, eine GPO-Einstellung definiert ist, wird sie nicht unbedingt auf die Organisationseinheit (OU) angewendet, die die CIFS-fähige Storage Virtual Machine (SVM) enthält. Bei der angewendeten Gruppenrichtlinieneinstellung handelt es sich um eine Untergruppe aller definierten Gruppenrichtlinienobjekte, die auf die CIFS-fähige SVM angewendet werden. Über die Gruppenrichtlinienobjekte angewandte BranchCache-Einstellungen überschreiben die über die CLI angewendeten Einstellungen.

Schritte

1. Zeigen Sie die definierte GPO-Einstellung für BranchCache für die Active Directory-Domäne an, indem Sie die verwenden `vserver cifs group-policy show-defined` Befehl.



In diesem Beispiel werden nicht alle verfügbaren Ausgabefelder für den Befehl angezeigt. Ausgabe wird abgeschnitten.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
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: version1  
[...]  
  
    GPO Name: Resultant Set of Policy  
    Status: enabled  
Advanced Audit Settings:  
    Object Access:  
        Central Access Policy Staging: failure  
Registry Settings:  
    Refresh Time Interval: 22  
    Refresh Random Offset: 8  
    Hash Publication for Mode BranchCache: per-share  
    Hash Version Support for BranchCache: version1  
[...]
```

2. Zeigen Sie die auf den CIFS-Server angewendete GPO-Einstellung für BranchCache mit dem an `vserver cifs group-policy show-applied` Befehl. ``



In diesem Beispiel werden nicht alle verfügbaren Ausgabefelder für den Befehl angezeigt. Ausgabe wird abgeschnitten.


```

cluster1::> vserver cifs group-policy show-applied -vserver vs1

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: version1
[...]

    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: version1
[...]

```

Verwandte Informationen

[Aktivieren oder Deaktivieren der GPO-Unterstützung auf einem CIFS-Server](#)

Deaktivieren Sie BranchCache auf SMB-Freigaben

Übersicht: BranchCache auf SMB-Freigaben deaktivieren

Wenn Sie BranchCache Caching-Services nicht für bestimmte SMB-Freigaben bereitstellen möchten, aber später auch für diese Freigaben Caching-Services bereitstellen möchten, lässt sich BranchCache auf Share-Basis deaktivieren. Wenn BranchCache für alle Freigaben konfiguriert ist, jedoch alle Caching-Services vorübergehend deaktivieren möchten, können Sie die Konfiguration von BranchCache ändern, um die automatische Cache-Speicherung auf allen Freigaben zu stoppen.

Wenn BranchCache auf einer SMB-Freigabe nach der ersten Aktivierung nachträglich deaktiviert wird, stoppt ONTAP das Senden von Metadaten an den Client, der die Anfrage stellt. Clients, die Daten benötigen, rufen

sie direkt vom Content Server ab (CIFS-Server auf der Storage Virtual Machine (SVM)).

Verwandte Informationen

[Konfigurieren von BranchCache-fähigen SMB-Freigaben](#)

Deaktivieren Sie BranchCache auf einer einzelnen SMB-Freigabe

Wenn Sie keine Caching-Services für bestimmte Freigaben anbieten möchten, für die zuvor zwischengespeicherte Inhalte angeboten wurden, können Sie BranchCache auf einer vorhandenen SMB-Freigabe deaktivieren.

Schritt

1. Geben Sie den folgenden Befehl ein: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

Die Eigenschaft BranchCache-Freigabe wird entfernt. Andere Eigenschaften der angewendeten Aktie bleiben wirksam.

Beispiel

Mit dem folgenden Befehl wird BranchCache auf einer vorhandenen SMB-Freigabe mit dem Namen „data2“ deaktiviert:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                    browsable
                    changenotify
                    attributecache
                    branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                    browsable
                    changenotify
                    attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

Stoppen Sie das automatische Caching für alle SMB-Freigaben

Wenn Ihre Konfiguration mit BranchCache automatisch das Caching auf allen SMB-Freigaben auf jeder Storage Virtual Machine (SVM) ermöglicht, können Sie die BranchCache-Konfiguration ändern, um Inhalte für alle SMB-Freigaben automatisch zu speichern.

Über diese Aufgabe

Um die automatische Cache-Speicherung auf allen SMB-Freigaben zu stoppen, wird der Betriebsmodus BranchCache auf Cache-Speicherung pro Freigabe geändert.

Schritte

1. Konfigurieren Sie BranchCache so, dass die automatische Cache-Speicherung auf allen SMB-Freigaben unterbrochen wird: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Vergewissern Sie sich, dass die BranchCache-Konfiguration korrekt ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiel

Mit dem folgenden Befehl wird die BranchCache-Konfiguration auf der Storage Virtual Machine (SVM, ehemals Vserver) vs1 geändert, um das automatische Caching auf allen SMB-Freigaben zu beenden:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

Deaktivieren oder aktivieren Sie BranchCache auf der SVM

Was passiert, wenn Sie BranchCache auf dem CIFS-Server deaktivieren bzw. erneut aktivieren

Wenn Sie zuvor BranchCache konfiguriert haben, die Filialclients aber nicht möchten, dass sie zwischengespeicherte Inhalte verwenden, können Sie das Caching auf dem CIFS-Server deaktivieren. Wenn Sie BranchCache deaktivieren, müssen Sie sich bewusst sein, was passiert.

Wenn Sie BranchCache deaktivieren, berechnet ONTAP nicht mehr die Hash-Werte und sendet die Metadaten nicht mehr an den Client, den die Anforderung stellt. Der Dateizugriff wird jedoch nicht unterbrochen. Wenn Clients mit BranchCache-Unterstützung anschließend Metadateninformationen für Inhalte anfordern, auf die sie zugreifen möchten, antwortet ONTAP mit einem Microsoft-definierten Fehler. Dies führt dazu, dass der Client eine zweite Anforderung sendet und den tatsächlichen Inhalt anfordert. Als Antwort auf die

Inhaltsanfrage sendet der CIFS-Server den tatsächlichen Content, der auf der Storage Virtual Machine (SVM) gespeichert ist.

Nachdem BranchCache auf dem CIFS-Server deaktiviert wurde, werben SMB-Freigaben nicht für BranchCache-Funktionen. Um auf Daten über neue SMB-Verbindungen zuzugreifen, führen Clients normale SMB-Leseanforderungen durch.

Sie können BranchCache jederzeit auf dem CIFS-Server reaktivieren.

- Da der Hash-Speicher beim Deaktivieren von BranchCache nicht gelöscht wird, kann ONTAP nach der erneuten Aktivierung von BranchCache die gespeicherten Hash-Werte verwenden, vorausgesetzt, der angeforderte Hash ist weiterhin gültig.
- Alle Clients, die während der Deaktivierung von BranchCache SMB-Verbindungen zu BranchCache-fähigen Freigaben hergestellt haben, erhalten keine Unterstützung für BranchCache, wenn BranchCache anschließend wieder aktiviert wird.

Der Grund dafür ist, dass ONTAP zum Zeitpunkt der Einrichtung der SMB-Session Support für BranchCache für eine Freigabe wirbt. Clients, die Sitzungen zu mit BranchCache-fähigen Freigaben erstellt haben, während BranchCache deaktiviert wurde, müssen die Verbindung trennen und eine erneute Verbindung herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.



Wenn Sie den Hash-Speicher nicht speichern möchten, nachdem Sie BranchCache auf einem CIFS-Server deaktiviert haben, können Sie ihn manuell löschen. Wenn Sie BranchCache erneut aktivieren, müssen Sie sicherstellen, dass das Hash-Speicherverzeichnis vorhanden ist. Nach der reaktivierten BranchCache-Funktion werden die BranchCache-aktivierten Freigaben für BranchCache-Funktionen angekündigt. ONTAP erstellt neue Hash-Funktionen, wenn neue Anforderungen von Clients mit BranchCache-Unterstützung gestellt werden.

Deaktivieren oder aktivieren Sie BranchCache

BranchCache auf der Storage Virtual Machine (SVM) lässt sich deaktivieren, indem der Betriebsmodus von BranchCache auf geändert wird `disabled`. Es ist jederzeit möglich, BranchCache zu aktivieren, indem der Betriebsmodus geändert wird, um BranchCache-Services entweder pro Freigabe oder automatisch für alle Freigaben anzubieten.

Schritte

1. Führen Sie den entsprechenden Befehl aus:

Ihr Ziel ist	Geben Sie anschließend Folgendes ein...
Deaktivieren Sie BranchCache	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</pre>
Aktivieren Sie BranchCache pro Freigabe	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</pre>

Ihr Ziel ist	Geben Sie anschließend Folgendes ein...
Aktivieren Sie BranchCache für alle Freigaben	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares</code>

2. Vergewissern Sie sich, dass der BranchCache-Betriebsmodus mit der gewünschten Einstellung konfiguriert ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird BranchCache auf SVM vs1 deaktiviert:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: disable
```

