



Configurer les scanner pool

ONTAP 9

NetApp
March 24, 2023

Table des matières

- Configurer les scanner pool 1
 - Présentation de la configuration des scanner pool 1
 - Créer un pool de scanner sur un seul cluster 1
 - Créer des pools de scanner dans les configurations MetroCluster 2
 - Appliquer une politique scanner sur un seul cluster 4
 - Appliquez les politiques de scanner dans les configurations MetroCluster 6
 - Commandes pour la gestion des scanner pool 8

Configurer les scanner pool

Présentation de la configuration des scanner pool

Un scanner pool définit les serveurs Vscan et les utilisateurs privilégiés qui peuvent se connecter aux SVM. Une politique scanner détermine si un pool de scanner est actif.



Si vous utilisez une export policy sur un serveur SMB, il faut ajouter chaque serveur Vscan à la export policy.

Créer un pool de scanner sur un seul cluster

Un scanner pool définit les serveurs Vscan et les utilisateurs privilégiés qui peuvent se connecter aux SVM. On peut créer un pool de scanner pour un SVM individuel ou pour tous les SVM d'un cluster.

Ce dont vous avez besoin

- Les SVM et les serveurs Vscan doivent se trouver dans le même domaine ou dans des domaines de confiance.
- Pour les scanner pool définis pour un SVM individuel, vous devez avoir configuré le ONTAP antivirus Connector avec la LIF de management SVM ou la LIF de données SVM.
- Pour les scanner pool définis pour tous les SVM d'un cluster, vous devez avoir configuré le ONTAP antivirus Connector avec la LIF cluster management.

Description de la tâche

La liste des utilisateurs privilégiés doit inclure le compte d'utilisateur de domaine que le serveur Vscan utilise pour se connecter à la SVM.

Étapes

1. Créer un pool de scanner :

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users
```

- Spécifier un SVM de données pour un pool défini pour un SVM individuel et spécifier un SVM d'administration du cluster pour un pool défini pour tous les SVM d'un cluster.
- Spécifiez une adresse IP ou un FQDN pour chaque nom d'hôte de serveur Vscan.
- Spécifiez le domaine et le nom d'utilisateur pour chaque utilisateur privilégié. Pour obtenir la liste complète des options, consultez la page man de la commande.

La commande suivante crée un pool de scanner nommé SP sur le vs1SVM :

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users cifs\u1,cifs\u2
```

2. Vérifiez que le scanner pool a été créé : `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool`

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

La commande suivante affiche les détails de SP scanner pool :

