Sicherer NFS-Zugriff über Exportrichtlinien

ONTAP 9

NetApp
April 24, 2024

Inhalt

Sicherer NFS-Zugriff über Exportrichtlinien

Wie Exportrichtlinien den Client-Zugriff auf Volumes oder qtrees steuern

Exportrichtlinien enthalten mindestens eine *Exportregel*, die jede Clientzugriffsanforderung verarbeitet. Das Ergebnis des Prozesses legt fest, ob der Client-Zugriff verweigert oder gewährt wird und welche Zugriffsstufe. Auf der Storage Virtual Machine (SVM) muss eine Exportrichtlinie mit Exportregeln vorhanden sein, damit Clients auf Daten zugreifen können.

Sie verknüpfen jedem Volume oder qtree exakt eine Exportrichtlinie, um den Client-Zugriff auf das Volume oder qtree zu konfigurieren. Die SVM kann mehrere Exportrichtlinien enthalten. Dies ermöglicht Ihnen die folgenden Aktionen für SVMs mit mehreren Volumes oder qtrees:

- Jedem Volume oder qtree der SVM müssen für jedes Volume oder qtree verschiedene Exportrichtlinien zugewiesen werden, um für jedes Volume oder qtree in der SVM individuelle Zugriffskontrollen zu ermöglichen.
- Weisen Sie für eine identische Client-Zugriffskontrolle dieselbe Exportrichtlinie mehreren Volumes oder qtrees der SVM zu, ohne dass für jedes Volume oder qtree eine neue Exportrichtlinie erstellt werden muss.

Wenn ein Client eine Zugriffsanforderung stellt, die von der entsprechenden Exportrichtlinie nicht zulässig ist, schlägt die Anforderung mit einer Nachricht, die eine Berechtigung verweigert hat, fehl. Wenn ein Client keine Regel in der Exportrichtlinie enthält, wird der Zugriff verweigert. Wenn eine Exportrichtlinie leer ist, werden alle Zugriffe implizit verweigert.

Sie können eine Exportrichtlinie auf einem System, auf dem ONTAP ausgeführt wird, dynamisch ändern.

Standardmäßige Exportrichtlinie für SVMs

Jede SVM verfügt über eine standardmäßige Exportrichtlinie, die keine Regeln enthält. Bevor Clients auf Daten auf der SVM zugreifen können, muss eine Exportrichtlinie mit Regeln vorhanden sein. Jedes FlexVol Volume in der SVM muss einer Exportrichtlinie zugeordnet werden.

Wenn Sie eine SVM erstellen, erstellt das Storage-System automatisch eine Standard-Exportrichtlinie mit dem Namen `default` Für das Root-Volume der SVM. Sie müssen eine oder mehrere Regeln für die Standard-Exportrichtlinie erstellen, bevor Clients auf Daten auf der SVM zugreifen können. Alternativ können Sie auch eine benutzerdefinierte Exportrichtlinie mit Regeln erstellen. Sie können die Standard-Exportrichtlinie ändern und umbenennen, aber Sie können die standardmäßige Exportrichtlinie nicht löschen.

Wenn Sie ein FlexVol Volume mit SVM erstellen, erstellt das Storage-System das Volume und ordnet das Volume der standardmäßigen Exportrichtlinie für das Root-Volume der SVM zu. Standardmäßig ist jedes in der SVM erstellte Volume der standardmäßigen Exportrichtlinie für das Root-Volume zugeordnet. Sie können die Standard-Exportrichtlinie für alle Volumes in der SVM verwenden oder für jedes Volume eine eindeutige Exportrichtlinie erstellen. Sie können mehrere Volumes derselben Exportrichtlinie zuordnen.

