Configuration antivirus

ONTAP 9

NetApp
March 24, 2023

Table des matières

Configuration antivirus

Présentation de la configuration antivirus

Vous pouvez utiliser l'analyse antivirus NetApp, appelée *Vscan*, pour protéger vos données contre les virus ou tout autre code malveillant. Il vous montre comment utiliser l'analyse sur accès pour rechercher des virus lorsque les clients accèdent aux fichiers via SMB et comment utiliser l'analyse à la demande pour rechercher des virus immédiatement ou selon un planning.

Vous pouvez utiliser Vscan en utilisant l'interface de ligne de commande de ONTAP, et non System Manager, ni un outil de script automatisé. Vscan n'est pas pris en charge par System Manager.

Informations associées

"Trellix (anciennement McAfee) Endpoint Security Storage protection"

"Rapport technique NetApp 4304 : solution antivirus pour clustered Data ONTAP Symantec"

"Rapport technique NetApp 4312 : solution antivirus pour clustered Data ONTAP Trend micro"

À propos de la protection antivirus NetApp

À propos de l'analyse antivirus NetApp

Vous pouvez utiliser la fonctionnalité antivirus intégrée sur les systèmes de stockage NetApp afin de protéger vos données contre les virus ou tout autre code malveillant. L'analyse antivirus NetApp, appelée *Vscan*, associe le meilleur logiciel antivirus tiers à des fonctionnalités ONTAP, vous offrant ainsi la flexibilité nécessaire pour contrôler quels fichiers sont analysés et à quel moment.

Fonctionnement de l'analyse antivirus

Les systèmes de stockage délèguent des opérations d'analyse à des serveurs externes hébergeant le logiciel antivirus de fournisseurs tiers. Le connecteur antivirus ONTAP, fourni par NetApp et installé sur le serveur externe, gère la communication entre le système de stockage et le logiciel antivirus.

- Vous pouvez utiliser *On-Access scan* pour rechercher des virus lorsque les clients ouvrent, lisent, renomment ou ferment des fichiers sur SMB. L'opération de fichier est suspendue jusqu'à ce que le serveur externe indique l'état de numérisation du fichier. Si le fichier a déjà été numérisé, ONTAP autorise l'opération de fichier. Dans le cas contraire, il demande un scan à partir du serveur.

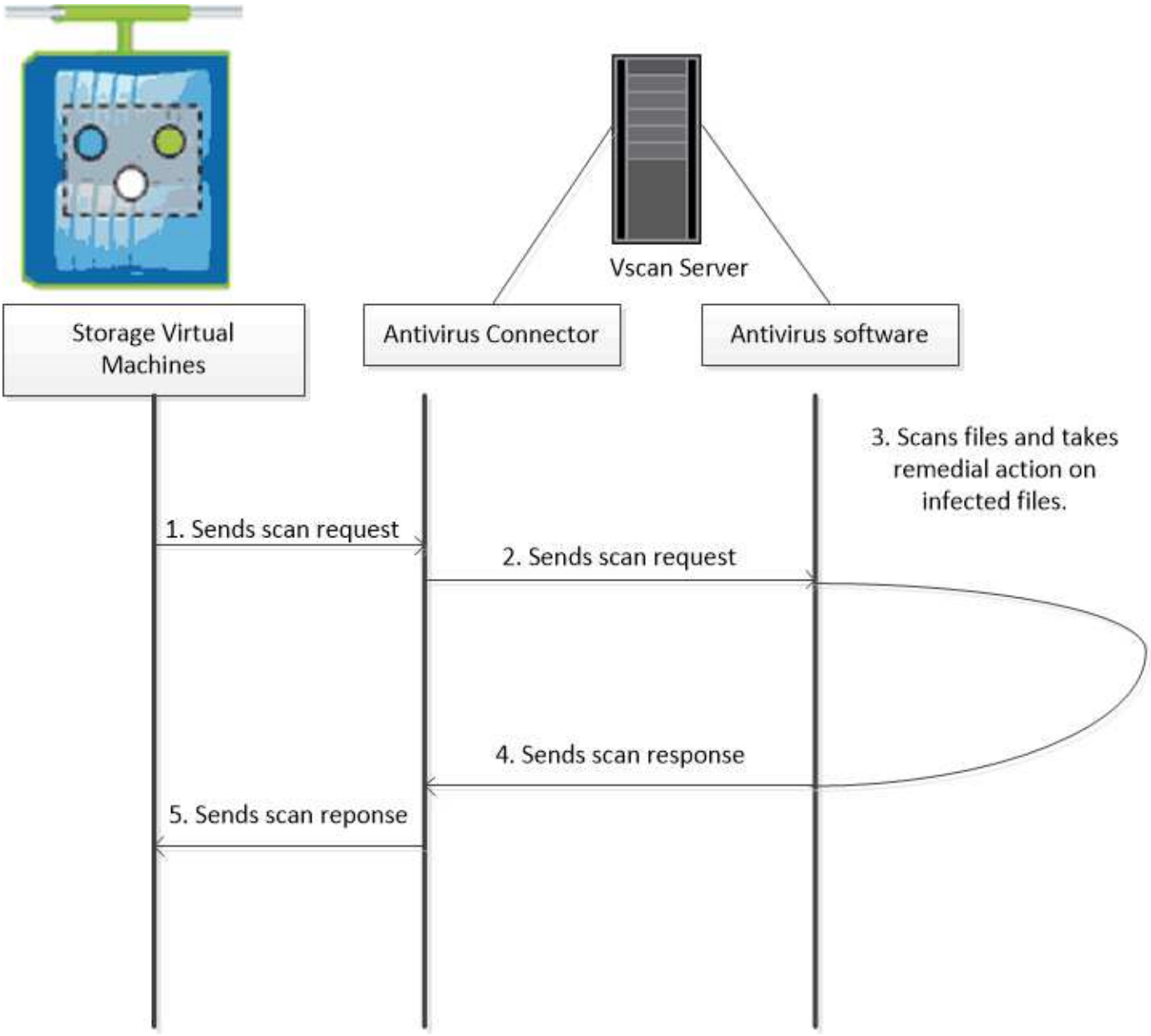
  L'analyse lors de l'accès n'est pas prise en charge par NFS.

