Sécurisation de l'accès NFS à l'aide de règles d'exportation

ONTAP 9

NetApp
April 24, 2024

Sommaire

Sécurisation de l’accès NFS à l’aide de règles d’exportation

Comment les règles d’exportation contrôlent l’accès des clients aux volumes ou aux qtrees

Les règles d’exportation contiennent une ou plusieurs *export rules* qui traitent chaque demande d’accès client. Le résultat du processus détermine si le client est refusé ou accordé et quel niveau d’accès. Un export policy avec règles d’export doit exister sur la machine virtuelle de stockage (SVM) afin que les clients puissent accéder aux données.

Vous associez exactement une export policy à chaque volume ou qtree pour configurer l’accès client au volume ou qtree. Le SVM peut contenir plusieurs export policy. Vous pouvez ainsi effectuer les opérations suivantes pour les SVM avec plusieurs volumes ou qtrees :

- Assigner différentes export policy à chaque volume ou qtree du SVM pour le contrôle d’accès client individuel à chaque volume ou qtree du SVM.
- Assigner la même export policy à plusieurs volumes ou qtree du SVM pour un contrôle d’accès client identique sans avoir à créer une nouvelle export policy pour chaque volume ou qtree.

Si un client effectue une demande d’accès qui n’est pas autorisée par la stratégie d’exportation applicable, la requête échoue et un message d’autorisation est refusé. Si un client ne correspond à aucune règle de l’export policy, l’accès est refusé. Si une export policy est vide, alors tous les accès sont implicitement refusés.

Vous pouvez modifier une export-policy de manière dynamique sur un système exécutant ONTAP.

Export policy par défaut pour SVM

Chaque SVM dispose d’une export policy par défaut qui ne contient aucune règle. Un export policy avec règles doit exister pour que les clients puissent accéder aux données sur la SVM. Chaque volume FlexVol contenu au SVM doit être associé à une export policy.

Lorsque vous créez un SVM, le système de stockage crée automatiquement une export policy par défaut appelée `default` Pour le volume root du SVM. On doit créer une ou plusieurs règles pour l’export policy par défaut avant que les clients puissent accéder aux données sur la SVM. Vous pouvez également créer une export-policy personnalisée avec des règles. Vous pouvez modifier et renommer l’export policy par défaut, mais vous ne pouvez pas supprimer l’export policy par défaut.

Lorsque vous créez un volume FlexVol dans son SVM contenant, le système de stockage crée le volume et associe le volume avec la export policy par défaut pour le volume root du SVM. Par défaut, chaque volume créé au sein du SVM est associé à l’export policy par défaut pour le volume root. Vous pouvez utiliser l’export policy par défaut pour tous les volumes contenus dans le SVM, ou bien créer une export policy unique pour chaque volume. Vous pouvez associer plusieurs volumes à la même export policy.

Fonctionnement des règles d’exportation

Les règles d’exportation sont les éléments fonctionnels d’une export-policy. Les règles

d'exportation correspondent aux demandes d'accès client à un volume par rapport à des paramètres spécifiques que vous configurez pour déterminer comment traiter les demandes d'accès client.

Une export-policy doit contenir au moins une règle d'exportation pour permettre l'accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l'ordre dans lequel elles apparaissent dans l'export-policy. L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Vous pouvez configurer des règles d'exportation pour déterminer les autorisations d'accès client à l'aide des critères suivants :

- Protocole d'accès aux fichiers utilisé par le client envoyant la requête, par exemple, NFSv4 ou SMB.
- Identifiant client, par exemple, nom d'hôte ou adresse IP.

  La taille maximale du `-clientmatch` le champ est composé de 4096 caractères.

- Type de sécurité utilisé par le client pour l'authentification, par exemple Kerberos v5, NTLM ou AUTH_SYS.

Si une règle spécifie plusieurs critères, le client doit tous les correspondre pour que la règle s'applique.

