



Sécurisez l'accès aux fichiers à l'aide des ACL de partage SMB

ONTAP 9

NetApp
September 12, 2024

Sommaire

- Sécurisez l'accès aux fichiers à l'aide des ACL de partage SMB 1
 - Directives pour la gestion des ACL de niveau partage SMB 1
 - Créer des listes de contrôle d'accès pour le partage SMB 1
 - Commandes de gestion des listes de contrôle d'accès au partage SMB 4

Sécurisez l'accès aux fichiers à l'aide des ACL de partage SMB

Directives pour la gestion des ACL de niveau partage SMB

Vous pouvez modifier les listes de contrôle d'accès au niveau du partage pour accorder aux utilisateurs plus ou moins de droits d'accès au partage. Vous pouvez configurer les listes de contrôle d'accès au niveau du partage en utilisant soit des utilisateurs et des groupes Windows, soit des utilisateurs et des groupes UNIX.

Après avoir créé un partage, par défaut, la liste de contrôle d'accès au niveau du partage donne un accès en lecture au groupe standard nommé Everyone. L'accès en lecture dans la liste de contrôle d'accès signifie que tous les utilisateurs du domaine et tous les domaines approuvés ont un accès en lecture seule au partage.

Vous pouvez modifier une liste de contrôle d'accès au niveau du partage en utilisant la console MMC (Microsoft Management Console) sur un client Windows ou la ligne de commande ONTAP.

Les directives suivantes s'appliquent lorsque vous utilisez la console MMC :

- Les noms d'utilisateur et de groupe spécifiés doivent être des noms Windows.
- Vous ne pouvez spécifier que des autorisations Windows.

Les consignes suivantes s'appliquent lorsque vous utilisez la ligne de commande ONTAP :

- Les noms d'utilisateur et de groupe spécifiés peuvent être des noms Windows ou UNIX.

Si un type d'utilisateur et de groupe n'est pas spécifié lors de la création ou de la modification des listes de contrôle d'accès, le type par défaut est utilisateurs et groupes Windows.

- Vous ne pouvez spécifier que des autorisations Windows.

Créer des listes de contrôle d'accès pour le partage SMB

La configuration des autorisations de partage en créant des listes de contrôle d'accès (ACL) pour les partages SMB vous permet de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes.

Description de la tâche

Vous pouvez configurer les listes de contrôle d'accès au niveau du partage à l'aide des noms d'utilisateur ou de groupe Windows locaux ou de domaine ou des noms d'utilisateur ou de groupe UNIX.

Avant de créer une nouvelle liste de contrôle d'accès, vous devez supprimer la liste de contrôle d'accès de partage par défaut `Everyone / Full Control`, qui pose un risque pour la sécurité.

En mode Workgroup, le nom de domaine local est le nom du serveur SMB.

Étapes

1. Supprimez la liste de contrôle d'accès du partage par défaut : « `vserver cifs share Access-control delete -vserver vserver_name -share share_name -user-or-group everyone` »

2. Configurer la nouvelle liste de contrôle d'accès :

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un...	Entrez la commande...
Utilisateur Windows	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\user_name -permission access_right</pre>
Groupe Windows	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\group_name -permission access_right</pre>
Utilisateur UNIX	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-user -user-or-group UNIX_user_name -permission access_right</pre>
Groupe UNIX	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-group -user-or-group UNIX_group_name -permission access_right</pre>

3. Vérifiez que la liste de contrôle d'accès appliquée au partage est correcte à l'aide de la `vserver cifs share access-control show` commande.

Exemple

La commande suivante donne Change Autorisations au groupe Windows "sales Team" pour la part "sales" sur le SVM "vs1.example.com":

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

```
cluster1::> vsserver cifs share access-control show -vsserver
vs1.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\Sales Team	windows	Change

La commande suivante donne Read Autorisation au groupe UNIX « ingénierie » pour la part « eng » sur le SVM « vs2.example.com » :

```
cluster1::> vsserver cifs share access-control create -vsserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read
```

```
cluster1::> vsserver cifs share access-control show -vsserver
vs2.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs2.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs2.example.com	eng	engineering	unix-group	Read

Les commandes suivantes fournissent Change L'autorisation au groupe Windows local nommé « Tiger Team » et Full_Control Autorisation à l'utilisateur Windows local nommé "rue Chang" pour le partage "vatavol5" sur le "SVM" "vs1":

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

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

```
cluster1::> vsriver cifs share access-control show -vsriver vs1
```

Vsriver	Share	User/Group	User/Group	Access
Permission	Name	Name	Type	
-----	-----	-----	-----	

vs1	c\$	BUILTIN\Administrators	windows	
Full_Control				
vs1	datavol5	Tiger Team	windows	Change
vs1	datavol5	Sue Chang	windows	Full_Control

Commandes de gestion des listes de contrôle d'accès au partage SMB

Vous devez connaître les commandes de gestion des listes de contrôle d'accès (ACL) SMB, notamment leur création, leur affichage, leur modification et leur suppression.

Les fonctions que vous recherchez...	Utilisez cette commande...
Créer une nouvelle liste de contrôle d'accès	<code>vsriver cifs share access-control create</code>
Afficher les ACL	<code>vsriver cifs share access-control show</code>
Modifier une ACL	<code>vsriver cifs share access-control modify</code>
Supprimer une ACL	<code>vsriver cifs share access-control delete</code>

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.