Wie Exportregeln funktionieren

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

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

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

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

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

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

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

> Ab ONTAP 9.3 können Sie die Überprüfung der Konfiguration der Exportrichtlinie als Hintergrundjob aktivieren, der Regelverletzungen in einer Fehlerregelliste aufzeichnet. Der `vserver export-policy config-checker` Befehle rufen den Checker auf und zeigen Ergebnisse an, mit denen Sie Ihre Konfiguration überprüfen und fehlerhafte Regeln aus der Richtlinie löschen können.
>
> Die Befehle validieren lediglich die Exportkonfiguration für Hostnamen, Netzwerkgruppen und anonyme Benutzer.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

Die Client-Zugriffsanforderung wird mithilfe des NFSv3-Protokolls versendet, und der Client hat die IP-Adresse 10.1.17.37.

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

nicht für diesen Client.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

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

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

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

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

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

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

Verwalten von Clients mit einem nicht aufgelisteten Sicherheitstyp

Wenn ein Client sich mit einem Sicherheitstyp präsentiert, der nicht in einem Zugriffsparameter einer Exportregel aufgeführt ist, haben Sie die Wahl, entweder den Zugriff auf den Client zu verweigern oder ihn stattdessen der anonymen Benutzer-ID zuzuordnen, indem Sie die Option verwenden `none` Im Zugriffsparameter.

Ein Client kann sich mit einem Sicherheitstyp präsentieren, der nicht in einem Zugriffsparameter aufgeführt ist, da er mit einem anderen Sicherheitstyp authentifiziert wurde oder überhaupt nicht authentifiziert wurde (Sicherheitstyp AUTH_NONE). Standardmäßig wird dem Client automatisch der Zugriff auf diese Ebene

verweigert. Sie können die Option jedoch hinzufügen `none` Zum Zugriffsparameter. Als Ergebnis werden Clients mit einem nicht aufgelisteten Sicherheitsstil stattdessen der anonymen Benutzer-ID zugeordnet. Der `-anon` Parameter legt fest, welche Benutzer-ID diesen Clients zugewiesen ist. Die für das angegebene Benutzer-ID `-anon` Der Parameter muss ein gültiger Benutzer sein, der mit Berechtigungen konfiguriert ist, die Sie für den anonymen Benutzer als geeignet erachten.

Gültige Werte für das `-anon` Parameterbereich von `0` Bis `65535`.

Benutzer-ID zugewiesen zu `-anon`	**Die sich daraus ergebende Bearbeitung von Client-Zugriffsanfragen**
`0 - 65533`	Die Clientzugriffsanforderung wird der anonymen Benutzer-ID zugeordnet und erhält je nach den für diesen Benutzer konfigurierten Berechtigungen Zugriff.
`65534`	Die Client-Zugriffsanforderung ist dem Benutzer niemand zugeordnet und erhält je nach den für diesen Benutzer konfigurierten Berechtigungen Zugriff. Dies ist die Standardeinstellung.
`65535`	Die Zugriffsanforderung eines beliebigen Clients wird verweigert, wenn diese ID zugeordnet ist, und der Client stellt sich mit dem Sicherheitstyp AUTH_NONE vor. Die Zugriffsanforderung von Clients mit Benutzer-ID 0 wird verweigert, wenn sie dieser ID zugeordnet sind und der Client sich mit jedem anderen Sicherheitstyp präsentiert.

Wenn Sie die Option verwenden `none`, Es ist wichtig zu beachten, dass der schreibgeschützte Parameter zuerst verarbeitet wird. Beachten Sie die folgenden Richtlinien, wenn Sie Exportregeln für Clients mit nicht aufgeführten Sicherheitstypen konfigurieren:

Read-Only umfasst `none`	**Lese-Schreib-enthält** `none`	**Dadurch wird Zugriff für Clients mit nicht aufgelisteten Sicherheitstypen gewährleistet**
Nein	Nein	Abgelehnt
Nein	Ja.	Abgelehnt, da schreibgeschützt zuerst verarbeitet wird
Ja.	Nein	Schreibgeschützt als anonym
Ja.	Ja.	Lese-Schreib als anonym

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

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

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

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert sich nicht (was bedeutet Sicherheitstyp AUTH_NONE).