> Depuis ONTAP 9.3, vous pouvez activer la vérification de la configuration des règles d'exportation en tant que tâche d'arrière-plan qui enregistre toutes les violations de règles dans une liste de règles d'erreur. Le `vserver export-policy config-checker` les commandes invoquent le vérificateur et affichent les résultats, que vous pouvez utiliser pour vérifier votre configuration et supprimer des règles erronées de la stratégie.
>
> Les commandes valident uniquement la configuration d'exportation pour les noms d'hôte, les groupes réseau et les utilisateurs anonymes.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

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

La requête d'accès client est envoyée à l'aide du protocole NFSv3 et le client a l'adresse IP 10.1.17.37.

Bien que le protocole d'accès client corresponde, l'adresse IP du client se trouve dans un sous-réseau différent de celui spécifié dans la règle d'exportation. Par conséquent, la correspondance des clients échoue et cette règle ne s'applique pas à ce client.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs`

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

La requête d'accès client est envoyée via le protocole NFSv4 et le client a l'adresse IP 10.1.16.54.

Le protocole d'accès client correspond et l'adresse IP du client se trouve dans le sous-réseau spécifié. Par conséquent, la correspondance du client a réussi et cette règle s'applique à ce client. Le client obtient un accès en lecture-écriture quel que soit son type de sécurité.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

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

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Par conséquent, les deux clients bénéficient d'un accès en lecture seule. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

Gérez les clients avec un type de sécurité non répertorié

Lorsqu'un client se présente avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès d'une règle d'exportation, vous pouvez soit refuser l'accès au client, soit le mapper à l'ID utilisateur anonyme à la place de l'aide de l'option `none` dans le paramètre d'accès.

Un client peut se présenter avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès car il a été authentifié avec un type de sécurité différent ou n'a pas été authentifié du tout (type de sécurité AUTH_NONE). Par défaut, l'accès au client est automatiquement refusé. Toutefois, vous pouvez ajouter l'option `none` au paramètre d'accès. Par conséquent, les clients dont le style de sécurité n'est pas répertorié sont mappés sur l'ID utilisateur anonyme. Le `-anon` Paramètre détermine quel ID utilisateur est attribué à ces clients. ID utilisateur spécifié pour le `-anon` le paramètre doit être un utilisateur valide configuré avec des autorisations appropriées pour l'utilisateur anonyme.

Valeurs valides pour le `-anon` plage de paramètres de `0` à `65535`.

ID utilisateur attribué à `-anon`	Traitement des demandes d'accès client résultant
`0 - 65533`	La demande d'accès client est mappée à l'ID utilisateur anonyme et obtient l'accès en fonction des autorisations configurées pour cet utilisateur.
`65534`	La demande d'accès client est mappée à l'utilisateur personne et obtient l'accès en fonction des autorisations configurées pour cet utilisateur. Il s'agit de la valeur par défaut.
`65535`	La demande d'accès de n'importe quel client est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec le type de sécurité AUTH_NONE. La demande d'accès des clients avec l'ID utilisateur 0 est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec tout autre type de sécurité.

Lorsque vous utilisez l'option `none`, il est important de se rappeler que le paramètre lecture seule est traité en premier. Lors de la configuration des règles d'exportation pour les clients dont les types de sécurité ne sont pas répertoriés, prenez en compte les consignes suivantes :

La lecture seule inclut `none`	Lecture-écriture incluse `none`	Accès résultant pour les clients avec des types de sécurité non répertoriés
Non	Non	Refusée
Non	Oui.	Refusé car la lecture seule est traitée en premier
Oui.	Non	Lecture seule comme anonyme
Oui.	Oui.	Lecture-écriture comme anonyme

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

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

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le client #3 a l'adresse IP 10.1.16.234, envoie une demande d'accès à l'aide du protocole NFSv3 et ne s'authentifie pas (ce qui signifie le type de sécurité AUTH_NONE).

Le protocole d'accès client et l'adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l'accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de AUTH_SYS. Le paramètre lecture seule permet l'accès en lecture seule en tant qu'utilisateur anonyme avec l'ID utilisateur 70 aux clients authentifiés à l'aide de n'importe quel autre type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture à n'importe quel type de sécurité, mais s'applique uniquement aux clients déjà filtrés par la règle en lecture seule.