- Vous pouvez utiliser *On-Demand scan* pour vérifier immédiatement ou selon un planning les fichiers à la recherche de virus. Il se peut que vous souhaitiez exécuter des analyses uniquement pendant les heures creuses, par exemple. Le serveur externe met à jour l'état d'analyse des fichiers vérifiés, de sorte que la latence d'accès aux fichiers pour ces fichiers (en supposant qu'ils n'ont pas été modifiés) est généralement réduite lorsqu'ils sont ensuite accédés par SMB.

  Vous pouvez utiliser l'analyse à la demande pour n'importe quel chemin du namespace du SVM, même

pour les volumes exportés uniquement via NFS.

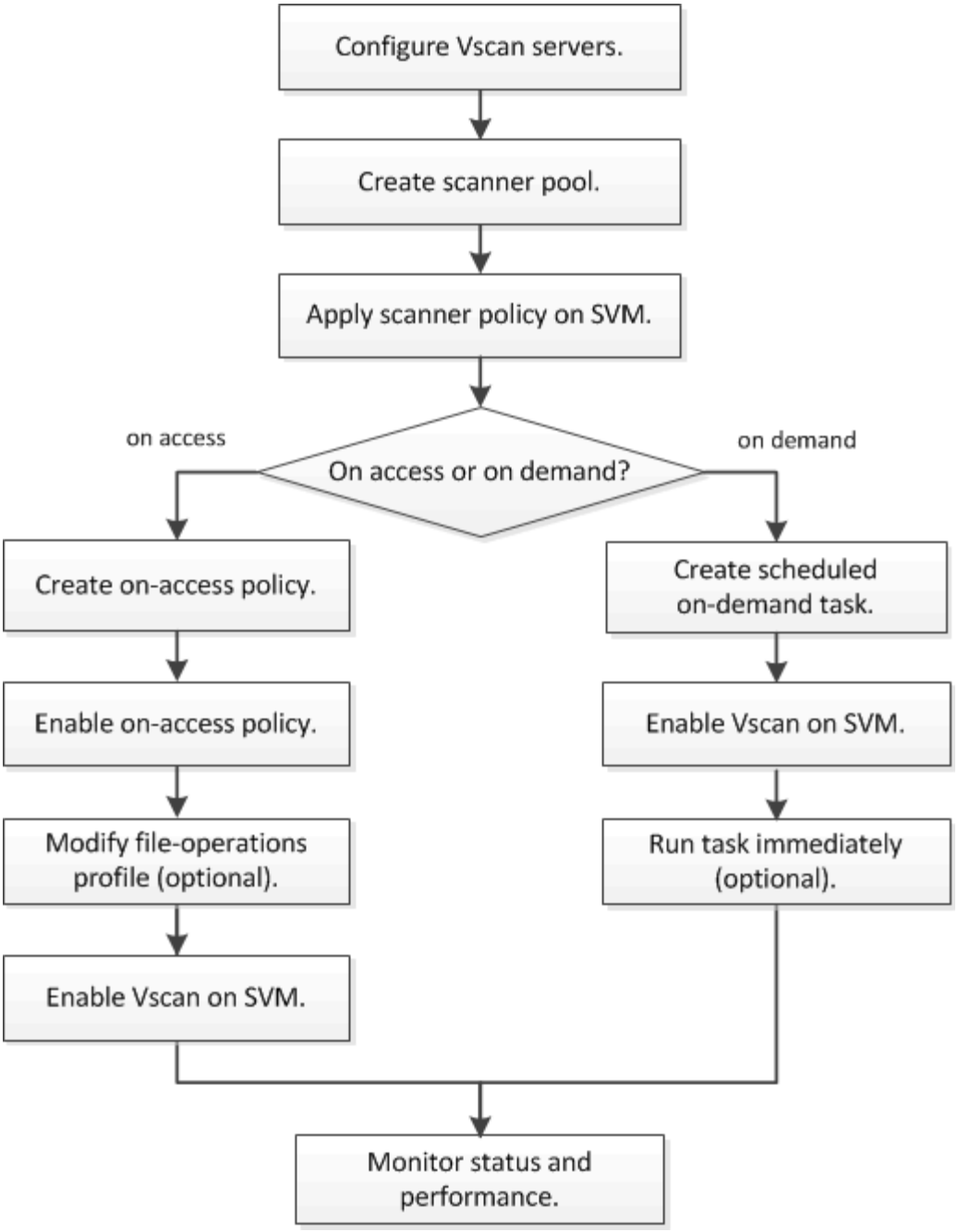
Vous activez généralement les deux modes de scan sur un SVM. Dans les deux modes, le logiciel antivirus prend des mesures correctives sur les fichiers infectés en fonction de vos paramètres dans le logiciel.



Workflow d'analyse de virus

Vous devez créer un pool de scanner et appliquer une politique de scanner avant de pouvoir activer la numérisation. Généralement, il active les analyses à la fois sur accès et à la demande sur un SVM.

Vous devez avoir terminé la configuration CIFS.



Architecture antivirus

L'architecture antivirus NetApp se compose d'un serveur Vscan et d'un ensemble de configurations ONTAP.

Composants du serveur Vscan

Vous devez installer les composants suivants sur le serveur Vscan.

- **ONTAP antivirus Connector**

  Le connecteur antivirus ONTAP fourni par NetApp gère la communication entre ONTAP et le serveur Vscan.

- **Logiciel antivirus**