Löschen Sie die BranchCache-Konfiguration auf SVMs

Was passiert, wenn Sie die BranchCache-Konfiguration löschen

Wenn Sie zuvor BranchCache konfiguriert haben, aber nicht möchten, dass die Storage Virtual Machine (SVM) weiterhin Inhalte im Cache bereitstellt, können Sie die BranchCache-Konfiguration auf dem CIFS-Server löschen. Sie müssen sich darüber im Klaren sein, was beim Löschen der Konfiguration geschieht.

Beim Löschen der Konfiguration ONTAP werden die Konfigurationsinformationen für diese SVM aus dem Cluster entfernt und der BranchCache Service wird angehalten. Sie können festlegen, ob ONTAP den Hash-Speicher auf der SVM löschen soll.

Durch das Löschen der BranchCache-Konfiguration wird der Zugriff von Clients, die mit BranchCache aktiviert sind, nicht unterbrochen. Wenn Clients mit BranchCache-Unterstützung anschließend für Inhalte, die bereits im Cache gespeichert sind, Metadateninformationen zu vorhandenen SMB-Verbindungen anfordern, antwortet ONTAP auf einen von Microsoft definierten Fehler. Dies führt dazu, dass der Client eine zweite Anforderung sendet und den tatsächlichen Inhalt anfordert. Als Antwort auf die Inhaltsanfrage sendet der CIFS-Server den tatsächlichen Content, der auf der SVM gespeichert ist

Nach dem Löschen der BranchCache-Konfiguration werden SMB-Freigaben nicht für BranchCache-Funktionen werben. Um auf Inhalte zuzugreifen, die zuvor mit neuen SMB-Verbindungen noch nicht im Cache gespeichert wurden, führen die Clients normale SMB-Leseanforderungen aus.

Löschen Sie die BranchCache-Konfiguration

Der Befehl, den Sie zum Löschen des BranchCache-Service auf Ihrer Storage Virtual Machine (SVM) verwenden, hängt davon ab, ob Sie bestehende Hash-Werte löschen oder beibehalten möchten.

Schritt

1. Führen Sie den entsprechenden Befehl aus:

Ihr Ziel ist	Geben Sie anschließend Folgendes ein...
Löschen Sie die BranchCache-Konfiguration, und löschen Sie vorhandene Hash-Werte	<pre>vserver cifs branchcache delete -vserver vserver_name -flush-hashes true</pre>
Löschen Sie die BranchCache-Konfiguration, behalten Sie jedoch die bestehenden Hash-Werte	<pre>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</pre>