Par conséquent, les clients n° 1 et n° 3 bénéficient de l'accès en lecture-écriture uniquement en tant qu'utilisateur anonyme avec l'ID utilisateur 70. Le client #2 obtient un accès en lecture-écriture avec son propre ID utilisateur.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

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

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le client #3 a l'adresse IP 10.1.16.234, envoie une demande d'accès à l'aide du protocole NFSv3 et ne s'authentifie pas (ce qui signifie le type de sécurité AUTH_NONE).

Le protocole d'accès client et l'adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l'accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de AUTH_SYS. Le paramètre lecture seule permet l'accès en lecture seule en tant qu'utilisateur anonyme avec l'ID utilisateur 70 aux clients authentifiés à l'aide de n'importe quel autre type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture uniquement en tant qu'utilisateur anonyme.

Par conséquent, les clients #1 et le client #3 obtiennent un accès en lecture-écriture uniquement en tant qu'utilisateur anonyme avec l'ID utilisateur 70. Le client #2 obtient un accès en lecture seule avec son propre ID utilisateur, mais il est refusé l'accès en lecture-écriture.

Comment les types de sécurité déterminent les niveaux d'accès client

Le type de sécurité auquel le client s'est authentifié joue un rôle particulier dans les règles d'exportation. Vous devez comprendre la manière dont le type de sécurité

détermine les niveaux d'accès du client à un volume ou à un qtree.

Les trois niveaux d'accès possibles sont les suivants :

1. Lecture seule
2. Lecture-écriture
3. Super-utilisateur (pour les clients ayant l'ID utilisateur 0)

Dans la mesure où le niveau d'accès par type de sécurité est évalué dans cet ordre, vous devez respecter les règles suivantes lors de la construction de paramètres de niveau d'accès dans les règles d'exportation :

Pour qu'un client puisse obtenir le niveau d'accès…	**Ces paramètres d'accès doivent correspondre au type de sécurité du client…**
Lecture seule normale par l'utilisateur	Lecture seule (`-rorule`)
Lecture-écriture utilisateur normale	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`)
Super-utilisateur en lecture seule	Lecture seule (`-rorule`) et `-superuser`
Super-utilisateur lecture-écriture	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`) et `-superuser`

Les types de sécurité suivants sont valides pour chacun de ces trois paramètres d'accès :

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

  Ce type de sécurité n'est pas valide pour une utilisation avec `-superuser` paramètre.

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

Lorsque vous faites correspondre le type de sécurité d'un client à chacun des trois paramètres d'accès, trois résultats sont possibles :

Si le type de sécurité du client…	**Ensuite, le client…**
Correspond à celui spécifié dans le paramètre d'accès.	Obtient l'accès à ce niveau avec son propre ID utilisateur.

Si le type de sécurité du client…	Ensuite, le client…
Ne correspond pas à celui spécifié, mais le paramètre d'accès inclut l'option `none`.	Obtient l'accès pour ce niveau, mais en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le `-anon` paramètre.
Ne correspond pas à celui spécifié et le paramètre d'accès n'inclut pas l'option `none`.	Ne dispose d'aucun accès pour ce niveau.cela ne s'applique pas à l' `-superuser` paramètre car il inclut toujours `none` même si elle n'est pas spécifiée.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

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

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le client #3 a l'adresse IP 10.1.16.234, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et n'a pas authentifié (AUTH_NONE).

Le protocole d'accès client et l'adresse IP correspondent aux trois clients. Le paramètre lecture seule permet un accès en lecture seule à tous les clients, quel que soit leur type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture aux clients avec leur propre ID utilisateur authentifié par AUTH_SYS ou Kerberos v5. Le paramètre superuser permet un accès superuser aux clients avec l'ID utilisateur 0 authentifié avec Kerberos v5.

Par conséquent, le client #1 obtient l'accès en lecture-écriture superutilisateur car il correspond aux trois paramètres d'accès. Le client #2 obtient un accès en lecture-écriture mais pas un accès super-utilisateur. Le client #3 obtient un accès en lecture seule mais pas un accès super-utilisateur.