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf Clients mit eigener Benutzer-ID, die mit AUTH_SYS authentifiziert wurde. Der schreibgeschützte Parameter ermöglicht schreibgeschützten Zugriff als anonymer Benutzer mit Benutzer-ID 70 auf Clients, die mit anderen Sicherheitstypen authentifiziert wurden. Der Lese-Schreib-Parameter erlaubt Lese-Schreib-Zugriff auf jeden Sicherheitstyp, gilt in diesem Fall jedoch nur für Clients, die bereits durch die schreibgeschützte Regel gefiltert sind.

Clients #1 und #3 erhalten daher Lese-/Schreibzugriff nur als anonymer Benutzer mit Benutzer-ID 70. Client #2 erhält Lese-/Schreibzugriff mit einer eigenen Benutzer-ID.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

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

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

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert sich nicht (was bedeutet Sicherheitstyp AUTH_NONE).

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf Clients mit eigener Benutzer-ID, die mit AUTH_SYS authentifiziert wurde. Der schreibgeschützte Parameter ermöglicht schreibgeschützten Zugriff als anonymer Benutzer mit Benutzer-ID 70 auf Clients, die mit anderen Sicherheitstypen authentifiziert wurden. Der Lese-Schreib-Parameter erlaubt den Lese-Schreib-Zugriff nur als anonymer Benutzer.

Client #1 und Client #3 erhalten daher nur Lese-/Schreibzugriff als anonymer Benutzer mit Benutzer-ID 70. Client #2 erhält schreibgeschützten Zugriff mit einer eigenen Benutzer-ID, wird aber Lese-Schreib-Zugriff

verweigert.

Wie Sicherheitstypen die Client-Zugriffsebenen bestimmen

Der Sicherheitstyp, mit dem der Client authentifiziert wurde, spielt eine besondere Rolle in den Exportregeln. Sie müssen verstehen, wie der Sicherheitstyp die Zugriffsebenen bestimmt, die der Client zu einem Volume oder qtree erhält.

Die drei möglichen Zugriffsebenen sind wie folgt:

1. Schreibgeschützt
2. Lesen und schreiben
3. Superuser (für Clients mit Benutzer-ID 0)

Da die Zugriffsebene nach Sicherheitstyp in dieser Reihenfolge ausgewertet wird, müssen Sie beim Erstellen von Parametern auf Zugriffsebene in Exportregeln folgende Regeln beachten:

Damit ein Client die Zugriffsebene abrufen kann…	**Diese Zugriffsparameter müssen dem Sicherheitstyp des Clients entsprechen…**
Normaler Benutzer schreibgeschützt	Schreibgeschützt (`-rorule`)
Normaler Benutzer Lese-/Schreibzugriff	Schreibgeschützt (`-rorule`) Und lesen-schreiben (`-rwrule`)
Schreibgeschützt für Superuser	Schreibgeschützt (`-rorule`) Und `-superuser`
Superuser lesen und schreiben	Schreibgeschützt (`-rorule`) Und lesen-schreiben (`-rwrule`) Und `-superuser`

Die folgenden Sicherheitstypen sind für jeden der folgenden drei Zugriffsparameter gültig:

- `any`
- `none`
- `never`

  Dieser Sicherheitstyp ist für die Verwendung mit dem nicht gültig `-superuser` Parameter.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Beim Abgleich des Sicherheitstyps eines Clients mit jedem der drei Zugriffsparameter gibt es drei mögliche Ergebnisse:

Falls der Sicherheitstyp des Clients…	Dann der Client…
Stimmt mit dem im Zugriffsparameter angegebenen überein.	Erhält Zugriff auf dieses Level mit eigener Benutzer-ID.
Stimmt nicht mit dem angegebenen überein, der Zugriffsparameter enthält jedoch die Option `none`.	Ruft Zugriff auf diese Ebene, jedoch als anonymer Benutzer mit der von angegebenen Benutzer-ID ab `-anon` Parameter.
Stimmt nicht mit dem angegebenen überein und der Zugriffsparameter enthält die Option nicht `none`.	Für diese Ebene wird kein Zugriff erhalten.Dies gilt nicht für die `-superuser` Parameter, da er immer enthält `none` Auch wenn sie nicht angegeben werden.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

Client #1 hat die IP-Adresse 10.1.16.207, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH_SYS.