Beispiel

Im folgenden Beispiel wird die BranchCache-Konfiguration auf der SVM vs1 gelöscht und alle vorhandenen Hash-Werte gelöscht:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes  
true
```

Was passiert mit BranchCache beim Zurücksetzen

Es ist wichtig, dass Sie die Ereignisse verstehen, die auftreten, wenn Sie ONTAP auf eine Version zurücksetzen, die BranchCache nicht unterstützt.

- Wenn Sie eine Version von ONTAP zurücksetzen, die BranchCache nicht unterstützt, werden die SMB-Freigaben BranchCache-Funktionen nicht für Clients mit BranchCache-Unterstützung werben. Die Clients werden daher keine Hash-Informationen anfordern.

Stattdessen werden die tatsächlichen Inhalte mit normalen SMB-Leseanforderungen angefordert. Als Antwort auf die Inhaltsanfrage sendet der SMB-Server die tatsächlichen Inhalte, die auf der Storage Virtual Machine (SVM) gespeichert sind.

- Wenn ein Node, der einen Hash-Speicher hostet, auf eine Version zurückgesetzt wird, die BranchCache-Konfiguration nicht unterstützt, muss der Storage-Administrator die BranchCache-Konfiguration manuell zurücksetzen. Dazu muss er einen Befehl verwenden, der während der Umrüstung ausgedruckt wird.

Mit diesem Befehl wird die BranchCache-Konfiguration gelöscht und die Hash-Funktion gelöscht.

Nach Abschluss der Zurücksetzen kann der Storage-Administrator bei Bedarf das Verzeichnis, das den Hash-Speicher enthält, manuell löschen.

Verwandte Informationen

Höhere Performance von Microsoft Remote Copy

Verbesserte Übersicht über die Performance von Microsoft Remote-Kopien

Microsoft Offloaded Data Transfer (ODX), auch bekannt als „*Copy Offload*“, ermöglicht direkte Datentransfers innerhalb und zwischen kompatiblen Storage-Geräten, ohne die Daten über den Host-Computer zu übertragen.

ONTAP unterstützt ODX sowohl für die SMB- als auch für SAN-Protokolle. Die Quelle kann entweder ein CIFS Server oder eine LUN sein, und als Ziel kann entweder ein CIFS Server oder eine LUN dienen.

Bei Dateiübertragungen ohne ODX werden die Daten von der Quelle gelesen und über das Netzwerk an den Client-Computer übertragen. Der Clientcomputer überträgt die Daten zurück über das Netzwerk an das Ziel. Zusammenfassend liest der Clientcomputer die Daten aus der Quelle und schreibt sie auf das Ziel. Bei der Übertragung von ODX-Dateien werden Daten direkt von der Quelle zum Ziel kopiert.

Da ODX Offloaded Kopien direkt zwischen Quell- und Ziel-Storage erstellt werden, ergeben sich erhebliche Performance-Vorteile. Zu den Performance-Vorteilen gehören eine schnellere Kopierzeit zwischen Quelle und Ziel, eine geringere Ressourcenauslastung (CPU, Speicher) auf dem Client und eine geringere Auslastung der Netzwerk-I/O-Bandbreite.

Bei SMB-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Storage-Server SMB 3.0 und die ODX-Funktion unterstützen. Bei SAN-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Storage-Server die ODX-Funktion unterstützen. Client-Computer, die ODX unterstützen und ODX-fähig sind, nutzen die verlagerte Dateiübertragung automatisch und transparent, wenn Dateien verschoben oder kopiert werden. ODX wird unabhängig davon verwendet, ob Sie Dateien per Drag-and-Drop über den Windows Explorer ziehen oder Befehle zum Kopieren von Dateien verwenden oder ob eine Client-Applikation Dateikopieanforderungen initiiert.

Verwandte Informationen

[Kürzere Client-Antwortzeiten durch automatische SMB-Node-Empfehlungen mit Auto Location](#)

["SMB-Konfiguration für Microsoft Hyper-V und SQL Server"](#)

Funktionsweise von ODX

Bei der ODX Copy-Offload wird ein Token-basierter Mechanismus zum Lesen und Schreiben von Daten innerhalb oder zwischen ODX-fähigen CIFS-Servern eingesetzt. Anstatt die Daten über den Host zu leiten, sendet der CIFS-Server ein kleines Token, das die Daten repräsentiert, an den Client. Der ODX-Client stellt dieses Token dem Ziel-Server bereit. Dieser kann dann die mit diesem Token vertretenen Daten von der Quelle zum Ziel übertragen.

Wenn ein ODX-Client erkennt, dass der CIFS-Server ODX-fähig ist, wird die Quelldatei geöffnet und ein Token vom CIFS-Server anfordert. Nach dem Öffnen der Zieldatei verwendet der Client das Token, um den Server anzuweisen, die Daten direkt von der Quelle auf das Ziel zu kopieren.

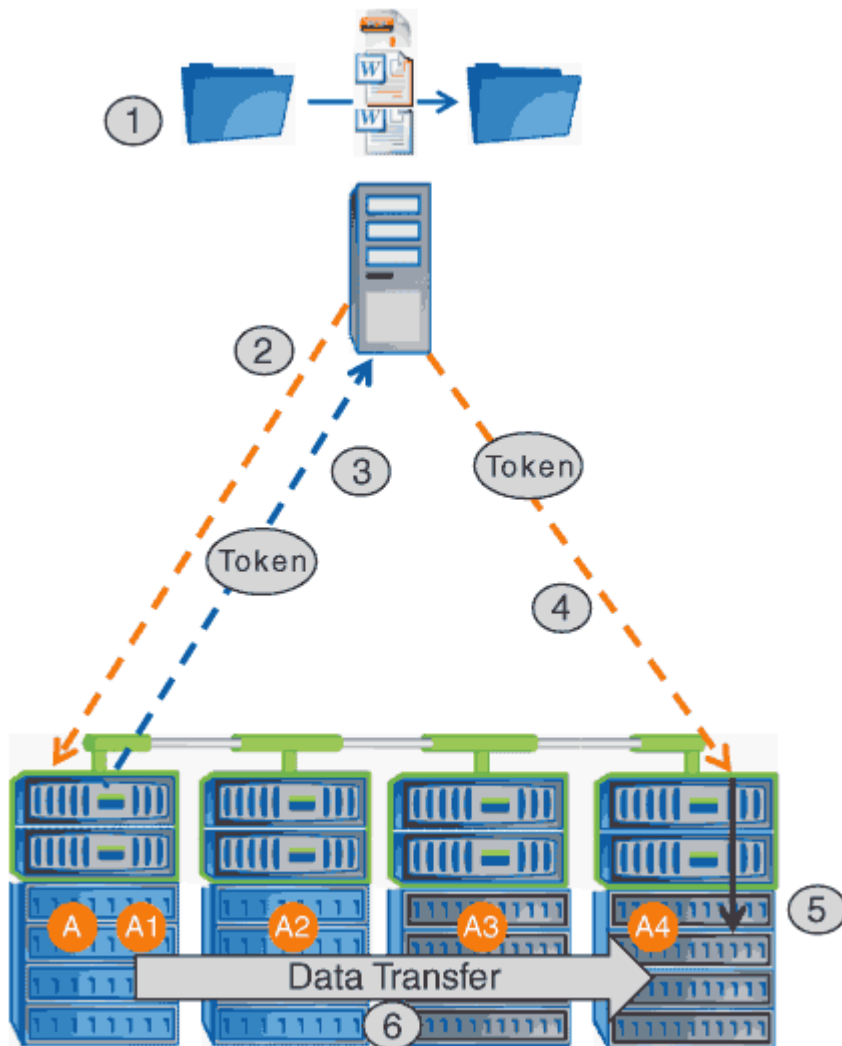


Quelle und Ziel können sich je nach Umfang des Kopiervorgangs auf derselben Storage Virtual Machine (SVM) oder auf unterschiedlichen SVMs befinden.

Das Token dient als Point-in-Time-Darstellung der Daten. Wenn Sie Daten beispielsweise zwischen den Storage-Standorten kopieren, wird ein Token, das ein Datensegment darstellt, an den anfordernden Client zurückgegeben. Der Client kopiert diesen an das Ziel. Dadurch entfällt das Kopieren der zugrunde liegenden Daten durch den Client.

ONTAP unterstützt Token mit 8 MB Daten. ODX-Kopien mit einer Größe von mehr als 8 MB werden mithilfe mehrerer Token durchgeführt. Jedes Token entspricht dabei 8 MB an Daten.

Die folgende Abbildung erläutert die Schritte, die bei einem ODX Kopiervorgang erforderlich sind:



1. Ein Benutzer kopiert oder verschiebt eine Datei mithilfe von Windows Explorer, einer Befehlszeilenoberfläche, einer Migration einer Virtual Machine oder einer Applikation Dateikopien oder -Verschiebungen.
2. Der ODX-fähige Client übersetzt diese Übertragungsanfrage automatisch in eine ODX-Anfrage.
Die an den CIFS-Server gesendete ODX-Anfrage enthält eine Token-Anfrage.
3. Wenn ODX auf dem CIFS-Server aktiviert ist und die Verbindung über SMB 3.0 erfolgt, generiert der CIFS-Server ein Token, das eine logische Darstellung der Daten auf dem Quellsystem ist.
4. Der Client erhält ein Token, das die Daten darstellt und das mit der Schreibanforderung an den CIFS-Zielserver sendet.

Dies sind die einzigen Daten, die von der Quelle an den Client und dann vom Client zum Ziel über das

Netzwerk kopiert werden.

5. Das Token wird dem Storage-Subsystem übergeben.
6. Die SVM führt den Kopiervorgang oder die Verschiebung intern durch.

Wenn die kopierte oder verschobene Datei größer als 8 MB ist, sind mehrere Token erforderlich, um die Kopie durchzuführen. Die Schritte 2 bis 6, wie zum Abschließen der Kopie ausgeführt.