Gérer les demandes d'accès superutilisateur

Lorsque vous configurez des stratégies d'exportation, vous devez tenir compte de ce que vous voulez faire si le système de stockage reçoit une demande d'accès client avec l'ID utilisateur 0, c'est-à-dire en tant que superutilisateur, et définir vos règles d'exportation en conséquence.

Dans le monde UNIX, un utilisateur avec l'ID utilisateur 0 est appelé superutilisateur, généralement appelé root, qui dispose de droits d'accès illimités sur un système. L'utilisation des privilèges de superutilisateur peut être dangereuse pour plusieurs raisons, y compris une violation du système et de la sécurité des données.

Par défaut, ONTAP mappe les clients présentant l'ID utilisateur 0 à l'utilisateur anonyme. Toutefois, vous pouvez spécifier le `- superuser` Paramètre dans les règles d'exportation pour déterminer comment gérer les clients présentant l'ID utilisateur 0 en fonction de leur type de sécurité. Les options suivantes sont valides pour le `-superuser` paramètre :

- `any`
- `none`

  Il s'agit du paramètre par défaut si vous ne spécifiez pas le `-superuser` paramètre.

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

Il existe deux façons différentes de gérer les clients présentant l'ID utilisateur 0, selon le `-superuser` configuration des paramètres :

Si le `-superuser` et le type de sécurité du client…	Ensuite, le client…
Correspondance	Obtient l'accès superutilisateur avec l'ID utilisateur 0.
Ne correspondent pas	Obtient l'accès en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le `-anon` paramètre et ses autorisations attribuées. Cette option est précise si le paramètre lecture seule ou lecture-écriture spécifie l'option `none`.

Si un client se présente avec l'ID utilisateur 0 pour accéder à un volume avec le style de sécurité NTFS et le `-superuser` le paramètre est défini sur `none`, ONTAP utilise le mappage de noms pour l'utilisateur anonyme afin d'obtenir les informations d'identification appropriées.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

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

Le client n° 1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 746, envoie une demande d'accès à l'aide du protocole NFSv3 et s'authentifie avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés.

Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier.

Le client #2 ne dispose pas d'un accès super-utilisateur. Au lieu de cela, il est mappé sur anonyme car le `-superuser` paramètre non spécifié. Cela signifie que la valeur par défaut est `none` Et mappe automatiquement l'ID utilisateur 0 sur anonyme. Le client #2 obtient également un accès en lecture seule car son type de sécurité ne correspond pas au paramètre lecture-écriture.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

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

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

La règle d'exportation permet l'accès superutilisateur pour les clients avec l'ID utilisateur 0. Le client #1 obtient l'accès superutilisateur car il correspond à l'ID utilisateur et au type de sécurité pour la lecture seule et `-superuser` paramètres. Le client #2 ne dispose pas d'un accès en lecture-écriture ou super-utilisateur, car son type de sécurité ne correspond pas au paramètre en lecture-écriture ou au `-superuser` paramètre. Au lieu de cela, le client #2 est mappé à l'utilisateur anonyme, qui a dans ce cas l'ID utilisateur 0.

Utilisation des caches de règles d'exportation par ONTAP

Pour améliorer les performances système, ONTAP utilise des caches locaux pour stocker des informations telles que les noms d'hôtes et les groupes de réseaux. Cela permet à ONTAP de traiter les règles des export-policy plus rapidement que de récupérer les informations à partir de sources externes. Comprendre ce qu'sont les caches et ce qu'ils font pour vous aider à résoudre les problèmes d'accès client.

Vous configurez les export policy pour contrôler l'accès client aux exports NFS. Chaque export policy contient des règles, et chaque règle contient des paramètres qui correspondent à la règle avec les clients demandant un accès. Certains de ces paramètres exigent que ONTAP contacte une source externe, telle que des serveurs DNS ou NIS, pour résoudre des objets tels que des noms de domaine, des noms d'hôtes ou des groupes réseau.