Client #3 hat die IP-Adresse 10.1.16.234, hat Benutzer-ID 0, sendet eine Zugriffsanforderung über das NFSv3-Protokoll und authentifiziert nicht (AUTH_NONE).

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen mit allen drei Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp. Der Lese-Schreib-Parameter ermöglicht den Lese-Schreib-Zugriff auf Clients mit eigener Benutzer-ID, die mit AUTH_SYS oder Kerberos v5 authentifiziert wurden. Der Superuser-Parameter ermöglicht Superuser-Zugriff auf Clients mit Benutzer-ID 0, die mit Kerberos v5 authentifiziert wurden.

Client #1 erhält daher Lese-/Schreibzugriff für Superuser, da er alle drei Zugriffsparameter einordnet. Client #2 erhält Lese-/Schreibzugriff, aber keinen Superuser-Zugriff. Client #3 erhält nur Lesezugriff, aber keinen Superuser-Zugriff.

Management von Zugriffsanfragen durch Superbenutzer

Wenn Sie Exportrichtlinien konfigurieren, müssen Sie berücksichtigen, was Sie tun möchten, wenn das Storage-System eine Client-Zugriffsanfrage mit Benutzer-ID 0 erhält, also als Superuser, und Ihre Exportregeln entsprechend festlegen.

In der UNIX-Welt wird ein Benutzer mit der Benutzer-ID 0 als Superuser bezeichnet, der normalerweise root genannt wird, der unbegrenzte Zugriffsrechte auf einem System besitzt. Die Verwendung von Superuser-

Berechtigungen kann aus verschiedenen Gründen gefährlich sein, einschließlich Verletzung des Systems und der Datensicherheit.

Standardmäßig ordnet ONTAP Clients, die mit der Benutzer-ID 0 angezeigt werden, dem anonymen Benutzer zu. Sie können jedoch die angeben `- superuser` Parameter in Exportregeln, um zu bestimmen, wie Clients, die je nach Sicherheitstyp mit Benutzer-ID 0 angegeben werden, behandelt werden. Die folgenden Optionen sind gültig für die `-superuser` Parameter:

- `any`
- `none`

  Dies ist die Standardeinstellung, wenn Sie den nicht angeben `-superuser` Parameter.

- `krb5`
- `ntlm`
- `sys`

Es gibt zwei verschiedene Arten, wie Clients, die mit der Benutzer-ID 0 angezeigt werden, je nach behandelt werden `-superuser` Parameterkonfiguration:

Wenn der `-superuser` Parameter und der Sicherheitstyp des Clients…	**Dann der Client…**
Übereinstimmung	Erhält Superuser-Zugriff mit Benutzer-ID 0.
Stimmen Sie nicht überein	Ruft als anonymer Benutzer mit der vom angegebenen Benutzer-ID auf `-anon` Parameter und seine zugewiesenen Berechtigungen. Dies ist unabhängig davon, ob der Parameter schreibgeschützt oder Lesen/Schreiben die Option angibt `none`.

Wenn ein Client mit der Benutzer-ID 0 angezeigt wird, um auf ein Volume mit dem NTFS-Sicherheitsstil und dem zuzugreifen `-superuser` Parameter ist auf festgelegt `none`, ONTAP verwendet die Namenszuweisung für den anonymen Benutzer, um die richtigen Anmeldedaten zu erhalten.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Client #1 hat die IP-Adresse 10.1.16.207, hat Benutzer-ID 746, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH_SYS.

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

Client #2 erhält keinen Superuser-Zugriff. Stattdessen wird sie anonym zugeordnet, weil die `-superuser` Parameter wurde nicht angegeben. Das bedeutet, dass es standardmäßig eingestellt ist `none` Und ordnet die Benutzer-ID 0 automatisch anonym zu. Client #2 erhält auch nur schreibgeschützten Zugriff, da sein Sicherheitstyp nicht mit dem Parameter Read-Write übereinstimmt.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Client #1 hat die IP-Adresse 10.1.16.207, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH_SYS.