Falls bei einer ODX Offloaded Copy ein Fehler auftritt, erfolgt der Kopier- und Ververschiebungsvorgang wieder auf die herkömmlichen Lese- und Schreibvorgänge, um den Kopier- oder Ververschiebungs-Vorgang durchzuführen. Gleiches gilt, wenn der CIFS-Ziel-Server ODX oder ODX nicht unterstützt, wenn der Copy- oder Move-Vorgang dann auf die herkömmlichen Lese- und Schreibvorgänge zurückgreift, wenn der Copy- oder Verschiebevorgang durchgeführt wird.

Anforderungen für die Nutzung von ODX

Bevor ODX für die Auslagerung von Kopien mit der SVM (Storage Virtual Machine) eingesetzt werden kann, müssen bestimmte Anforderungen unbedingt bekannt sein.

ONTAP-Versionsanforderungen

ONTAP Versionen unterstützen ODX bei Copy-Offloaded.

Anforderungen an die SMB-Version

- ONTAP unterstützt ODX mit SMB 3.0 und höher.
- SMB 3.0 muss auf dem CIFS Server aktiviert sein, bevor ODX aktiviert werden kann:
 - Durch die Aktivierung von ODX ist auch SMB 3.0 möglich, falls noch nicht aktiviert.
 - Wenn SMB 3.0 deaktiviert wird, wird auch ODX deaktiviert.

Windows Server- und Client-Anforderungen

Bevor Sie ODX für Copy-Offloaded verwenden können, muss der Windows-Client die Funktion unterstützen. Support für ODX beginnt mit Windows 2012 Server und Windows 8.

Die Interoperabilitäts-Matrix enthält die neuesten Informationen zu unterstützten Windows-Clients.

["NetApp Interoperabilitäts-Matrix-Tool"](#)

Volume-Anforderungen

- Die Quell-Volumes müssen mindestens 1.25 GB betragen.
- Die Deduplizierung muss für Volumes aktiviert sein, die zusammen mit dem Copy-Offload verwendet werden.
- Bei Verwendung von komprimierten Volumes muss der Komprimierungstyp anpassungsfähig sein und es muss nur die Größe der Komprimierungsgruppe 8K unterstützt werden.

Der Typ der sekundären Komprimierung wird nicht unterstützt.

Richtlinien für die Nutzung von ODX

Bevor ODX zur Copy-Offload eingesetzt werden kann, müssen Sie sich mit den Richtlinien im Klaren sein. Beispielsweise müssen Sie wissen, welche Volume-Typen Sie ODX verwenden können, und Sie sollten die Überlegungen zu ODX im Cluster und zwischen Clustern verstehen.

Volume-Richtlinien

- ODX kann bei der Copy-Offload-Funktion mit den folgenden Volume-Konfigurationen nicht genutzt werden:

- Die Größe des Quellvolumens ist kleiner als 1.25 GB

Die Volume-Größe muss 1.25 GB oder mehr betragen, um ODX zu verwenden.

- Schreibgeschützte Volumes

ODX wird nicht für Dateien und Ordner auf Load-Sharing-Spiegeln oder in SnapMirror oder SnapVault Ziel-Volumes eingesetzt.

- Wenn das Quell-Volume nicht dedupliziert wird

- ODX-Kopien werden nur für Cluster-interne Kopien unterstützt.

Mit ODX können Sie keine Dateien oder Ordner auf ein Volume in einem anderen Cluster kopieren.

Andere Richtlinien

- In SMB-Umgebungen müssen diese Dateien für den Offloaded Data Transfer mit ODX 256 kb oder mehr liegen.

Kleinere Dateien werden mittels eines herkömmlichen Kopiervorgangs übertragen.

- Bei der Offloaded Data Transfer wird die Deduplizierung als Teil des Kopierprozesses verwendet.

Wenn beim Kopieren oder Verschieben von Daten keine Deduplizierung auf SVM Volumes durchgeführt werden soll, sollte die ODX Copy-Offload für diese SVM deaktiviert werden.

- Die Applikation, die den Datentransfer durchführt, muss zur Unterstützung von ODX geschrieben werden.

Zu den Applikationsprozessen, die ODX unterstützen, gehören unter anderem:

- Management von Hyper-V, z. B. Erstellen und Konvertieren von virtuellen Festplatten (VHDs), Verwalten von Snapshot Kopien und Kopieren von Dateien zwischen Virtual Machines
- Betrieb in Windows Explorer
- Windows PowerShell Kopierbefehle
- Kopierbefehle für Windows-Befehle

Robocopy an der Windows-Eingabeaufforderung unterstützt ODX.



Die Applikationen müssen auf Windows-Servern oder Clients ausgeführt werden, die ODX unterstützen.

+ Weitere Informationen zu unterstützten ODX-Anwendungen auf Windows-Servern und -Clients finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Anwendungsfälle für ODX

Bei der Verwendung von ODX auf SVMs sollten Sie sich die Anwendungsfälle bewusst sein, damit Sie unter den Umständen, unter denen ODX Ihnen Performance-Vorteile bietet, die Ergebnisse erkennen können.

Windows-Server und -Clients, die ODX unterstützen, nutzen den Copy-Offload als Standardfunktion zum Kopieren von Daten zwischen Remote-Servern. Wenn der Windows-Server oder -Client keine ODX oder eine ODX-Copy-Offload unterstützt, können der Kopier- oder Verladevorgang wieder auf herkömmliche Lese- und Schreibvorgänge für den Kopier- oder Verschiebevorgang zurückgreift.

In den folgenden Anwendungsfällen werden ODX Kopien und Verschiebungen unterstützt:

- Intra-Volume

Die Quell- und Zieldateien oder LUNs befinden sich innerhalb desselben Volumes.

- Zwischen Volumes, demselben Node, gleiche SVM

Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen Volumes, verschiedenen Nodes, dieselbe SVM

Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen SVM, demselben Node

Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Zwischen SVMs, unterschiedliche Nodes

Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Cluster zwischen Clustern

Die Quell- und Ziel-LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Nodes über die Cluster befinden. Dies wird nur für SAN unterstützt und funktioniert nicht für CIFS.

Es gibt einige weitere spezielle Anwendungsfälle:

- Bei der ONTAP ODX Implementierung können mit ODX Dateien zwischen SMB-Freigaben und virtuellen FC- oder iSCSI-Attached-Laufwerken kopiert werden.

Mit Windows Explorer, Windows CLI, PowerShell, Hyper-V oder anderen Applikationen, die ODX

unterstützen, können Dateien durch eine nahtlose Verschiebung von ODX Kopien zwischen SMB-Freigaben und verbundenen LUNs kopiert oder verschoben werden, sofern sich SMB-Freigaben und LUNs im selben Cluster befinden.

- Hyper-V stellt weitere Anwendungsfälle für den ODX Copy-Offload zur Verfügung:
 - Mithilfe des ODX Copy-Offload-Pass-Through mit Hyper-V können Daten innerhalb oder zwischen VHD-Dateien (Virtual Hard Disk) kopiert oder Daten zwischen zugewiesenen SMB-Shares und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

