



Configurer la numérisation à l'accès ONTAP 9

NetApp
April 24, 2024

Sommaire

- Configurer la numérisation à l'accès 1
 - Création d'une règle on-Access 1
 - Activez une stratégie on-Access 3
 - Modifier le profil des opérations-fichiers Vscan pour un partage SMB 4
 - Commandes permettant de gérer les règles d'accès. 4

Configurer la numérisation à l'accès

Création d'une règle on-Access

Une règle On-Access définit l'étendue d'une analyse on-Access. On peut créer une on-Access policy pour un SVM individuel ou pour tous les SVM d'un cluster. Si vous avez créé une on-Access policy pour tous les SVM d'un cluster, vous devez activer la politique sur chaque SVM individuellement.

Description de la tâche

- Vous pouvez spécifier la taille maximale du fichier à numériser, les extensions de fichier et les chemins à inclure dans la numérisation, ainsi que les extensions de fichier et les chemins à exclure de la numérisation.
- Vous pouvez définir le `scan-mandatory` Option désactivée pour spécifier que l'accès aux fichiers est autorisé lorsqu'aucun serveur Vscan n'est disponible pour l'analyse antivirus.
- Par défaut, ONTAP crée une on-Access policy nommée « `default_CIFS` » et l'active pour tous les SVM d'un cluster.
- Tout fichier admissible à l'exclusion de numérisation en fonction du `paths-to-exclude`, `file-ext-to-exclude`, ou `max-file-size` les paramètres ne sont pas pris en compte pour l'acquisition, même si l' `scan-mandatory` l'option est activée. (Cochez cette case "dépannage" pour les problèmes de connectivité liés au `scan-mandatory` option.)
- Par défaut, seuls les volumes en lecture-écriture sont analysés. Vous pouvez spécifier des filtres qui permettent la numérisation de volumes en lecture seule ou qui limitent la numérisation aux fichiers ouverts avec l'accès d'exécution.
- L'analyse antivirus n'est pas effectuée sur un partage SMB pour lequel le paramètre disponible en continu est défini sur Oui.
- Voir la "[Architecture antivirus](#)" Pour plus d'informations sur le profil *Vscan file-Operations*.
- Vous pouvez créer un maximum de dix (10) règles d'accès par SVM. Toutefois, vous ne pouvez activer qu'une seule stratégie d'accès à la fois.
 - Vous pouvez exclure un maximum de cent (100) chemins et extensions de fichiers de l'analyse antivirus dans une stratégie d'accès.
- Quelques recommandations d'exclusion de fichiers :
 - Pensez à exclure les fichiers volumineux (la taille de fichier peut être spécifiée) de l'analyse antivirus car ils peuvent entraîner un temps de réponse lent ou des délais de requête d'analyse pour les utilisateurs CIFS. La taille de fichier par défaut pour l'exclusion est de 2 Go.
 - Pensez à exclure les extensions de fichier telles que `.vhd` et `.tmp` car les fichiers avec ces extensions peuvent ne pas être appropriés pour la numérisation.
 - Pensez à exclure les chemins de fichiers tels que le répertoire de quarantaine ou les chemins dans lesquels seuls les disques durs virtuels ou les bases de données sont stockés.
 - Vérifiez que toutes les exclusions sont spécifiées dans la même stratégie, car une seule stratégie peut être activée à la fois. NetApp recommande vivement de disposer du même ensemble d'exclusions que celui spécifié dans le moteur antivirus.
- Une stratégie d'accès est requise pour un [analyse à la demande](#). Pour éviter la numérisation à l'accès, vous devez définir `-scan-files-with-no-ext` pour faux et `-file-ext-to-exclude` à `*` pour exclure tous les postes.

Étapes

1. Création d'une règle on-Access :

```
vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
-policy-name policy_name -protocol CIFS -max-file-size
max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
-file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
-exclude paths_of_files_to_exclude -scan-mandatory on|off
```

- Spécifier un SVM de données pour une politique définie pour un SVM individuel, un SVM d'administration du cluster pour une politique définie pour tous les SVM d'un cluster.
- Le `-file-ext-to-exclude` le réglage remplace le `-file-ext-to-include` réglage.
- Réglez `-scan-files-with-no-ext` à vrai pour numériser des fichiers sans extensions. La commande suivante crée une on-Access policy nommée Policy1 sur le vs1 SVM :

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include "mp*", "tx*" -file-ext-to-exclude "mp3", "txt" -scan
-files-with-no-ext false -paths-to-exclude "\\vol\\a b\\", "\\vol\\a,b\\"
```

2. Vérifiez que la stratégie on-Access a été créée : `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante affiche les détails de Policy1 règle :

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```

Vserver: vs1
Policy: Policy1
Policy Status: off
Policy Config Owner: vserver
File-Access Protocol: CIFS
Filters: scan-ro-volume
Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
File Paths Not to Scan: \\vol\\a b\\, \\vol\\a,b\\
File Extensions Not to Scan: mp3, txt
File Extensions to Scan: mp*, tx*
Scan Files with No Extension: false
```

Activez une stratégie on-Access

Une règle On-Access définit l'étendue d'une analyse on-Access. Vous devez activer une on-Access policy sur un SVM avant que ses fichiers ne puissent être analysés.

