Sécurisez l'accès SMB à l'aide de règles d'exportation

ONTAP 9

NetApp
April 24, 2024

Sommaire

Sécurisez l’accès SMB à l’aide de règles d’exportation

Mode d’utilisation des export-policy avec les accès SMB

Si les export policy pour accès SMB sont activées sur le serveur SMB, les export policies sont utilisées lors du contrôle de l’accès aux volumes du SVM par les clients SMB. Pour accéder aux données, vous pouvez créer une export policy qui autorise l’accès SMB, puis associer la policy aux volumes contenant des partages SMB.

Une export policy applique une ou plusieurs règles qui lui permettent de spécifier les clients autorisés à accéder aux données et les protocoles d’authentification pris en charge pour l’accès en lecture seule et en lecture/écriture. Vous pouvez configurer des stratégies d’exportation afin d’autoriser l’accès via SMB à tous les clients, à un sous-réseau de clients ou à un client spécifique et autoriser l’authentification à l’aide de l’authentification Kerberos, de l’authentification NTLM ou des deux authentifications Kerberos et NTLM lors de la détermination de l’accès en lecture seule et en lecture/écriture aux données.

Après le traitement de toutes les règles d’exportation appliquées à l’export policy, ONTAP peut déterminer si le client dispose d’un accès et quel niveau d’accès. Les règles d’exportation s’appliquent aux ordinateurs clients et non aux utilisateurs et groupes Windows. Les règles d’exportation ne remplacent pas l’authentification et l’autorisation basées sur les utilisateurs et les groupes Windows. Les règles d’exportation offrent une autre couche de sécurité d’accès en plus des autorisations de partage et d’accès aux fichiers.

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

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

Chaque SVM possède au moins une export policy appelée « default », qui ne contient aucune règle. Vous ne pouvez pas supprimer cette export-policy, mais vous pouvez la renommer ou la modifier. Par défaut, chaque volume du SVM est associé aux export policy par défaut. Si les export policy pour accès SMB sont désactivées sur le SVM, la « default » export policy n’a aucun impact sur l’accès SMB.

Vous pouvez configurer les règles fournissant l’accès aux hôtes NFS et SMB et associer cette règle à une export policy, qui peut ensuite être associée au volume qui contient des données auxquelles les hôtes NFS et SMB ont besoin d’accéder. Alternativement, s’il existe des volumes dans lesquels seuls les clients SMB ont besoin d’accéder, vous pouvez configurer une export policy avec des règles qui autorisent uniquement l’accès à l’aide du protocole SMB et qui utilisent uniquement Kerberos ou NTLM (ou les deux) pour l’authentification en lecture seule et l’accès en écriture. L’export policy est ensuite associée aux volumes pour lesquels seul l’accès SMB est souhaité.

Si les export policy pour SMB sont activées et qu’un client effectue une demande d’accès qui n’est pas autorisée par les export policy applicables, la requête échoue et un message d’autorisation refusée. Si un client ne correspond à aucune règle de l’export policy du volume, l’accès est refusé. Si une export policy est vide, alors tous les accès sont implicitement refusés. Ceci est vrai même si les autorisations de partage et de fichier autorisent autrement l’accès. Cela signifie que vous devez configurer votre export policy de manière à limiter les possibilités suivantes sur les volumes contenant des partages SMB :

- Autoriser l'accès à tous les clients ou au sous-ensemble de clients approprié
- Autoriser l'accès via SMB
- Autoriser un accès en lecture seule et en écriture approprié via l'authentification Kerberos ou NTLM (ou les deux)

Découvrez "configuration et gestion des export-policies".

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.

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.

Exemples de règles d'export-policy qui limitent ou autorisent l'accès à SMB

Les exemples montrent comment créer des règles d'export policy qui limitent ou autorisent l'accès via SMB sur un SVM dont les export policy pour l'accès SMB sont activées.

Les export policy pour accès SMB sont désactivées par défaut. Vous devez configurer des règles d'export policy qui limitent ou autorisent l'accès sur SMB uniquement si vous avez activé les export policy pour l'accès SMB.

Règle d'exportation pour l'accès SMB uniquement

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 » qui dispose de la configuration suivante :

- Nom de la politique: Cifs1

- Numéro d'index : 1
- Correspondance client : correspond uniquement aux clients sur le réseau 192.168.1.0/24
- Protocole : autorise uniquement l'accès SMB
- Accès en lecture seule : aux clients utilisant l'authentification NTLM ou Kerberos
- Accès en lecture/écriture : aux clients utilisant l'authentification Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Règle d'exportation pour les accès SMB et NFS

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 », qui dispose de la configuration suivante :

- Nom de la politique: Cifs1
- Numéro d'index : 2
- Correspondance client : correspond à tous les clients
- Protocole : accès SMB et NFS
- Accès en lecture seule : pour tous les clients
- Accès en lecture/écriture : aux clients utilisant l'authentification Kerberos (NFS et SMB) ou NTLM (SMB)
- Mappage de l'ID utilisateur UNIX 0 (zéro) : mappé à l'ID utilisateur 65534 (qui correspond généralement au nom utilisateur personne)
- L'accès SUID et sgID permet

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

Règle d'exportation pour accès SMB uniquement à l'aide de NTLM

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 » qui dispose de la configuration suivante :

- Nom de la stratégie : ntlm1
- Numéro d'index : 1
- Correspondance client : correspond à tous les clients
- Protocole : autorise uniquement l'accès SMB
- Accès en lecture seule : uniquement aux clients utilisant NTLM
- Accès en lecture/écriture : uniquement aux clients utilisant NTLM

Si vous configurez l'option lecture seule ou l'option lecture/écriture pour l'accès NTLM uniquement, vous devez utiliser des entrées basées sur l'adresse IP dans l'option de correspondance client. Autrement, vous recevez `access denied` erreurs. En effet, ONTAP utilise les noms de service Kerberos (SPN) lors de l'utilisation d'un nom d'hôte pour vérifier les droits d'accès du client. L'authentification NTLM ne prend pas en charge les noms SPN.

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

Activez ou désactivez les export policy pour l'accès SMB

Vous pouvez activer ou désactiver les export policy pour l'accès SMB sur les SVM (Storage Virtual machines). L'utilisation des règles d'exportation pour contrôler l'accès SMB aux ressources est facultative.

Avant de commencer

Les conditions suivantes sont requises pour l'activation des export policy pour SMB :

- Le client doit avoir un enregistrement « PTR » dans DNS avant de créer les règles d'exportation pour ce client.
- Un ensemble supplémentaire d'enregistrements « A » et « PTR » pour les noms d'hôte est nécessaire si la SVM fournit l'accès aux clients NFS et que le nom d'hôte que vous souhaitez utiliser pour l'accès NFS est différent du nom du serveur CIFS.

Description de la tâche

Lors de la configuration d'un nouveau serveur CIFS sur votre SVM, l'utilisation des export policies pour l'accès SMB est désactivée par défaut. Vous pouvez activer des export policy pour l'accès SMB si vous souhaitez contrôler l'accès en fonction du protocole d'authentification, des adresses IP clientes ou des noms d'hôte. Vous pouvez activer ou désactiver des export policy pour l'accès SMB à tout moment.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Activer ou désactiver les export-policies :
   - Activer les export-policies : `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`
   - Désactiver les export-policies : `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled false`
3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant permet d'utiliser les export policy pour contrôler l'accès des clients SMB aux ressources sur le 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 -is-exportpolicy
-enabled true

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