Damit können Kopien von Gastbetriebssystemen an den zugrunde liegenden Storage weitergegeben werden.

- Bei der Erstellung von VHDs mit fester Größe wird ODX zur Initialisierung der Festplatte mit Nullen verwendet, wobei ein bekannter Token mit dem Namen „Zeroed“ verwendet wird.
- Wenn sich der Quell- und Ziel-Storage auf demselben Cluster befindet, wird eine ODX Copy Offload für die Storage-Migration bei Virtual Machines eingesetzt.



Um von den Anwendungsfällen für einen ODX Copy-Offload-Pass-Through mit Hyper-V zu profitieren, muss das Gastbetriebssystem ODX unterstützen. Und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die durch Storage (SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten auf dem Gastbetriebssystem unterstützen keine ODX-Pass-Through-Unterstützung.

Aktivieren oder Deaktivieren von ODX

ODX lässt sich auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Der Standard soll die Unterstützung für einen ODX Copy-Offload ermöglichen, wenn SMB 3.0 ebenfalls aktiviert ist.

Bevor Sie beginnen

SMB 3.0 muss aktiviert sein.

Über diese Aufgabe

Wenn Sie SMB 3.0 deaktivieren, deaktiviert ONTAP auch SMB ODX. Wenn Sie SMB 3.0 erneut aktivieren, müssen Sie SMB ODX manuell neu aktivieren.

Schritte

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

Falls eine ODX Copy-Offload sein soll:	Geben Sie den Befehl ein...
Aktiviert	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</code>
Deaktiviert	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</code>

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

Beispiel

Das folgende Beispiel ermöglicht den ODX Copy-Offload auf SVM vs1:

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

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

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

Verwandte Informationen

[Verfügbare SMB-Server-Optionen](#)

Verkürzen Sie die Antwortzeiten von Clients durch automatische SMB-Node-Empfehlungen mit Auto Location

Durch die Bereitstellung automatischer SMB-Node-Empfehlungen mit Auto Location-Übersicht lassen sich die Antwortzeiten von Clients verkürzen

Auto Location verwendet automatische SMB-Node-Empfehlungen, um die SMB-Client-Performance auf Storage Virtual Machines (SVMs) zu steigern. Automatische Node-Empfehlungen leiten den anfordernden Client automatisch zu einer logischen Schnittstelle auf der Node-SVM um, die das Volume hostet, in dem sich die Daten befinden. Dadurch werden die Client-Reaktionszeiten verbessert.

Wenn ein SMB-Client eine Verbindung zu einer auf der SVM gehosteten SMB-Freigabe herstellt, wird möglicherweise eine Verbindung über ein LIF hergestellt, das sich auf einem Node befindet, dem die angeforderten Daten nicht gehören. Der Node, mit dem der Client verbunden ist, greift über das Cluster-Netzwerk auf Daten eines anderen Node zu, die Eigentum sind. Der Client kann kürzere Reaktionszeiten erleben, wenn die SMB-Verbindung eine LIF auf dem Node verwendet, die die angeforderten Daten enthält:

- ONTAP bietet diese Funktion mithilfe von Microsoft DFS-Empfehlungen, um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein angefragter Ordner im Namespace irgendwo anders gehostet wird.

Ein Node empfiehlt, wenn er feststellt, dass eine anSVM LIF auf dem Node vorhanden ist, der die Daten enthält.

- Automatische Node-Empfehlungen werden für IPv4- und IPv6-LIF-IP-Adressen unterstützt.
- Empfehlungen werden basierend auf dem Speicherort des Stammes der Freigabe gemacht, über die der Client verbunden ist.
- Die Empfehlung erfolgt während der SMB-Verhandlung.

Die Empfehlung erfolgt, bevor die Verbindung hergestellt wird. Nachdem ONTAP den SMB-Client auf den Ziel-Node bezieht, wird die Verbindung hergestellt und der Client greift über den genannten LIF-Pfad von diesem Punkt an auf Daten zu. Dies ermöglicht einen schnelleren Zugriff auf die Daten und vermeidet eine zusätzliche Cluster-Kommunikation.



Wenn ein Share mehrere Verbindungspunkte umfasst und einige Verbindungen zu Volumes auf anderen Nodes bestehen, werden die Daten innerhalb der Freigabe über mehrere Nodes verteilt. Da ONTAP Empfehlungen bereitstellt, die lokal im Stammverzeichnis der Freigabe sind, muss ONTAP das Clusternetzwerk verwenden, um die Daten aus diesen nicht lokalen Volumes abzurufen. In dieser Art der Namespace-Architektur bieten automatische Node-Empfehlungen möglicherweise keine wesentlichen Performance-Vorteile.

Wenn der Node, der die Daten hostet, über kein verfügbares LIF verfügt, stellt ONTAP die Verbindung mithilfe der vom Client ausgewählten LIF her. Nachdem eine Datei von einem SMB-Client geöffnet wurde, wird der Zugriff auf die Datei über dieselbe empfohlene Verbindung fortgesetzt.

Wenn der CIFS-Server aus irgendeinem Grund keine Empfehlung vornehmen kann, wird der SMB-Service nicht unterbrochen. Die SMB-Verbindung wird so aufgebaut, als ob die automatischen Node-Empfehlungen nicht aktiviert wären.

Verwandte Informationen

[Verbesserung der Performance von Microsoft Remote Kopien](#)

Anforderungen und Richtlinien für die Nutzung automatischer Node-Empfehlungen

Bevor Sie die automatischen SMB-Node-Empfehlungen, auch bekannt als *autolocation*, verwenden können, müssen Sie sich mit bestimmten Anforderungen bewusst sein, einschließlich welcher Versionen von ONTAP die Funktion unterstützen. Auch über unterstützte SMB-Protokollversionen und bestimmte weitere spezielle Richtlinien sollten Sie sich informieren.

ONTAP-Version- und Lizenzanforderungen

- Auf allen Nodes im Cluster muss eine Version von ONTAP ausgeführt werden, die automatische Node-Empfehlungen unterstützt.
- Widelinks müssen auf einer SMB-Freigabe aktiviert sein, um die automatische Verlagerung zu verwenden.
- CIFS muss lizenziert sein, und auf den SVMs muss ein SMB-Server vorhanden sein.

Versionsanforderungen für SMB-Protokolle

- Für SVMs unterstützt ONTAP unter allen SMB-Versionen automatische Node-Empfehlungen.

Anforderungen von SMB-Clients

Alle von ONTAP unterstützten Microsoft Clients unterstützen automatische Node-Empfehlungen für SMB.

Die Interoperabilitäts-Matrix enthält die neuesten Informationen, die Windows Clients ONTAP unterstützen.

["NetApp Interoperabilitäts-Matrix-Tool"](#)

Anforderungen an Daten-LIF