  Un logiciel antivirus tiers conforme à ONTAP analyse les fichiers à la recherche de virus ou d'autres codes malveillants. Lors de la configuration du logiciel, vous spécifiez les actions correctives à effectuer sur les fichiers infectés.

Configurables ONTAP

Vous devez configurer les éléments suivants sur le système de stockage NetApp.

- **Scanner pool**

  Un scanner pool définit les serveurs Vscan et les utilisateurs privilégiés qui peuvent se connecter aux SVM. Il définit également une période de temporisation de la demande de scan, après laquelle la requête de scan est envoyée à un autre serveur Vscan si un serveur est disponible.

  > Il est recommandé de définir la période de temporisation dans le logiciel antivirus sur le serveur Vscan à cinq secondes que la période d'expiration de la requête scanner-pool, pour éviter les situations dans lesquelles l'accès aux fichiers est retardé ou refusé, car le délai d'expiration du logiciel est supérieur au délai d'attente de la demande de numérisation.

- **Utilisateur privilégié**

  Un utilisateur privilégié est un compte utilisateur de domaine qu'un serveur Vscan utilise pour se connecter à la SVM. Le compte doit figurer dans la liste des utilisateurs privilégiés définis dans le scanner pool.

- **Politique du scanner**

  Une politique scanner détermine si un pool de scanner est actif. 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. Les règles relatives aux scanner sont définies par le système. Vous ne pouvez pas créer de politique scanner personnalisée.