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

Die Exportregel erlaubt Superuser-Zugriff für Clients mit Benutzer-ID 0. Client #1 erhält Superuser-Zugriff, da er mit der Benutzer-ID und dem Sicherheitstyp für den schreibgeschützten und übereinstimmt `-superuser` Parameter. Client #2 erhält keinen Lese-/Schreib- oder Superuser-Zugriff, da sein Sicherheitstyp nicht mit dem Lese-Schreib-Parameter oder dem übereinstimmt `-superuser` Parameter. Stattdessen wird Client #2 dem anonymen Benutzer zugeordnet, der in diesem Fall die Benutzer-ID 0 hat.

So nutzt ONTAP Exportrichtlinien-Caches

Zur Verbesserung der Systemperformance verwendet ONTAP lokale Caches zum Speichern von Informationen wie Hostnamen und Netzwerkgruppen. So kann ONTAP die Regeln für Exportrichtlinien schneller verarbeiten als die Informationen aus externen Quellen abzurufen. Informationen über die Caches und ihre Maßnahmen können Ihnen bei der Fehlerbehebung bei Problemen mit dem Client-Zugriff helfen.

Sie konfigurieren Exportrichtlinien, um den Client-Zugriff auf NFS-Exporte zu steuern. Jede Exportrichtlinie enthält Regeln, und jede Regel enthält Parameter, die der Regel entsprechen, die Clients, die Zugriff

anfordern, anfordert. Bei einigen dieser Parameter muss ONTAP eine externe Quelle kontaktieren, z. B. DNS- oder NIS-Server, um Objekte wie Domain-Namen, Host-Namen oder Netzwerkgruppen zu lösen.

Diese Kommunikation mit externen Quellen nimmt eine kleine Menge Zeit in Anspruch. Um die Performance zu steigern, reduziert ONTAP die benötigte Zeit zur Auflösung von Objekten für Exportregelungen, indem Informationen lokal auf jedem Node in mehreren Caches gespeichert werden.

Cache-Name	Art der gespeicherten Informationen
Datenzugriff	Zuordnung von Clients zu entsprechenden Exportrichtlinien
Name	Zuordnungen von UNIX-Benutzernamen zu entsprechenden UNIX-Benutzer-IDs
ID	Zuordnungen von UNIX-Benutzer-IDs zu entsprechenden UNIX-Benutzer-IDs und erweiterten UNIX-Gruppen-IDs
Host	Zuordnung von Hostnamen zu entsprechenden IP-Adressen
Netzgruppe	Zuordnung von Netzgruppen zu entsprechenden IP-Adressen der Mitglieder
Showmount	Liste der exportierten Verzeichnisse aus SVM Namespace

Wenn Sie nach dem Abrufen und Speichern von ONTAP Daten über die externen Nameserver in Ihrer Umgebung ändern, können die Caches nun veraltete Informationen enthalten. Auch wenn ONTAP Cache-Aktualisierungen nach bestimmten Zeiträumen automatisch aktualisiert, haben verschiedene Caches unterschiedliche Ablaufdaten, Aktualisierungszeiten und Algorithmen.

Ein weiterer möglicher Grund, warum Caches veraltete Informationen enthalten, ist, wenn ONTAP versucht, zwischengespeicherte Informationen zu aktualisieren, aber beim Versuch, mit Name-Servern zu kommunizieren, einen Fehler auftritt. Sollte dies der Fall sein, verwendet ONTAP die derzeit in den lokalen Caches gespeicherten Informationen weiter, um eine Client-Unterbrechung zu vermeiden.

Dadurch können Clientzugriffsanforderungen, die erfolgreich ausgeführt werden sollen, fehlschlagen, und Clientzugriffsanfragen, die fehlschlagen sollen, können erfolgreich ausgeführt werden. Sie können einige der Caches für Exportrichtlinien anzeigen und manuell bereinigen, wenn Sie solche Probleme mit dem Clientzugriff beheben.