Wenn Sie eine Daten-LIF als potenzielle Empfehlung für SMB-Clients verwenden möchten, müssen Sie Daten-LIFs erstellen, bei denen NFS und CIFS aktiviert sind.

Automatische Node-Empfehlungen können nicht funktionieren, wenn der Ziel-Node Daten-LIFs enthält, die nur für das NFS-Protokoll aktiviert oder nur für das SMB-Protokoll aktiviert sind.

Wird diese Anforderung nicht erfüllt, ist der Datenzugriff nicht beeinträchtigt. Der SMB-Client ordnet die Freigabe mithilfe des ursprünglichen LIF zu, das der Client zur Verbindung mit der SVM verwendet hat.

NTLM-Authentifizierungsanforderungen, wenn eine weiterbezeichnete SMB-Verbindung hergestellt wird

Die NTLM-Authentifizierung muss in der Domäne erlaubt sein, die den CIFS-Server enthält, und in den Domänen mit Clients, die automatische Node-Empfehlungen verwenden möchten.

Bei einer Empfehlung bezieht der SMB-Server eine IP-Adresse auf den Windows-Client. Da die NTLM-Authentifizierung beim Verbindungsaufbau mit einer IP-Adresse verwendet wird, wird die Kerberos-Authentifizierung nicht für die genannten Verbindungen durchgeführt.

Dies geschieht, weil der Windows-Client den von Kerberos verwendeten Service-Principal-Namen (der des Formulars ist) nicht erstellen kann `service/NetBIOS_name` und `service/FQDN`), was bedeutet, dass der Client kein Kerberos-Ticket für den Service anfordern kann.

Richtlinien für die Verwendung automatischer Node-Empfehlungen mit der Home Directory-Funktion

Wenn Freigaben mit der Eigenschaft Home Directory Share konfiguriert sind, kann es einen oder mehrere Suchpfade für Home Directory geben, die für eine Home Directory-Konfiguration konfiguriert sind. Die Suchpfade können auf Volumes verweisen, die auf jedem Node enthalten sind, der SVM Volumes enthält. Clients erhalten eine Empfehlung und stellen bei Verfügbarkeit einer aktiven logischen Datenschnittstelle eine Verbindung über eine empfohlene logische Schnittstelle her, die sich lokal mit dem Home-Verzeichnis des Home-Benutzers befindet.

Es gibt Richtlinien, wenn SMB 1.0-Clients mit aktivierten automatischen Node-Empfehlungen auf dynamische Home Directories zugreifen. Der Grund dafür ist, dass SMB 1.0-Clients die automatische Knotenverweisung benötigen, bevor sie authentifiziert wurden. Dies liegt vor dem Namen des SMB-Servers. Der Zugriff auf das SMB Home-Verzeichnis funktioniert jedoch für SMB 1.0-Clients ordnungsgemäß, wenn die folgenden Aussagen richtig sind:

- SMB-Home-Verzeichnisse werden für die Verwendung einfacher Namen konfiguriert, z. B. „%w“ (Windows Benutzername) oder „%u“ (zugeordneter UNIX-Benutzername) und keine Domain-Name-Stilnamen wie „`%d\%w`“ (Domain-Name\Benutzername).
- Beim Erstellen von Home-Directory-Freigaben werden die Namen von CIFS-Home-Verzeichnissen mit Variablen („%w`“ oder “%u”) konfiguriert und nicht mit statischen Namen, wie z. B. „`HOME“.

Für SMB 2.x und SMB 3.0 Clients gibt es keine besonderen Richtlinien für den Zugriff auf Home Directories unter Verwendung automatischer Node-Empfehlungen.

Richtlinien zum Deaktivieren der automatischen Node-Empfehlungen auf CIFS-Servern mit vorhandenen versprochenen Verbindungen

Wenn Sie die automatischen Knotenempfehlungen deaktivieren, nachdem die Option aktiviert wurde, behalten Clients, die derzeit mit einem genannten LIF verbunden sind, die erwähnte Verbindung. Da ONTAP DFS-

Empfehlungen als Mechanismus für automatische SMB-Knotenempfehlungen verwendet, können Clients sogar eine erneute Verbindung zu der genannten LIF herstellen, nachdem Sie die Option deaktiviert haben, bis die DFS-Empfehlung im Cache des Clients für die genannten Verbindungszeiten deaktiviert ist. Dies gilt auch bei der Wiederherstellung auf eine Version von ONTAP, die keine automatischen Node-Empfehlungen unterstützt. Clients verwenden weiterhin Empfehlungen, bis sich die DFS-Verweisungszeiten aus dem Cache des Clients ergeben.

Autoolocation verwendet automatische SMB-Node-Empfehlungen, um die SMB-Client-Performance zu steigern, indem Clients auf die LIF auf dem Node verwiesen werden, der das Daten-Volumen einer SVM besitzt. Wenn ein SMB-Client eine Verbindung zu einer auf einer SVM gehosteten SMB-Freigabe herstellt, kann er eine Verbindung über eine LIF auf einem Node herstellen, der nicht den angeforderten Daten besitzt, und über das Cluster-Interconnect-Netzwerk Daten abrufen. Der Client kann schnellere Antwortzeiten erleben, wenn die SMB-Verbindung eine LIF auf dem Node verwendet, der die angeforderten Daten enthält.

ONTAP bietet diese Funktion mithilfe von DFS-Empfehlungen (Microsoft Distributed File System), um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein angefragter Ordner im Namespace irgendwo anders gehostet wird. Ein Node empfiehlt, wenn er feststellt, dass eine LIF der SVM auf dem Node mit den Daten vorhanden ist. Empfehlungen werden basierend auf dem Speicherort des Stammes der Freigabe gemacht, über die der Client verbunden ist.

Die Empfehlung erfolgt während der SMB-Verhandlung. Die Empfehlung erfolgt, bevor die Verbindung hergestellt wird. Nachdem ONTAP den SMB-Client auf den Ziel-Node bezieht, wird die Verbindung hergestellt und der Client greift über den genannten LIF-Pfad von diesem Punkt an auf Daten zu. Dies ermöglicht einen schnelleren Zugriff auf die Daten und vermeidet eine zusätzliche Cluster-Kommunikation.

Richtlinien für die Verwendung automatischer Knotenempfehlungen mit Mac OS Clients

Mac OS X-Clients unterstützen keine automatischen SMB-Node-Empfehlungen, obwohl das Mac OS das verteilte Dateisystem (DFS) von Microsoft unterstützt. Windows-Clients stellen eine DFS-Verweisanfrage vor, bevor sie eine Verbindung zu einer SMB-Freigabe herstellen. ONTAP enthält eine Empfehlung zu einer Daten-LIF auf demselben Node, der die angeforderten Daten hostet. Dadurch werden die Client-Reaktionszeiten verkürzt. Obwohl das Mac OS DFS unterstützt, verhalten sich Mac OS Clients nicht genau wie Windows Clients in diesem Bereich.

Verwandte Informationen

[So ermöglicht ONTAP dynamische Home Directories](#)

["Netzwerkmanagement"](#)

["NetApp Interoperabilitäts-Matrix-Tool"](#)

Unterstützung für automatische SMB-Node-Empfehlungen

