Protection contre les virus

ONTAP 9

NetApp
April 24, 2024

Sommaire

Protection contre les virus

Présentation de la configuration antivirus

Vscan est une solution d'analyse antivirus développée par NetApp qui permet aux clients de protéger leurs données contre toute compromission par des virus ou d'autres codes malveillants.

Vscan effectue des analyses antivirus lorsque les clients accèdent aux fichiers via SMB. Vous pouvez configurer Vscan pour scanner à la demande ou selon une planification. Vous pouvez interagir avec Vscan en utilisant l'interface de ligne de commande (CLI) ONTAP ou les interfaces de programmation d'applications (API) ONTAP.

Informations associées

"Solutions partenaires Vscan"

À propos de la protection antivirus NetApp

À propos de l'analyse antivirus NetApp

Vscan est une solution d'analyse antivirus développée par NetApp qui permet aux clients de protéger leurs données contre toute compromission par des virus ou d'autres codes malveillants. Il associe un logiciel antivirus fourni par le partenaire aux fonctionnalités de ONTAP pour offrir aux clients la flexibilité dont ils ont besoin pour gérer l'analyse des fichiers.

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.

En fonction du mode d'analyse actif, ONTAP envoie des demandes d'analyse lorsque les clients accèdent aux fichiers via SMB (on-Access) ou accèdent à des fichiers dans des emplacements spécifiques, selon une planification ou immédiatement (on-Demand).

- Vous pouvez utiliser *On-Access scan* pour rechercher des virus lorsque les clients ouvrent, lisent, renomment ou ferment des fichiers sur SMB. Les opérations sur les fichiers sont suspendues jusqu'à ce que le serveur externe indique l'état d'analyse 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.

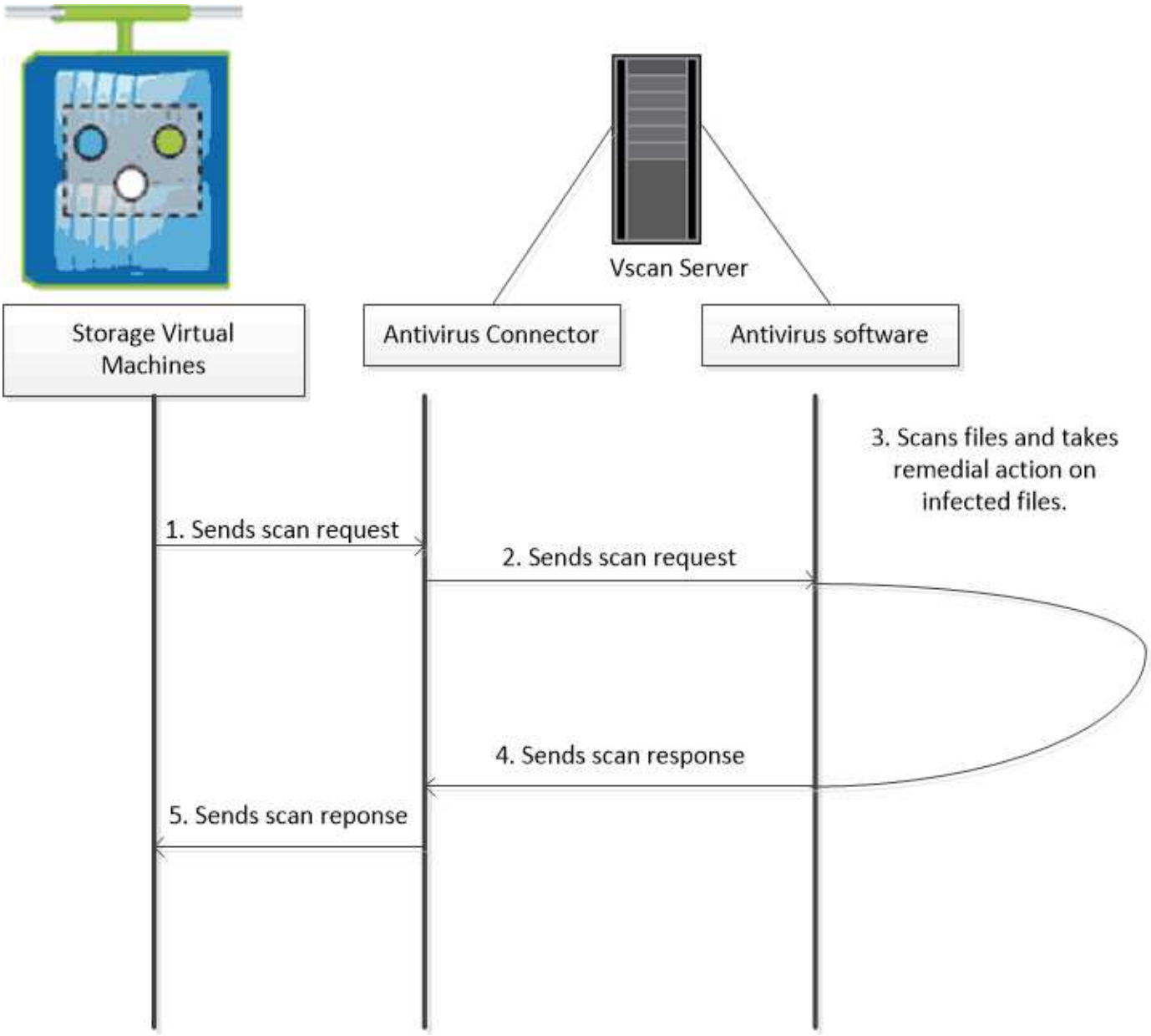
- Vous pouvez utiliser *On-Demand scan* pour vérifier immédiatement ou selon un planning les fichiers à la recherche de virus. Nous recommandons que les analyses à la demande ne s'exécutent qu'en dehors des heures de pointe pour éviter de surcharger l'infrastructure AV existante, qui est normalement dimensionnée pour l'analyse à l'accès. Le serveur externe met à jour l'état d'analyse des fichiers vérifiés afin de réduire la latence d'accès aux fichiers par rapport à SMB. S'il y a eu des modifications de fichier ou des mises à jour de version de logiciel, il demande une nouvelle analyse de fichier à partir du serveur externe.