- **Politique sur accès**

  Une règle On-Access définit l'étendue d'une analyse on-Access. Vous pouvez spécifier la taille maximale des fichiers à scanner, les extensions des fichiers à inclure dans le scan, ainsi que les extensions et chemins des fichiers à exclure du scan.

  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 :

  - `scan-ro-volume` permet d'analyser les volumes en lecture seule.
  - `scan-execute-access` limite la numérisation aux fichiers ouverts avec l'accès d'exécution.

« Exécuter l'accès » n'est pas identique à « permission d'exécution ». Un client donné aura « l'accès d'exécution » sur un fichier exécutable uniquement si le fichier a été ouvert avec « l'intention d'exécution ».

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.

- **Tâche à la demande**

  Une tâche à la demande définit la portée d'une analyse à la demande. Vous pouvez spécifier la taille maximale des fichiers à scanner, les extensions et les chemins des fichiers à inclure dans le scan, ainsi que les extensions et chemins des fichiers à exclure du scan. Les fichiers des sous-répertoires sont analysés par défaut.

  Vous utilisez une planification cron pour spécifier quand la tâche s'exécute. Vous pouvez utiliser le `vserver vscan on-demand-task run` commande permettant d'exécuter la tâche immédiatement.

- **Profil d'opérations fichier Vscan (analyse sur accès uniquement)**

  Le `-vscan-fileop-profile` paramètre pour le `vserver cifs share create` Commande définit les opérations qui peuvent déclencher l'analyse antivirus sur un partage SMB. Par défaut, le paramètre est défini sur `standard`, Qui est la meilleure pratique NetApp.

  Vous pouvez régler ce paramètre si nécessaire lorsque vous créez ou modifiez un partage SMB :

  - `no-scan` spécifie que les analyses antivirus ne sont jamais déclenchées pour le partage.
  - `standard` spécifie que les analyses antivirus peuvent être déclenchées par les opérations ouvrir, fermer et renommer.
  - `strict` spécifie que les analyses antivirus peuvent être déclenchées par les opérations ouvrir, lire, fermer et renommer.

    Le `strict` le profil offre une sécurité améliorée dans les situations où plusieurs clients accèdent simultanément à un fichier. Si un client ferme un fichier après avoir écrit un virus, et que le même fichier reste ouvert sur un deuxième client, `strict` assure qu'une opération de lecture sur le second client déclenche une analyse avant la fermeture du fichier.

    Veillez à restreindre le `strict` le profil des partages contenant des fichiers que vous prévoyez sera accessible simultanément. Comme le profil génère plus de demandes de numérisation que les autres, il peut nuire aux performances.

  - `writes-only` spécifie que les analyses de virus ne peuvent être déclenchées que lorsqu'un fichier modifié est fermé.

    Si une application client effectue une opération de renommage, le fichier est fermé avec le nouveau nom et n'est pas analysé. Si de telles opérations posent un problème de sécurité dans votre environnement, vous devez utiliser le `standard` ou `strict` profil.

    Parce que `writes-only` génère moins de demandes de numérisation que les autres profils (sauf `no-scan`), il améliore généralement les performances.

N'oubliez pas, cependant, que si vous utilisez ce profil pour un partage, le scanner doit être configuré pour supprimer ou mettre en quarantaine un fichier infecté non réparable, de sorte qu'il ne puisse plus être

consulté par les clients ultérieurement. Si, par exemple, un client ferme un fichier après l'écriture d'un virus et que le fichier n'est pas réparé, supprimé ou mis en quarantaine, tout client qui accède au fichier *sans* écrire sur celui-ci sera infecté.

Installation et configuration du serveur Vscan

Vous devez configurer un ou plusieurs serveurs Vscan pour que les fichiers de votre système soient analysés. Suivez les instructions fournies par votre fournisseur pour installer et configurer le logiciel antivirus sur le serveur. Suivez les instructions du fichier readme fourni par NetApp pour installer et configurer l'antivirus Connector de ONTAP.

Pour la reprise sur incident et les configurations MetroCluster, il faut configurer des serveurs Vscan séparés pour les clusters locaux et partenaires.

Configuration logicielle requise pour l'antivirus

- Pour plus d'informations sur la configuration requise pour le logiciel antivirus, reportez-vous à la documentation du fournisseur.
- Pour plus d'informations sur les fournisseurs, les logiciels et les versions pris en charge par Vscan, consultez la matrice d'interopérabilité NetApp.