Si vous avez créé une on-Access policy pour tous les SVM d'un cluster, vous devez activer la politique sur chaque SVM individuellement. Vous ne pouvez activer qu'une seule stratégie à la fois sur un SVM.

Étapes

1. Activer une stratégie on-Access :

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name  
policy_name
```

La commande suivante active une on-Access policy nommée Policy1 sur le vs1 SVM :

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy  
-name Policy1
```

2. Vérifiez que la stratégie on-Access est activée :

```
vserver vscan on-access-policy show -instance data_SVM -policy-name  
policy_name
```

Pour obtenir la liste complète des options, consultez la page man de la commande.


La commande suivante affiche les détails de Policy1 règle d'accès :

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy  
-name Policy1  
  
Vserver: vs1  
Policy: Policy1  
Policy Status: on  
Policy Config Owner: vserver  
File-Access Protocol: CIFS  
Filters: scan-ro-volume  
Mandatory Scan: on  
Max File Size Allowed for Scanning: 3GB  
File Paths Not to Scan: \vol\ a b\, \vol\ a,b\  
File Extensions Not to Scan: mp3, txt  
File Extensions to Scan: mp*, tx*  
Scan Files with No Extension: false
```

Modifier le profil des opérations-fichiers Vscan pour un partage SMB

Le profil `_Vscan opérations-fichiers_` pour un partage SMB définit les opérations sur le partage qui peuvent déclencher le scan. Par défaut, le paramètre est défini sur `standard`. Vous pouvez régler le paramètre si nécessaire lors de la création ou de la modification d'un partage SMB.

Voir la ["Architecture antivirus"](#) Pour plus d'informations sur le profil *Vscan file-Operations*.



L'analyse antivirus n'est pas effectuée sur un partage SMB disposant du `continuously-available` paramètre défini sur `Yes`.

Étape

- 1. Modifier la valeur du profil *Vscan file-Operations* pour un partage SMB :

```
vserver cifs share modify -vserver data_SVM -share-name share -path share_path -vscan-fileop-profile no-scan|standard|strict|writes-only
```

Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante remplace le profil des opérations de fichier Vscan pour un partage SMB par `strict`:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name SALES_SHARE -path /sales -vscan-fileop-profile strict
```

Commandes permettant de gérer les règles d'accès

Vous pouvez modifier, désactiver ou supprimer une stratégie On-Access. Vous pouvez afficher un résumé et les détails de la règle.

| Les fonctions que vous recherchez... | Saisissez la commande suivante... |
|--------------------------------------|---|
| Création d'une règle on-Access | <code>vserver vscan on-access-policy create</code> |
| Modifier une stratégie d'accès | <code>vserver vscan on-access-policy modify</code> |
| Activez une stratégie on-Access | <code>vserver vscan on-access-policy enable</code> |
| Désactivez une stratégie on-Access | <code>vserver vscan on-access-policy disable</code> |
| Supprimez une on-Access policy | <code>vserver vscan on-access-policy delete</code> |

| | |
|--|--|
| Afficher un récapitulatif et des détails d'une stratégie d'accès | <code>vserver vscan on-access-policy show</code> |
| Ajouter à la liste des chemins à exclure | <code>vserver vscan on-access-policy paths-to-exclude add</code> |
| Supprimer de la liste des chemins à exclure | <code>vserver vscan on-access-policy paths-to-exclude remove</code> |
| Afficher la liste des chemins à exclure | <code>vserver vscan on-access-policy paths-to-exclude show</code> |
| Ajouter à la liste des extensions de fichier à exclure | <code>vserver vscan on-access-policy file-ext-to-exclude add</code> |
| Supprimer de la liste des extensions de fichier à exclure | <code>vserver vscan on-access-policy file-ext-to-exclude remove</code> |
| Afficher la liste des extensions de fichier à exclure | <code>vserver vscan on-access-policy file-ext-to-exclude show</code> |
| Ajouter à la liste des extensions de fichier à inclure | <code>vserver vscan on-access-policy file-ext-to-include add</code> |
| Supprimer de la liste des extensions de fichier à inclure | <code>vserver vscan on-access-policy file-ext-to-include remove</code> |
| Afficher la liste des extensions de fichier à inclure | <code>vserver vscan on-access-policy file-ext-to-include show</code> |

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

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.