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                Vserver: vs1
                                Scanner Pool: SP
                                Applied Policy: idle
                                Current Status: off
                                Cluster on Which Policy Is Applied: -
                                Scanner Pool Config Owner: vserver
                                List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
                                List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
                                27.fsct.nb
                                List of Privileged Users: cifs\u1, cifs\u2
```

Vous pouvez également utiliser le `vserver vscan scanner-pool show` Commande pour afficher tous les scanner pool d'un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Créer des pools de scanner dans les configurations MetroCluster

Il faut créer des pools de scanner primaires et secondaires sur chaque cluster dans une configuration MetroCluster, ce qui correspond aux SVM principal et secondaire sur le cluster.

Ce dont vous avez besoin

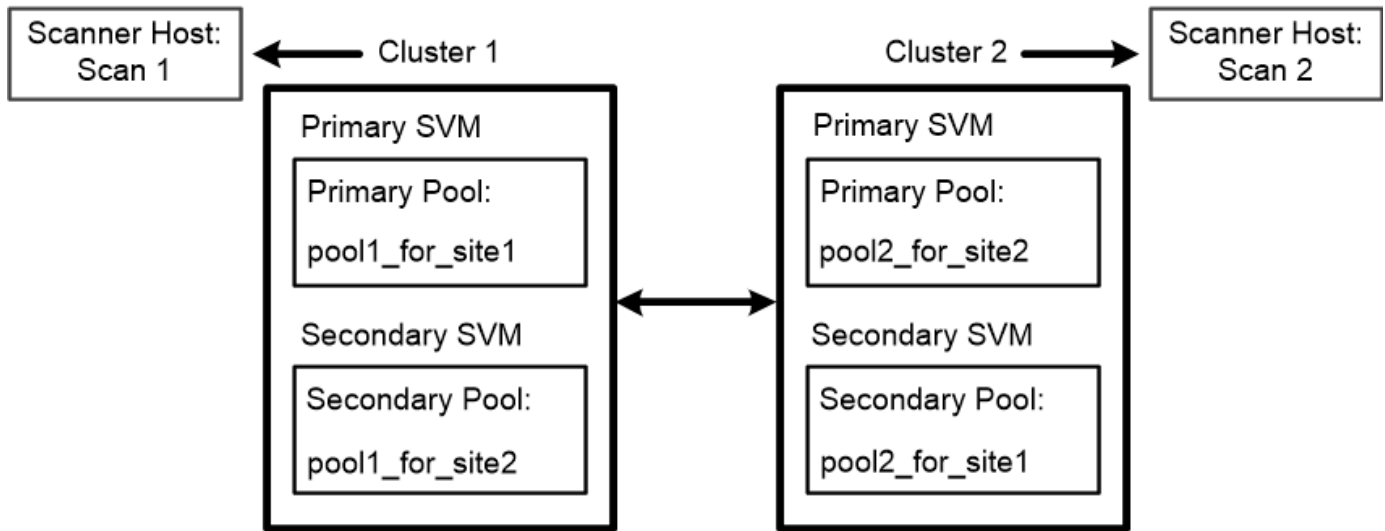
- Les SVM et les serveurs Vscan doivent se trouver dans le même domaine ou dans des domaines de confiance.
- Pour les scanner pool définis pour un SVM individuel, vous devez avoir configuré le ONTAP antivirus Connector avec la LIF de management SVM ou la LIF de données SVM.
- Pour les scanner pool définis pour tous les SVM d'un cluster, vous devez avoir configuré le ONTAP antivirus Connector avec la LIF cluster management.

Description de la tâche

Les configurations MetroCluster protègent les données grâce à la mise en œuvre de deux clusters en miroir séparés physiquement. Chaque cluster réplique de manière synchrone les données et la configuration SVM de l'autre. Un SVM principal sur le cluster local diffuse des données lorsque le cluster est en ligne. Un SVM secondaire situé sur le cluster local transmet des données lorsque le cluster distant est hors ligne.

Cela signifie que vous devez créer des pools de scanner principal et secondaire sur chaque cluster dans une

configuration MetroCluster correspondant aux SVM principal et secondaire sur le cluster. Le pool secondaire devient actif lorsque le cluster commence à transmettre les données du SVM secondaire. L'illustration suivante montre une configuration MetroCluster typique.



La liste des utilisateurs privilégiés doit inclure le compte d'utilisateur de domaine que le serveur Vscan utilise pour se connecter à la SVM.

Étapes

1. Créer un pool de scanner :

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
privileged_users
```

- Spécifier un SVM de données pour un pool défini pour un SVM individuel et spécifier un SVM d'administration du cluster pour un pool défini pour tous les SVM d'un cluster.
- Spécifiez une adresse IP ou un FQDN pour chaque nom d'hôte de serveur Vscan.
- Spécifiez le domaine et le nom d'utilisateur pour chaque utilisateur privilégié.



On doit créer tous les scanner pool depuis le cluster contenant le SVM principal.

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

Les commandes suivantes créent des scanner pool principal et secondaire sur chaque cluster en configuration MetroCluster :

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Vérifiez que les scanner pool ont été créés : `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool`

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

La commande suivante affiche les détails du scanner pool pool1:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1
```

```

                                Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                                Applied Policy: idle
                                Current Status: off
                                Cluster on Which Policy Is Applied: -
                                Scanner Pool Config Owner: vserver
                                List of IPs of Allowed Vscan Servers:
                                List of Host Names of Allowed Vscan Servers: scan1
                                List of Privileged Users: cifs\u1,cifs\u2
```

Vous pouvez également utiliser le `vserver vscan scanner-pool show` Commande pour afficher tous les scanner pool d'un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Appliquer une politique scanner sur un seul cluster

Une politique scanner détermine si un pool de scanner est actif. On doit rendre un pool de scanner actif avant les serveurs Vscan définis dans le pool de scanner peuvent se

connecter à une SVM.

Description de la tâche

- Vous ne pouvez appliquer qu'une seule politique scanner à un pool de scanner.
- Si vous avez créé un pool de scanner pour tous les SVM d'un cluster, vous devez appliquer une scanner policy sur chaque SVM individuellement.
- Pour les configurations MetroCluster et de reprise sur incident, vous devez appliquer une scanner policy aux pools de scanner pour le cluster local et le cluster partenaire.

Dans la règle que vous créez pour le cluster local, vous devez spécifier le cluster local dans le `cluster` paramètre. Dans la règle que vous créez pour le cluster partenaire, vous devez spécifier le cluster partenaire dans le `cluster` paramètre. Le cluster partenaire peut alors reprendre les opérations d'analyse antivirus en cas d'incident.

Étapes

1. Appliquer une politique scanner :

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on
```