  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.

Il est généralement possible d'activer les modes d'analyse à la fois on-Access et on-Demand sur une SVM. Dans les deux modes, le logiciel antivirus effectue des actions correctives sur les fichiers infectés en fonction des paramètres de votre logiciel.

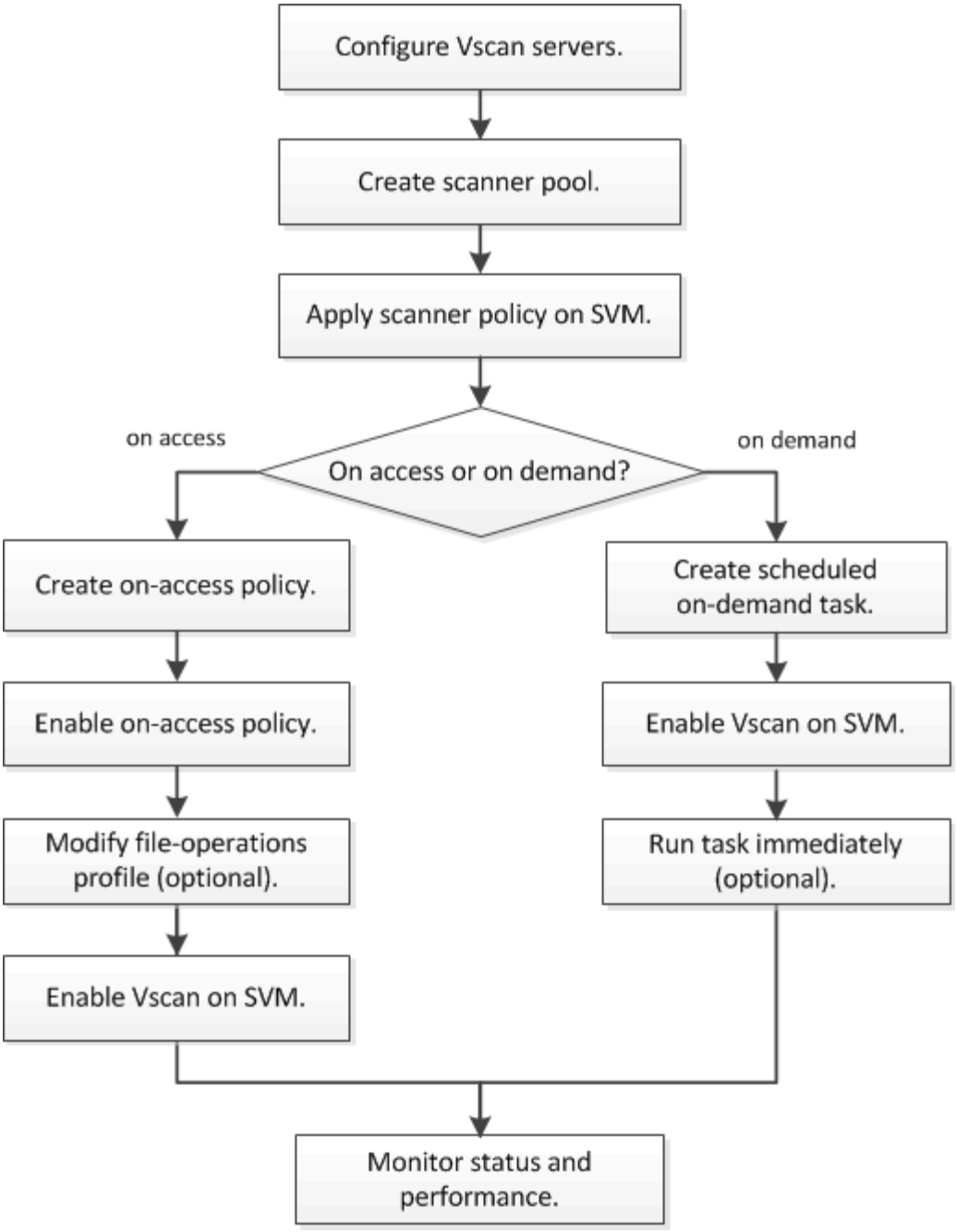
Le connecteur antivirus ONTAP, fourni par NetApp et installé sur le serveur externe, gère la communication entre le système de stockage et le logiciel antivirus.



Workflow d'analyse de virus

Vous devez créer un pool de scanner et appliquer une politique de scanner avant de pouvoir activer la numérisation. Il est généralement possible d'activer les modes d'analyse à la fois on-Access et on-Demand sur une SVM.

Vous devez avoir terminé la configuration CIFS.



Étapes suivantes

- Créer un pool de scanner sur un seul cluster
- Appliquer une politique scanner sur un seul cluster
- Création d'une règle on-Access

Architecture antivirus

L'architecture antivirus NetApp se compose du logiciel du serveur Vscan et des paramètres associés.

Logiciel du serveur Vscan

Vous devez installer ce logiciel sur le serveur Vscan.

- **ONTAP antivirus Connector**

  Il s'agit d'un logiciel fourni par NetApp qui gère les communications de demande et de réponse de scan entre les SVM et le logiciel antivirus. Il peut être exécuté sur une machine virtuelle, mais pour optimiser les performances, il convient d'utiliser une machine physique. Vous pouvez télécharger ce logiciel sur le site du support NetApp (vous devez disposer d'un identifiant).

- **Logiciel antivirus**

  Il s'agit d'un logiciel fourni par un partenaire qui 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.

Paramètres du logiciel Vscan

Vous devez configurer ces paramètres logiciels sur le serveur Vscan.

- **Scanner pool**

  Ce paramètre 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.

  > Vous devez définir la période de temporisation dans le logiciel antivirus sur le serveur Vscan à cinq secondes de moins que le délai d'expiration de la demande de scan-pool. Cela permet d'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'expiration de la demande d'analyse.