  "mysupport.netapp.com/matrix"

Conditions requises pour ONTAP antivirus Connector

- Vous pouvez télécharger l'antivirus ONTAP Connector à partir de la page de téléchargement des logiciels du site de support NetApp. "Téléchargements NetApp : logiciels"
- Pour plus d'informations sur les versions Windows prises en charge par ONTAP antivirus Connector, consultez la matrice d'interopérabilité NetApp.

  "mysupport.netapp.com/matrix"

  Vous pouvez installer différentes versions de serveurs Windows pour différents serveurs Vscan dans un cluster.

- .NET 3.0 ou version ultérieure doit être installé sur le serveur Windows.
- SMB 2.0 doit être activé sur le serveur Windows.

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 `vs1`SVM :

   ```
   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.

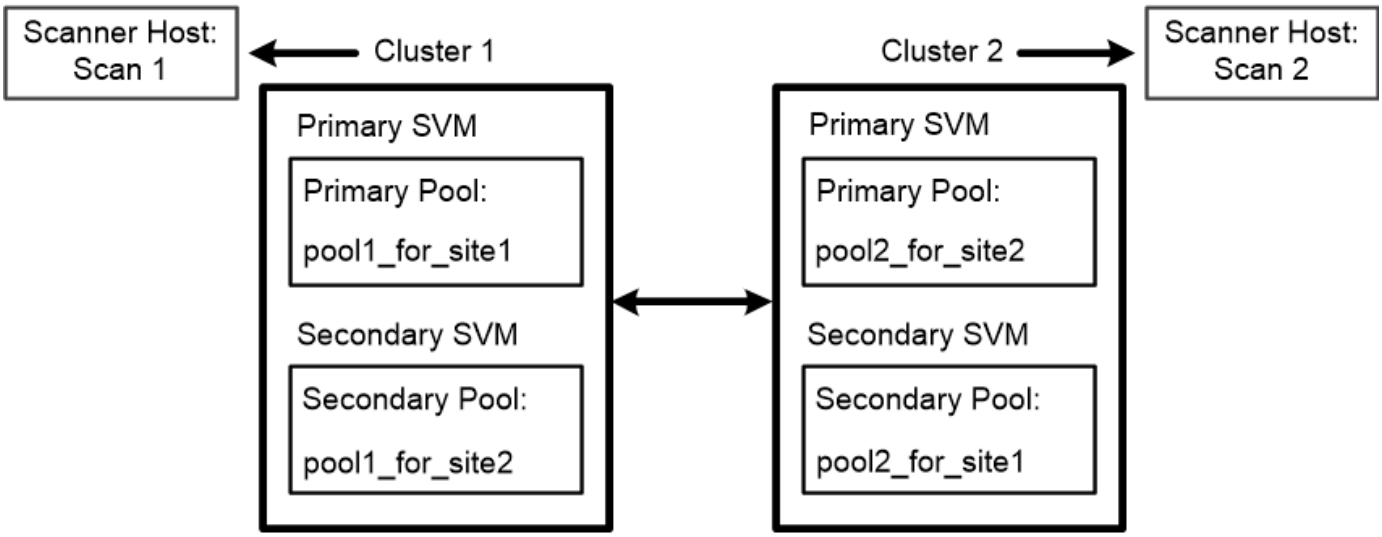
Ce dont vous avez besoin

- 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	`vserver vscan scanner-pool modify`
Supprimer un pool de scanner	`vserver vscan scanner-pool delete`
Ajouter des utilisateurs privilégiés à un pool de scanner	`vserver vscan scanner-pool privileged-users add`
Supprimer des utilisateurs privilégiés d'un pool de scanner	`vserver vscan scanner-pool privileged-users remove`
Ajout de serveurs Vscan à un pool de scanner	`vserver vscan scanner-pool servers add`
Supprimer les serveurs Vscan d'un pool de scanner	`vserver vscan scanner-pool servers remove`
Afficher le résumé et les détails d'un pool de scanner	`vserver vscan scanner-pool show`
Afficher les utilisateurs privilégiés d'un pool de scanner	`vserver vscan scanner-pool privileged-users show`
Afficher les serveurs Vscan pour tous les pools de scanner	`vserver vscan scanner-pool servers show`

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

Configurer la numérisation à l'accès

Création d'une règle on-Access

Une règle On-Access définit l'étendue d'une analyse on-Access. Vous pouvez spécifier la taille maximale des fichiers à scanner, les extensions des fichiers à inclure dans le scan, ainsi que les extensions et chemins des fichiers à exclure du scan. On peut créer une on-Access policy pour un SVM individuel ou pour tous les SVM d'un cluster.

Description de la tâche

Par défaut, ONTAP crée une on-Access policy nommée « default_CIFS » et la permet à tous les SVM d'un cluster.

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. Gardez à l'esprit que tout fichier admissible à l'exclusion de numérisation basée sur le `paths-to-exclude`, `file-ext-to-exclude`, ou

`max-file-size` les paramètres ne sont pas pris en compte pour l'acquisition, même si le `scan-mandatory` l'option est activée.

> Pour les problèmes potentiels liés au `scan-mandatory` option, voir Problèmes de connectivité potentiels impliquant l'option Scan-obligatoire.

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.

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 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 :