Bevor Sie die automatischen SMB-Node-Empfehlungen aktivieren, sollten Sie beachten, dass bestimmte ONTAP-Funktionen keine Empfehlungen unterstützen.

- Die folgenden Volume-Typen unterstützen keine automatischen SMB-Node-Empfehlungen:
 - Schreibgeschützte Mitglieder einer Load-Sharing-Spiegelung
 - Ziel-Volumen einer Datensicherungs-Spiegelung
- Node-Empfehlungen werden nicht zusammen mit einer LIF-Verschiebung verschoben.

Wenn ein Client eine verwiesene Verbindung über eine SMB 2.x- oder SMB 3.0-Verbindung verwendet und eine Daten-LIF sich unterbrechungsfrei verschiebt, verwendet der Client weiterhin dieselbe verwiesene

Verbindung, auch wenn die LIF nicht mehr lokal auf die Daten bezogen ist.

- Node-Empfehlungen werden nicht zusammen mit einer Volume-Verschiebung verschoben.

Wenn ein Client eine über eine beliebige SMB-Verbindung bezeichnete Verbindung nutzt und eine Volume-Verschiebung stattfindet, verwendet der Client weiterhin dieselbe verwiesene Verbindung, auch wenn sich das Volume nicht mehr auf demselben Node wie die Daten-LIF befindet.

Aktivieren oder Deaktivieren von SMB-Empfehlungen für automatische Nodes

Sie können automatische Node-Empfehlungen für SMB aktivieren, um die Performance für SMB-Client-Zugriffe zu steigern. Sie können automatische Node-Empfehlungen deaktivieren, wenn ONTAP keine Empfehlungen an SMB-Clients vornehmen soll.

Bevor Sie beginnen

Ein CIFS-Server muss auf der Storage Virtual Machine (SVM) konfiguriert und ausgeführt werden.

Über diese Aufgabe

Die Funktion „Automatische Node-Empfehlungen von SMB“ ist standardmäßig deaktiviert. Sie können diese Funktion bei Bedarf für jede SVM aktivieren oder deaktivieren.

Diese Option ist auf der erweiterten Berechtigungsebene verfügbar.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Aktivieren oder Deaktivieren der automatischen SMB-Node-Empfehlungen nach Bedarf:

Die automatischen Node-Empfehlungen von SMB sollen...	Geben Sie den folgenden Befehl ein...
Aktiviert	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</code>
Deaktiviert	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</code>

Die Einstellung der Option wird für neue SMB-Sessions wirksam. Clients mit vorhandener Verbindung können Node-Referral nur nutzen, wenn ihr vorhandenes Cache-Timeout abgelaufen ist.

3. Wechseln zur Berechtigungsstufe des Administrators: `set -privilege admin`

Verwandte Informationen

[Verfügbare SMB-Server-Optionen](#)

Mithilfe von Statistiken können Sie die Aktivitäten der automatischen Knotenverweisung überwachen

Um festzustellen, wie viele SMB-Verbindungen angesprochen werden, können Sie die

Aktivitäten zur automatischen Knotenverweisung mithilfe von `überwachen statistics` Befehl. Durch die Überwachung von Empfehlungen können Sie bestimmen, inwieweit automatische Empfehlungen Verbindungen auf Knoten, die die Freigaben hosten, suchen und ob Sie Ihre Daten-LIFs neu verteilen sollten, um besseren lokalen Zugriff auf Freigaben auf dem CIFS-Server zu ermöglichen.

Über diese Aufgabe

Der `cifs` Das Objekt bietet mehrere Zähler auf der erweiterten Berechtigungsebene, die beim Monitoring von SMB-Empfehlungen für automatische Nodes hilfreich sind:

- `node_referral_issued`

Anzahl der Clients, die eine Empfehlung an den Knoten des Stammes der Freigabe erhalten haben, nachdem der Client mit einer logischen Schnittstelle verbunden wurde, die von einem anderen Knoten als dem Stammknoten der Freigabe gehostet wird.

- `node_referral_local`

Anzahl der Clients, die mit einer logischen Schnittstelle verbunden sind, die von demselben Node gehostet wird, der den Share-Root hostet. Lokaler Zugriff bietet in der Regel eine optimale Performance.

- `node_referral_not_possible`

Anzahl der Clients, die nach der Verbindung mit einer logischen Schnittstelle, die von einem anderen Node als dem Stammknoten der Freigabe gehostet wird, keine Empfehlung an den Knoten erteilt wurden, der den Stammverzeichnis hostet. Dies liegt daran, dass eine aktive Daten-LIF für den Node des Share-Root nicht gefunden wurde.

- `node_referral_remote`

Anzahl der Clients, die mit einer logischen Schnittstelle verbunden sind, die von einem Node gehostet wird, der sich vom Node unterscheidet, der das Share-Root hostet. Remote-Zugriff kann zu Performance-Beeinträchtigungen führen.

Sie können die Statistiken zur automatischen Node-Empfehlungen für Ihre Storage Virtual Machine (SVM) überwachen, indem Sie Daten für einen bestimmten Zeitraum (ein Beispiel) erfassen und anzeigen. Sie können Daten aus der Probe anzeigen, wenn Sie die Datenerfassung nicht beenden. Wenn Sie die Datenerfassung anhalten, erhalten Sie eine feste Probe. Wenn Sie die Datenerfassung nicht stoppen, können Sie aktualisierte Daten abrufen, die Sie zum Vergleich mit früheren Abfragen verwenden können. Der Vergleich kann Ihnen dabei helfen, Performance-Trends zu identifizieren.



Zur Auswertung und Verwendung der Informationen, die Sie aus dem `sammeln statistics` Befehl, sollten Sie die Verteilung von Clients in Ihren Umgebungen verstehen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Zeigen Sie die Statistiken zur automatischen Knotenverweisung mithilfe von `an statistics` Befehl.

In diesem Beispiel werden die Statistiken zur automatischen Knotenverweisung angezeigt, indem Daten für einen Probenzeitraum erfasst und angezeigt werden:

- a. Starten Sie die Sammlung: `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

- b. Warten Sie, bis die gewünschte Abholzeit abgelaufen ist.

- c. Beenden Sie die Sammlung: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

- d. Anzeigen der Statistiken zur automatischen Knotenverweisung: `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

Counter                                     Value
-----
node_name                                   node1
node_referral_issued                       0
node_referral_local                        1
node_referral_not_possible                 2
node_referral_remote                       2
...

node_name                                   node2
node_referral_issued                       2
node_referral_local                        1
node_referral_not_possible                 0
node_referral_remote                       2
...
```