- **Utilisateur privilégié**

  Ce paramétrage 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 du scanner pool.

- **Politique du scanner**

  Ce paramètre détermine si un scanner pool est actif. Les règles de scanner sont définies par le système ; vous ne pouvez donc pas créer de règles de scanner personnalisées. Seules les trois règles suivantes sont disponibles :

  - `Primary` indique que le pool de scanner est actif.
  - `Secondary` Précise 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.

- **Politique sur accès**

  Ce paramètre définit la portée d'une analyse à l'accès. 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.

  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 » est différent de « Exécuter l'autorisation ». Un client donné aura « accès à l'exécution » sur un fichier exécutable uniquement si le fichier a été ouvert avec « 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. En mode On-Access, vous pouvez choisir parmi les deux options mutuellement exclusives suivantes :

- Obligatoire : avec cette option, Vscan tente de livrer la demande de scan au serveur jusqu'à expiration du délai. Si la demande d'analyse n'est pas acceptée par le serveur, la demande d'accès client est refusée.
- Non obligatoire : avec cette option, Vscan permet toujours l'accès client, qu'un serveur Vscan soit disponible ou non pour l'analyse antivirus.

- **Tâche à la demande**

Ce paramètre définit l'étendue d'une acquisition à la demande. 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. 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` Définit les opérations de fichier SMB qui déclenchent l'analyse antivirus. Par défaut, le paramètre est défini sur `standard`, Qui est la meilleure pratique de NetApp. Vous pouvez ajuster ce paramètre si nécessaire lors de la création ou de la modification d'un partage SMB :

- `no-scan` spécifie que les analyses antivirus ne sont jamais déclenchées pour le partage.
- `standard` indique que les analyses antivirus sont déclenchées par les opérations ouvrir, fermer et renommer.
- `strict` spécifie que les analyses antivirus sont déclenchées par les opérations d'ouverture, de lecture, de fermeture et de renommage.

  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. Étant donné que ce profil génère davantage de demandes d'analyse, il peut avoir un impact sur les performances.

- `writes-only` spécifie que les analyses de virus ne sont déclenchées que lorsque les fichiers modifiés sont fermés.

Depuis `writes-only` génère moins de demandes d'analyse, ce qui améliore généralement les performances.

Si vous utilisez ce profil, le scanner doit être configuré pour supprimer ou mettre en quarantaine les fichiers infectés irréparables, afin qu'ils ne soient pas accessibles. 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 `without` écrire à elle sera infecté.

> 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.

Solutions partenaires Vscan

NetApp collabore avec Trellix, Symantec, Trend micro et Sentinel One afin de proposer des solutions anti-malware et anti-virus de pointe basées sur la technologie ONTAP Vscan. Ces solutions vous aident à rechercher des programmes malveillants dans les fichiers et à corriger les fichiers affectés.

Comme le montre le tableau ci-dessous, les informations d'interopérabilité pour Trellix, Symantec et Trend micro sont conservées dans la matrice d'interopérabilité NetApp. Les détails sur l'interopérabilité de Trellix et Symantec sont également disponibles sur les sites Web des partenaires. Les informations d'interopérabilité pour Sentinel One et les autres nouveaux partenaires seront conservées par le partenaire sur son site Web.

En tant que partenaire	Documentation de la solution	Détails sur l'interopérabilité
Trellix (anciennement McAfee)	"Documentation produit Trellix"	• "Matrice d'interopérabilité NetApp" • "Plates-formes prises en charge pour la protection du stockage Endpoint Security (trellix.com)"
Symantec	"Symantec protection Engine 9.0.0"	• "Matrice d'interopérabilité NetApp" • "Matrice de prise en charge des périphériques partenaires certifiés avec Symantec protection Engine (SPE) pour le stockage en réseau (NAS) 9.x.x." • "Matrice de prise en charge des périphériques partenaires certifiés avec Symantec protection Engine (SPE) pour le stockage en réseau (NAS) 8.x (broadcom.com)"