```
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

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 des opérations-fichier d'un partage SMB définit les opérations sur le partage qui peuvent déclencher l'analyse. 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.

Description de la tâche

Pour plus d'informations sur les valeurs disponibles pour un profil d'opérations de fichiers Vscan, reportez-vous à la section « profil d'opérations de fichiers Vscan ».

"Profil des opérations de fichiers Vscan (analyse accessible uniquement)"

> L'analyse antivirus n'est pas réalisée sur un partage SMB pour lequel `continuously-available` le paramètre est défini sur `Yes`.

Étape

1. Modifier la valeur du profil des fichiers-opérations Vscan 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 modifie le profil des opérations de fichier Vscan pour un partage SMB à `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…
Modifier une stratégie d'accès	`vserver vscan on-access-policy modify`
Désactivez une stratégie on-Access	`vserver vscan on-access-policy disable`
Supprimez une on-Access policy	`vserver vscan on-access-policy delete`
Afficher un récapitulatif et des détails d'une stratégie d'accès	`vserver vscan on-access-policy show`
Ajouter à la liste des chemins à exclure	`vscan on-access-policy paths-to-exclude add`
Supprimer de la liste des chemins à exclure	`vscan on-access-policy paths-to-exclude remove`
Afficher la liste des chemins à exclure	`vscan on-access-policy paths-to-exclude show`
Ajouter à la liste des extensions de fichier à exclure	`vscan on-access-policy file-ext-to-exclude add`
Supprimer de la liste des extensions de fichier à exclure	`vscan on-access-policy file-ext-to-exclude remove`
Afficher la liste des extensions de fichier à exclure	`vscan on-access-policy file-ext-to-exclude show`
Ajouter à la liste des extensions de fichier à inclure	`vscan on-access-policy file-ext-to-include add`
Supprimer de la liste des extensions de fichier à inclure	`vscan on-access-policy file-ext-to-include remove`
Afficher la liste des extensions de fichier à inclure	`vscan on-access-policy file-ext-to-include show`

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

Configurer l'acquisition à la demande

Configuration de la numérisation à la demande

Vous pouvez utiliser l'analyse à la demande pour rechercher immédiatement ou planifier la présence de virus dans les fichiers. Vous pouvez exécuter des analyses uniquement pendant les heures creuses, par exemple. Vous pouvez également rechercher des fichiers très volumineux exclus de cette analyse lors d'une analyse à l'accès.

Vous pouvez utiliser une planification cron pour spécifier quand la tâche s'exécute :

- Vous pouvez affecter un planning lorsque vous créez une tâche.
- Vous pouvez créer une tâche sans affecter un planning, et utiliser le `vserver vscan on-demand-task schedule` commande permettant d'affecter un planning.
- Vous pouvez utiliser le `vserver vscan on-demand-task run` commande pour exécuter une tâche immédiatement, que vous ayez affecté ou non un planning.

Une seule tâche peut être planifiée à la fois sur un SVM.

La numérisation à la demande ne prend pas en charge la lecture de liens symboliques ou de fichiers de flux.

Créer une tâche à la demande

Une tâche à la demande définit la portée d'une analyse à la demande. Vous pouvez spécifier la taille maximale des fichiers à scanner, les extensions et les chemins des fichiers à inclure dans le scan, ainsi que les extensions et chemins des fichiers à exclure du scan. Les fichiers des sous-répertoires sont analysés par défaut.