Die Ausgabe zeigt Zähler für alle an SVM vs1 teilnehmenden Nodes an. Um Klarheit zu schaffen, werden im Beispiel nur Ausgabefelder mit Statistiken zur automatischen Knotenverweisung bereitgestellt.

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

Verwandte Informationen

[Anzeigen von Statistiken](#)

Überwachen Sie mithilfe eines Windows-Clients die Client-seitigen SMB-Informationen zur automatischen Knotenverweisung

Um zu bestimmen, welche Empfehlungen aus der Perspektive des Clients gemacht werden, können Sie die Windows verwenden `dfsutil.exe` Utility:

Das RSAT-Kit (Remote Server Administration Tools), das mit Windows 7 und späteren Clients verfügbar ist, enthält das `dfsutil.exe` Utility: Mithilfe dieses Dienstprogramms können Sie Informationen über den Inhalt des Empfehlungscache anzeigen sowie Informationen über jede Empfehlung anzeigen, die der Client derzeit verwendet. Sie können das Dienstprogramm auch verwenden, um den Empfehlungscache des Clients zu löschen. Weitere Informationen finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Bereitstellen der Ordnersicherheit für Freigaben mit Access-Based Enumeration

Bieten Sie die Ordnersicherheit für Freigaben mit einer Zugriffsübersicht zur Aufzählung

Wenn Access-Based Enumeration (ABE) auf einer SMB-Freigabe aktiviert ist, sehen Benutzer, die nicht über die Berechtigung zum Zugriff auf einen Ordner oder eine Datei in der Freigabe verfügen (sei es durch einzelne oder Gruppen-Berechtigungsbeschränkungen), nicht, dass freigegebene Ressourcen in ihrer Umgebung angezeigt werden, obwohl die Freigabe selbst sichtbar bleibt.

Mit herkömmlichen Freigabeeigenschaften können Sie festlegen, welche Benutzer (einzeln oder in Gruppen) die Berechtigung haben, Dateien oder Ordner in der Freigabe anzuzeigen oder zu ändern. Sie erlauben Ihnen jedoch nicht, zu steuern, ob Ordner oder Dateien innerhalb der Freigabe für Benutzer sichtbar sind, die nicht über die Berechtigung zum Zugriff auf sie verfügen. Dies kann zu Problemen führen, wenn die Namen dieser Ordner oder Dateien innerhalb der Freigabe vertrauliche Informationen beschreiben, z. B. die Namen der Kunden oder Produkte, die in der Entwicklung sind.

Access-Based Enumeration (ABE) erweitert die Share-Eigenschaften um die Aufzählung von Dateien und Ordnern innerhalb der Freigabe. ABE ermöglicht es Ihnen daher, die Anzeige von Dateien und Ordnern innerhalb der Freigabe anhand von Benutzerzugriffsrechten zu filtern. Das heißt, die Freigabe selbst wäre für alle Benutzer sichtbar, aber Dateien und Ordner innerhalb der Freigabe können angezeigt oder ausgeblendet werden von bestimmten Benutzern. Neben dem Schutz sensibler Informationen in Ihrem Arbeitsplatz ermöglicht Ihnen ABE, die Darstellung großer Verzeichnisstrukturen zu vereinfachen, und zwar zum Vorteil von Anwendern, die keinen Zugriff auf Ihre gesamte Bandbreite benötigen. Beispielsweise würde die Freigabe selbst für alle Benutzer sichtbar sein, aber Dateien und Ordner innerhalb der Freigabe können angezeigt oder ausgeblendet werden.

Erfahren Sie mehr über "[Auswirkungen auf die Performance bei Verwendung von SMB/CIFS Access Based Enumeration](#)".

Aktivieren oder deaktivieren Sie die Access-Based Enumeration von SMB-Freigaben

Sie können ABE (Access-Based Enumeration) auf SMB-Freigaben aktivieren oder deaktivieren, um Benutzern zu ermöglichen oder zu verhindern, dass sie freigegebene Ressourcen sehen, auf die sie keinen Zugriff haben.

Über diese Aufgabe

ABE ist standardmäßig deaktiviert.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein...
Aktivieren Sie ABE für eine neue Freigabe	<pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration</pre> Beim Erstellen einer SMB-Freigabe können Sie zusätzliche optionale Freigabeneinstellungen und zusätzliche Freigabeneigenschaften festlegen. Weitere Informationen finden Sie auf der man-Page für das <code>vserver cifs share create</code> Befehl.
Aktivieren Sie ABE für eine vorhandene Freigabe	<pre>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</pre> Bestehende Freigabegenschaften bleiben erhalten. Die ABE-Share-Eigenschaft wird der bestehenden Liste der Freigabeliegenschaften hinzugefügt.
Deaktivieren Sie ABE für eine vorhandene Freigabe	<pre>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</pre> Andere gemeinsame Eigenschaften bleiben erhalten. Nur die ABE-Share-Eigenschaft wird aus der Liste der Share-Eigenschaften entfernt.

2. Überprüfen Sie, ob die Share-Konfiguration mit dem korrekt ist `vserver cifs share show` Befehl.

Beispiele

Im folgenden Beispiel wird eine ABE SMB-Freigabe mit dem Namen „sales“ mit einem Pfad von `/sales` auf SVM vs1. Die Freigabe wird mit `access-based-enumeration` als Freigabegenschaft:

```

cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                Vserver: vs1
                Share: sales
CIFS Server NetBIOS Name: VS1
                Path: /sales
                Share Properties: access-based-enumeration
                                oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

```

Im folgenden Beispiel wird das hinzugefügt `access-based-enumeration` Eigenschaft für SMB-Freigabe mit dem Namen „data2“:

```

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2       oplocks,browsable,changenotify,access-based-enumeration

```

Verwandte Informationen

[Hinzufügen oder Entfernen von Share-Eigenschaften für eine vorhandene SMB-Freigabe](#)

Aktivieren oder deaktivieren Sie die Access-Based Enumeration von einem Windows-Client

Sie können ABE (Access-Based Enumeration) auf SMB-Freigaben von einem Windows-Client aktivieren oder deaktivieren. Dadurch können Sie diese

Freigabegationseinstellung konfigurieren, ohne eine Verbindung zum CIFS-Server herstellen zu müssen.



Der abecmd Dienstprogramm ist in neuen Versionen von Windows Server und Windows Clients nicht verfügbar. Sie wurde im Rahmen von Windows Server 2008 freigegeben. Der Support für Windows Server 2008 wurde am 14. Januar 2020 eingestellt.

Schritte

1. Geben Sie von einem Windows-Client, der ABE unterstützt, den folgenden Befehl ein: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

Weitere Informationen zum abecmd Weitere Informationen finden Sie in der Dokumentation des Windows-Clients.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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