So funktioniert der Zugriffs-Cache

ONTAP verwendet einen Zugriffs-Cache, um die Ergebnisse der Bewertung von Exportrichtlinien für Client-Zugriffsoperationen auf ein Volume oder einen qtree zu speichern. Das führt zu Performance-Verbesserungen, da die Informationen viel schneller aus dem Zugriffs-Cache abgerufen werden können als jedes Mal, wenn ein Client eine I/O-Anforderung sendet, den Auswertungsprozess für die Richtlinie für den Export

durchzugehen.

Sobald ein NFS-Client eine I/O-Anforderung für den Zugriff auf Daten eines Volume oder qtree sendet, muss ONTAP jede I/O-Anfrage bewerten, um zu ermitteln, ob die I/O-Anforderung erteilt oder abgelehnt werden soll. Diese Bewertung beinhaltet die Überprüfung jeder Regel für die Exportrichtlinie, die mit dem Volume oder qtree verknüpft ist. Wenn der Pfad zum Volume oder qtree einen oder mehrere Verbindungspunkte überschreiten muss, muss diese Prüfung möglicherweise für mehrere Exportrichtlinien entlang des Pfads durchgeführt werden.

Beachten Sie, dass diese Bewertung für jede von einem NFS-Client gesendete I/O-Anfrage, z. B. Lesen, Schreiben, Liste, Kopieren und andere Vorgänge, nicht nur für anfängliche Mount-Anforderungen durchgeführt wird.

Nachdem ONTAP die geltenden Regeln für die Exportrichtlinie ermittelt und entschieden hat, ob die Anfrage zugelassen werden soll oder abgelehnt wird, erstellt ONTAP dann zum Speichern dieser Informationen einen Eintrag im Zugriffs-Cache.

Wenn ein NFS-Client eine I/O-Anfrage sendet, nimmt ONTAP die IP-Adresse des Clients, die ID der SVM und die dem Ziel-Volume oder qtree zugeordnete Exportrichtlinie zur Kenntnis. Außerdem überprüft er zuerst den Zugriffs-Cache auf einen entsprechenden Eintrag. Wenn im Zugriffs-Cache ein übereinstimmender Eintrag vorhanden ist, verwendet ONTAP die gespeicherten Informationen, um die I/O-Anforderung zuzulassen oder abzulehnen. Wenn kein übereinstimmender Eintrag vorhanden ist, durchläuft ONTAP den normalen Prozess der Auswertung aller anwendbaren Richtlinienregeln, wie oben erläutert.

Einträge im Zugriffs-Cache, die nicht aktiv genutzt werden, werden nicht aktualisiert. Dies reduziert unnötige und verschwenderische Kommunikation mit externen Namen dient.

Das Abrufen der Informationen aus dem Zugriffs-Cache ist wesentlich schneller als das Auswertungsprozess für die gesamte Exportrichtlinie für jede I/O-Anforderung. Daher verbessert die Nutzung des Zugriffs-Cache die Performance immens, indem der Overhead von Client-Zugriffsprüfungen verringert wird.

Funktionsweise von Zugriffsparametern im Cache

Mehrere Parameter steuern die Aktualisierungszeiträume für Einträge im Zugriffs-Cache. Wenn Sie die Funktionsweise dieser Parameter verstehen, können Sie sie ändern, um den Zugriffs-Cache zu optimieren und die Performance mit den neuesten gespeicherten Informationen abzustimmen.

Im Zugriffs-Cache werden Einträge gespeichert, die aus einer oder mehreren Exportregeln bestehen, die für Clients gelten, die auf Volumes oder qtrees zugreifen möchten. Diese Einträge werden für eine bestimmte Zeit gespeichert, bevor sie aktualisiert werden. Die Aktualisierungszeit wird durch Parameter des Zugriffs-Caches bestimmt und hängt vom Typ des Eintrags aus dem Zugriffs-Cache ab.

Sie können Parameter für den Zugriffs-Cache für einzelne SVMs festlegen. Dadurch können die Parameter entsprechend den SVM-Zugriffsanforderungen variieren. Nicht aktiv verwendete Zugriffs-Cache-Einträge werden nicht aktualisiert, was die unnötige und verschwenderische Kommunikation mit externen Namen reduziert.