Étapes

1. Créer une tâche à la demande :

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude
paths_of_files_to_exclude -file-ext-to-exclude extensions_of_files_to_exclude
-file-ext-to-include extensions_of_files_to_include -scan-files-with-no-ext
true|false -directory-recursion true|false
```

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

     La commande suivante crée une tâche à accès nommée `Task1` sur le `vs1`SVM :

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

> Vous pouvez utiliser le `job show` commande permettant d'afficher l'état du travail. Vous pouvez utiliser le `job pause` et `job resume` commandes permettant d'interrompre et de redémarrer le travail, ou le `job stop` commande pour mettre fin au travail.

2. Vérifiez que la tâche à la demande a été créée : `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

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

   La commande suivante affiche les détails de `Task1` tâche :

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                           Vserver: vs1
                         Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

Une fois que vous avez terminé

Vous devez activer l'analyse sur la SVM avant que la tâche ne soit planifiée.

Planifiez une tâche à la demande

Si vous avez créé une tâche à la demande sans affecter un planning, ou si vous souhaitez attribuer un planning différent à une tâche, vous pouvez utiliser le `vserver vscan on-demand-task schedule` commande permettant d'affecter un planning à la tâche.

Description de la tâche

Planification affectée avec `vserver vscan on-demand-task schedule` la commande remplace un planning déjà affecté par le `vserver vscan on-demand-task create` commande.

Étapes

1. Planifier une tâche à la demande :

   ```
   vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name
   -schedule cron_schedule
   ```

   La commande suivante planifie une tâche à accès nommée `Task2` sur le `vs2`SVM :

   ```
   cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
   -name Task2 -schedule daily
   [Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
   command to view the status.
   ```

   > Vous pouvez utiliser le `job show` commande permettant d'afficher l'état du travail. Vous pouvez utiliser le `job pause` et `job resume` commandes permettant d'interrompre et de redémarrer le travail, ou le `job stop` commande pour mettre fin au travail.

2. Vérifiez que la tâche à la demande a été planifiée : `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

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

   La commande suivante affiche les détails de `Task 2` tâche :

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
```

Une fois que vous avez terminé

Vous devez activer l'analyse sur la SVM avant que la tâche ne soit planifiée.

Exécutez immédiatement une tâche à la demande

Vous pouvez exécuter une tâche à la demande immédiatement, que vous ayez affecté ou non un planning.

Ce dont vous avez besoin

On doit avoir activé l'analyse sur le SVM.

Étape

1. Exécuter une tâche à la demande immédiatement :

   `vserver vscan on-demand-task run -vserver data_SVM -task-name task_name`

   La commande suivante exécute une tâche à accès nommée `Task1` sur le `vs1`SVM :

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

Vous pouvez utiliser le `job show` commande permettant d'afficher l'état du travail. Vous pouvez utiliser le `job pause` et `job resume` commandes permettant d'interrompre et de redémarrer le travail, ou le `job stop` commande pour mettre fin au travail.

Commandes permettant de gérer des tâches à la demande

Vous pouvez modifier, supprimer ou annuler la planification d'une tâche à la demande. Vous pouvez afficher un résumé et des détails de la tâche et gérer les rapports de la tâche.

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Modifier une tâche à la demande	`vserver vscan on-demand-task modify`
Supprimer une tâche à la demande	`vserver vscan on-demand-task delete`
Annulez la planification d'une tâche à la demande	`vserver vscan on-demand-task unschedule`
Consultez le récapitulatif des tâches à la demande et les détails correspondant	`vserver vscan on-demand-task show`
Consultez les rapports à la demande	`vserver vscan on-demand-task report show`
Supprimer des rapports à la demande	`vserver vscan on-demand-task report delete`

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

Activer l'analyse antivirus sur un SVM

Vous devez activer l'analyse antivirus sur un SVM avant de pouvoir exécuter une analyse à la demande ou à l'accès. La configuration Vscan doit exister.

Étapes

1. Activer l'analyse antivirus sur un SVM :

```
vserver vscan enable -vserver data_SVM
```

Vous pouvez utiliser le `vserver vscan disable` commande permettant de désactiver l'analyse antivirus si nécessaire.

La commande suivante active l'analyse antivirus sur le `vs1`SVM :

```
cluster1::> vserver vscan enable -vserver vs1
```

2. Vérifier que l'analyse antivirus est activée sur le SVM :

   `vserver vscan show -vserver data_SVM`

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

   La commande suivante affiche le statut Vscan du `vs1`SVM :

```
cluster1::> vserver vscan show -vserver vs1

                            Vserver: vs1
                        Vscan Status: on
```

Réinitialisez l'état des fichiers numérisés

Il peut arriver que vous souhaitiez réinitialiser l'état d'analyse des fichiers numérisés correctement sur un SVM en utilisant le `vserver vscan reset` commande pour ignorer les informations mises en cache pour les fichiers. Vous pouvez utiliser cette commande pour redémarrer le traitement de l'analyse antivirus en cas de mauvaise configuration d'une analyse, par exemple.