Une politique scanner peut avoir l'une des valeurs suivantes :

- `Primary` indique que le pool de scanner est actif.
- `Secondary` Spécifie que le pool de scanner est actif uniquement si aucun des serveurs Vscan du pool de scanner principal n'est connecté.
- `Idle` indique que le pool de scanner est inactif.

L'exemple suivant montre que le pool de scanner est nommé `SP` sur le `vs1` Le SVM est actif :

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP -scanner-policy primary
```

2. Vérifiez que le pool de scanner est actif :

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

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

La commande suivante affiche les détails de `SP` scanner pool :

```

cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                Vserver: vs1
                Scanner Pool: SP
                Applied Policy: primary
                Current Status: on
                Cluster on Which Policy Is Applied: cluster1
                Scanner Pool Config Owner: vserver
                List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
                List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
                27.fsct.nb
                List of Privileged Users: cifs\u1, cifs\u2

```

Vous pouvez utiliser le `vserver vscan scanner-pool show-active` Commande pour afficher les scanner pool actifs sur un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man de la commande.

Appliquez les politiques de scanner dans les configurations MetroCluster

Une politique scanner détermine si un pool de scanner est actif. Vous devez appliquer une scanner policy aux scanner pool principal et secondaire sur chaque cluster dans une configuration MetroCluster.

Description de la tâche

- Vous ne pouvez appliquer qu'une seule politique scanner à un pool de scanner.
- Si vous avez créé un pool de scanner pour tous les SVM d'un cluster, vous devez appliquer une scanner policy sur chaque SVM individuellement.

Étapes

1. Appliquer une politique scanner :

```

vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on

```

Une politique scanner peut avoir l'une des valeurs suivantes :

- `Primary` indique que le pool de scanner est actif.
- `Secondary` Spécifie que le pool de scanner est actif uniquement si aucun des serveurs Vscan du pool de scanner principal n'est connecté.
- `Idle` indique que le pool de scanner est inactif.



Vous devez appliquer toutes les scanner policy à partir du cluster qui contient la SVM principale.

Les commandes suivantes appliquent des scanner policy aux scanner pool principal et secondaire sur chaque cluster de la configuration MetroCluster :

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Vérifiez que le pool de scanner est actif :

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

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

La commande suivante affiche les détails du scanner pool pool1:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                Vserver: cifssvm1
                Scanner Pool: pool1_for_site1
                Applied Policy: primary
                Current Status: on
Cluster on Which Policy Is Applied: cluster1
                Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                List of Privileged Users: cifs\u1,cifs\u2
```

Vous pouvez utiliser le `vserver vscan scanner-pool show-active` Commande pour afficher les scanner pool actifs sur un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Commandes pour la gestion des scanner pool

Vous pouvez modifier et supprimer des pools de scanner et gérer des utilisateurs privilégiés et des serveurs Vscan pour un pool de scanner. Vous pouvez afficher le résumé et les détails d'un pool de scanner.

Les fonctions que vous recherchez...	Saisissez la commande suivante...
Modifier un pool de scanner	<code>vserver vscan scanner-pool modify</code>
Supprimer un pool de scanner	<code>vserver vscan scanner-pool delete</code>
Ajouter des utilisateurs privilégiés à un pool de scanner	<code>vserver vscan scanner-pool privileged-users add</code>
Supprimer des utilisateurs privilégiés d'un pool de scanner	<code>vserver vscan scanner-pool privileged-users remove</code>
Ajout de serveurs Vscan à un pool de scanner	<code>vserver vscan scanner-pool servers add</code>
Supprimer les serveurs Vscan d'un pool de scanner	<code>vserver vscan scanner-pool servers remove</code>
Afficher le résumé et les détails d'un pool de scanner	<code>vserver vscan scanner-pool show</code>
Afficher les utilisateurs privilégiés d'un pool de scanner	<code>vserver vscan scanner-pool privileged-users show</code>
Afficher les serveurs Vscan pour tous les pools de scanner	<code>vserver vscan scanner-pool servers show</code>

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

Informations sur le copyright

Copyright © 2023 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.