Eintragstyp für den Zugriffs-Cache	Beschreibung	Aktualisierung innerhalb von Sekunden

Positive Beiträge	Einträge im Zugriffs-Cache, die nicht zu einem Denial-Access-Zugriff auf Clients geführt haben.	Minimum: 300 Maximal 86,400 Standard: 3,600
Negative Einträge	Einträge im Zugriffs-Cache, die zu einem Denial-Access-Zugriff auf Clients geführt haben.	Minimum: 60 Maximal 86,400 Standard: 3,600

Beispiel

Ein NFS-Client versucht, auf ein Volume in einem Cluster zuzugreifen. ONTAP stimmt den Client mit einer Regel für die Exportrichtlinie ab und legt fest, dass der Client basierend auf der Konfiguration der Regel für die Exportrichtlinie auf Zugriff erhält. Als positiver Eintrag speichert ONTAP die Regel für die Exportrichtlinie im Zugriffs-Cache. Standardmäßig behält ONTAP den positiven Eintrag im Zugriffs-Cache eine Stunde (3,600 Sekunden) bei und aktualisiert den Eintrag automatisch, um die Informationen auf dem aktuellen Stand zu halten.

Um zu verhindern, dass der Zugriffs-Cache unnötig auffüllt wird, gibt es einen zusätzlichen Parameter, um vorhandene Einträge aus dem Zugriffs-Cache zu löschen, die für einen bestimmten Zeitraum nicht verwendet wurden, um den Client-Zugriff zu bestimmen. Das `-harvest-timeout` Der zulässige Bereich für den Parameter beträgt 60 bis 2,592,000 Sekunden und die Standardeinstellung 86,400 Sekunden.

Entfernen Sie eine Exportrichtlinie von einem qtree

Wenn Sie sich entscheiden, dass einer bestimmten Exportrichtlinie einem qtree nicht mehr zugewiesen wird, können Sie die Exportrichtlinie entfernen, indem Sie den qtree ändern, um die Exportrichtlinie des enthaltenden Volumes stattdessen zu übernehmen. Dies können Sie mit dem tun `volume qtree modify` Befehl mit dem `-export -policy` Parameter und eine leere Namenszeichenfolge („").

Schritte

1. Geben Sie den folgenden Befehl ein, um eine Exportrichtlinie von einem qtree zu entfernen:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Vergewissern Sie sich, dass der qtree entsprechend geändert wurde:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Qtree IDs für qtree-Dateivorgänge validieren

ONTAP kann eine zusätzliche Validierung von qtree IDs optional durchführen. Diese Validierung stellt sicher, dass Anforderungen der Client-Dateioperationen eine gültige qtree ID verwenden und dass Clients Dateien nur innerhalb desselben qtree verschieben

können. Sie können diese Validierung aktivieren oder deaktivieren, indem Sie den ändern `-validate-qtree-export` Parameter. Dieser Parameter ist standardmäßig aktiviert.

Über diese Aufgabe

Dieser Parameter ist nur dann effektiv, wenn Sie einer oder mehreren qtrees auf der Storage Virtual Machine (SVM) eine Exportrichtlinie direkt zugewiesen haben.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn die qtree ID-Validierung gewünscht wird…	Geben Sie den folgenden Befehl ein…
Aktiviert	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Deaktiviert	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Einschränkungen der Exportrichtlinien und verschachtelte Verbindungen für FlexVol Volumes

Wenn Sie Exportrichtlinien so konfiguriert haben, dass eine weniger restriktive Richtlinie für eine verschachtelte Verbindung festgelegt wird, jedoch eine restriktivere Richtlinie für eine Verbindung höherer Ebene, kann der Zugriff auf die untere Ebene fehlschlagen.

Sie sollten sicherstellen, dass Verbindungen auf höherer Ebene weniger restriktive Exportrichtlinien aufweisen als Verbindungen auf niedrigerer Ebene.