Description de la tâche

Après avoir exécuté le `vserver vscan reset` commande, tous les fichiers admissibles seront numérisés la prochaine fois qu'ils seront consultés.

> Cette commande peut avoir un impact négatif sur les performances, en fonction du nombre et de la taille des fichiers à réanalyser.

Étape

1. Réinitialiser l'état des fichiers numérisés :

   `vserver vscan reset -vserver data_SVM`

   La commande suivante réinitialise l'état des fichiers numérisés sur le `vs1`SVM :

```
cluster1::> vserver vscan reset -vserver vs1
```

Afficher les informations du journal des événements Vscan

Vous pouvez utiliser le `vserver vscan show-events` Commande pour afficher les informations du journal des événements concernant les fichiers infectés, les mises à jour

vers les serveurs Vscan, et le même type. Vous pouvez afficher les informations d'événements pour le cluster ou pour des nœuds, SVM ou serveurs Vscan spécifiques.

Ce dont vous avez besoin

Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Afficher les informations du journal des événements Vscan :

   ```
   vserver vscan show-events
   ```

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

   La commande suivante affiche les informations du journal des événements du cluster `cluster1`:

   ```
   cluster1::*> vserver vscan show-events

   Vserver     Node            Server          Event Type         Event Time
   ----------- --------------- --------------- -----------------
   -----------------
   vs1         Cluster-01      192.168.1.1     file-infected      9/5/2014
   11:37:38
   vs1         Cluster-01      192.168.1.1     scanner-updated    9/5/2014
   11:37:08
   vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
   11:34:55
   3 entries were displayed.
   ```

Résoudre les problèmes de connectivité

Problèmes de connectivité potentiels impliquant l'option Scan-obligatoire

Vous pouvez utiliser le `vserver vscan connection-status show` Commandes pour afficher des informations sur les connexions du serveur Vscan qui vous seront peut-être utiles dans le dépannage des problèmes de connectivité.

Par défaut, le `scan-mandatory` L'option d'analyse On-Access refuse l'accès aux fichiers lorsqu'une connexion au serveur Vscan n'est pas disponible pour l'analyse. Bien que cette option offre des fonctions de sécurité importantes, elle peut entraîner des problèmes dans quelques situations.

- Avant d'activer l'accès client, il faut s'assurer qu'au moins un serveur Vscan est connecté à un SVM sur chaque nœud qui dispose d'une LIF. Si vous devez connecter les serveurs aux SVM après avoir autorisé l'accès client, vous devez désactiver le `scan-mandatory` Option sur le SVM pour s'assurer que l'accès aux fichiers n'est pas refusé car une connexion au serveur Vscan n'est pas disponible. Vous pouvez

réactiver l'option après la connexion du serveur.

- Si une LIF cible héberge toutes les connexions de serveur Vscan pour un SVM, la connexion entre le serveur et la SVM sera perdue si la LIF est migrée. Pour vous assurer que l'accès aux fichiers n'est pas refusé car une connexion au serveur Vscan n'est pas disponible, vous devez désactiver le système `scan-mandatory` Option avant de migrer la LIF. Vous pouvez réactiver l'option après la migration de la LIF.

Chaque SVM doit disposer d'au moins deux serveurs Vscan qui lui sont affectés. Il s'agit d'une meilleure pratique de connexion des serveurs Vscan au système de stockage sur un réseau différent de celui utilisé pour l'accès client.

Commandes pour afficher l'état de connexion du serveur Vscan

Vous pouvez utiliser le `vserver vscan connection-status show` Commandes pour afficher les informations récapitulatives et détaillées sur l'état de la connexion au serveur Vscan.

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Afficher un récapitulatif des connexions du serveur Vscan	`vserver vscan connection-status show`
Afficher les détails des connexions du serveur Vscan	`vserver vscan connection-status show-all`
Afficher les détails des serveurs Vscan connectés	`vserver vscan connection-status show-connected`
Afficher les détails des serveurs Vscan disponibles qui ne sont pas connectés	`vserver vscan connection-status show-not-connected`

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