Ces communications avec des sources externes prennent peu de temps. Afin d'améliorer les performances,

ONTAP réduit le temps nécessaire à la résolution des objets de règles d'exportation en stockant les informations localement sur chaque nœud dans plusieurs caches.

Nom du cache	Type d'information stockée
L'accès	Mise en correspondance des clients avec les règles d'exportation correspondantes
Nom	Mappage des noms d'utilisateur UNIX avec les ID utilisateur UNIX correspondants
ID	Mappage des ID utilisateur UNIX avec les ID utilisateur UNIX correspondants et les ID de groupe UNIX étendus
Hôte	Mappages de noms d'hôtes sur les adresses IP correspondantes
Groupe réseau	Mappages de groupes réseau aux adresses IP correspondantes des membres
Showmount	Liste des répertoires exportés depuis le namespace du SVM

Si vous modifiez les informations sur les serveurs de noms externes de votre environnement après la récupération et le stockage en local par ONTAP, les caches peuvent désormais contenir des informations obsolètes. Bien que les mises à jour ONTAP se placent automatiquement après certaines périodes, différents caches ont des temps d'expiration et d'actualisation et des algorithmes différents.

Une autre raison possible pour que les caches contiennent des informations obsolètes est le moment où ONTAP tente d'actualiser les informations en cache mais rencontre un échec lors de tentatives de communication avec des serveurs de noms. Dans ce cas, ONTAP continue d'utiliser les informations actuellement stockées dans les caches locaux pour éviter toute perturbation du client.

Par conséquent, les demandes d'accès des clients qui sont censées réussir risquent d'échouer et les demandes d'accès des clients qui sont censées échouer pourraient réussir. Vous pouvez afficher et vider manuellement certains caches de règles d'exportation lors du dépannage de tels problèmes d'accès client.

Fonctionnement du cache d'accès

ONTAP utilise un cache d'accès pour stocker les résultats de l'évaluation de la règle d'export policy pour les opérations d'accès client à un volume ou à un qtree. Il en résulte une amélioration des performances, car les informations peuvent être récupérées beaucoup plus rapidement depuis le cache d'accès qu'un processus d'évaluation des règles d'export-policy à chaque fois qu'un client envoie une requête d'E/S.

Lorsqu'un client NFS envoie une requête d'E/S pour accéder aux données d'un volume ou qtree, ONTAP doit évaluer chaque demande d'E/S afin de déterminer s'il faut accorder ou refuser la demande d'E/S. Cette évaluation implique de vérifier chaque règle d'export policy de la export policy associée au volume ou à qtree. Si le chemin vers le volume ou qtree implique de franchir un ou plusieurs points de jonction, cette vérification

peut s’avérer nécessaire pour rechercher plusieurs règles d’exportation le long du chemin.

Notez que cette évaluation est effectuée pour chaque demande d’E/S envoyée depuis un client NFS, par exemple pour la lecture, l’écriture, la liste, la copie et d’autres opérations. Il ne s’agit pas uniquement de demandes de montage initiales.

Une fois que ONTAP a identifié les règles d’export policy applicables et a décidé d’autoriser ou de refuser la requête, ONTAP crée ensuite une entrée dans le cache d’accès pour stocker ces informations.

Lorsqu’un client NFS envoie une requête d’E/S, ONTAP note l’adresse IP du client, l’ID de la SVM et la export policy associée au volume cible ou au qtree, et recherche d’abord une entrée correspondante dans le cache d’accès. S’il existe une entrée correspondante dans le cache d’accès, ONTAP utilise les informations stockées pour autoriser ou refuser la demande d’E/S. Si aucune entrée correspondante n’existe, ONTAP passe par le processus normal d’évaluation de toutes les règles de politique applicables, comme expliqué ci-dessus.

Les entrées du cache d’accès qui ne sont pas utilisées activement ne sont pas actualisées. Cela permet de réduire les communications inutiles et inutiles avec des services de noms externes.

La récupération des informations à partir du cache d’accès est bien plus rapide qu’au cours de l’intégralité du processus d’évaluation des règles des règles d’export-policy pour chaque demande d’E/S. Par conséquent, l’utilisation du cache d’accès améliore nettement les performances en réduisant la surcharge liée aux vérifications d’accès client.

Fonctionnement des paramètres de cache d’accès

Plusieurs paramètres contrôlent les périodes d’actualisation des entrées dans le cache d’accès. Le fonctionnement de ces paramètres vous permet de les modifier pour régler le cache d’accès et équilibrer les performances avec la récente information stockée.

Le cache d’accès stocke des entrées composées d’une ou plusieurs règles d’exportation qui s’appliquent aux clients qui essaient d’accéder aux volumes ou aux qtrees. Ces entrées sont stockées pendant un certain temps avant leur actualisation. La durée d’actualisation est déterminée par les paramètres du cache d’accès et dépend du type d’entrée du cache d’accès.

Vous pouvez spécifier les paramètres du cache d’accès pour chaque SVM. Cela permet aux paramètres de différer en fonction des exigences d’accès des SVM. Les entrées de cache d’accès qui ne sont pas utilisées activement ne sont pas réactualisées, ce qui réduit les communications inutiles et inutiles avec le nom externe sert.

Accès au type d’entrée du cache	Description	Période d’actualisation en secondes
Entrées positives	Les entrées du cache d’accès qui n’ont pas entraîné de refus d’accès aux clients.	Minimum: 300 Maximum : 86,400 Valeur par défaut : 3,600
Entrées négatives	Les entrées du cache d’accès qui ont entraîné un refus d’accès aux clients.	Minimum : 60 Maximum : 86,400 Valeur par défaut : 3,600

Exemple

Un client NFS tente d'accéder à un volume sur un cluster. ONTAP mappe le client sur une règle export policy et détermine que le client accède à cette règle en fonction de la configuration de la règle export policy. ONTAP stocke la règle d'export policy dans le cache d'accès sous forme d'entrée positive. Par défaut, ONTAP conserve l'entrée positive dans le cache d'accès pendant une heure (3,600 secondes), puis actualise automatiquement l'entrée pour maintenir les informations à jour.

Pour éviter que le cache d'accès ne se remplit inutilement, il existe un paramètre supplémentaire pour effacer les entrées existantes du cache d'accès qui n'ont pas été utilisées pendant une certaine période pour décider de l'accès client. C'est ça `-harvest-timeout` le paramètre a une plage autorisée de 60 à 2,592,000 secondes et un réglage par défaut de 86,400 secondes.

Supprimer une export policy d'un qtree

Si vous décidez de ne plus vouloir attribuer une export policy spécifique à un qtree, vous pouvez supprimer la export policy en modifiant le qtree de manière à hériter de la export policy du volume contenant. Pour ce faire, utilisez le `volume qtree modify` commande avec `-export-policy` paramètre et chaîne de nom vide ("").

Étapes

1. Pour supprimer une export policy d'un qtree, entrez la commande suivante :

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

2. Vérifier que le qtree a été modifié en conséquence :

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

Valider les ID de qtree pour les opérations sur les fichiers qtree

ONTAP peut procéder à une validation supplémentaire facultative des ID de qtree. Cette validation garantit que les demandes d'opérations de fichiers client utilisent un ID qtree valide et que les clients ne peuvent déplacer que les fichiers au sein du même qtree. Vous pouvez activer ou désactiver cette validation en modifiant le `-validate-qtree -export` paramètre. Ce paramètre est activé par défaut.

Description de la tâche

Ce paramètre n'est efficace que lorsque vous avez attribué une export policy directement à un ou plusieurs qtrees sur la machine virtuelle de stockage (SVM).

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Pour que la validation de l'ID qtree soit…	Saisissez la commande suivante…
Activé	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Désactivé	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Restrictions des export policy et jonctions imbriquées pour volumes FlexVol

Si vous avez configuré des stratégies d'exportation pour définir une stratégie moins restrictive sur une jonction imbriquée mais une règle plus restrictive sur une jonction de niveau supérieur, l'accès à la jonction de niveau inférieur peut échouer.

Vous devez vous assurer que les jonctions de niveau supérieur disposent de règles d'exportation moins restrictives que les jonctions de niveau inférieur.