En tant que partenaire	Documentation de la solution	Détails sur l'interopérabilité
Trend micro	"Guide de démarrage de Trend micro ServerProtect for Storage 6.0"	"Matrice d'interopérabilité NetApp"
Sentinel One	• "Sécurité des données du cloud de singularité de SentinelOne" • "Assistance SentinelOne" Ce lien requiert une connexion utilisateur. Vous pouvez demander l'accès à Sentinel One.	Instinct profond

Installation et configuration du serveur Vscan

Installation et configuration du serveur Vscan

Configurez un ou plusieurs serveurs Vscan pour vous assurer que les fichiers de votre système sont analysés pour détecter d'éventuels virus. 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 ONTAP antivirus Connector. Vous pouvez également suivre les instructions du "Installez la page ONTAP antivirus Connector".

> Pour les configurations de reprise après incident et MetroCluster, vous devez installer et configurer des serveurs Vscan distincts pour les clusters ONTAP principal/local et secondaire/partenaire.

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, voir le "Solutions partenaires Vscan" page.

Conditions requises pour ONTAP antivirus Connector

- Vous pouvez télécharger ONTAP antivirus Connector à partir de la page **Téléchargement de logiciels** du site de support NetApp. "Téléchargements NetApp : logiciels"
- Pour plus d'informations sur les versions de Windows prises en charge par le connecteur antivirus ONTAP et les conditions d'interopérabilité, voir "Solutions partenaires Vscan".

> 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.

Installez ONTAP antivirus Connector

Installer le ONTAP antivirus Connector sur le serveur Vscan pour permettre la communication entre le système exécutant ONTAP et le serveur Vscan. Une fois ONTAP antivirus Connector installé, le logiciel antivirus peut communiquer avec un ou plusieurs SVM.

Description de la tâche

- Voir la "Solutions partenaires Vscan" Page pour plus d'informations sur les protocoles pris en charge, les versions de logiciels des fournisseurs antivirus, les versions de ONTAP, les conditions d'interopérabilité et les serveurs Windows.
- .NET 4.5.1 ou version ultérieure doit être installé.
- ONTAP antivirus Connector peut s'exécuter sur une machine virtuelle. Toutefois, pour de meilleures performances, NetApp recommande l'utilisation d'une machine virtuelle dédiée à l'analyse antivirus.
- SMB 2.0 doit être activé sur le serveur Windows sur lequel vous installez et exécutez ONTAP antivirus Connector.

Avant de commencer

- Téléchargez le fichier d'installation de ONTAP antivirus Connector à partir du site de support et enregistrez-le dans un répertoire de votre disque dur.
- Vérifiez que vous répondez aux exigences requises pour installer ONTAP antivirus Connector.
- Vérifiez que vous disposez des privilèges d'administrateur pour installer l'antivirus Connector.

Étapes

1. Démarrez l'assistant d'installation de l'antivirus Connector en exécutant le fichier d'installation approprié.
2. Sélectionnez *Suivant*. La boîte de dialogue dossier de destination s'ouvre.
3. Sélectionnez *Next* pour installer l'antivirus Connector dans le dossier qui est répertorié ou sélectionnez *change* pour l'installer dans un autre dossier.
4. La boîte de dialogue informations d'identification du service Windows du connecteur AV ONTAP s'ouvre.
5. Entrez vos informations d'identification de service Windows ou sélectionnez **Ajouter** pour sélectionner un utilisateur. Pour un système ONTAP, cet utilisateur doit être un utilisateur de domaine valide et doit exister dans la configuration scanner pool de la SVM.
6. Sélectionnez **Suivant**. La boîte de dialogue prêt à installer le programme s'ouvre.
7. Sélectionnez **installer** pour commencer l'installation ou sélectionnez **Précédent** si vous souhaitez modifier les paramètres. Une boîte de dialogue d'état s'ouvre et indique la progression de l'installation, suivie de la boîte de dialogue Assistant InstallShield terminé.
8. Cochez la case configurer les LIFs ONTAP si vous souhaitez poursuivre la configuration des LIFs de données ou de gestion ONTAP. Vous devez configurer au moins une LIF de données ou de gestion ONTAP avant d'utiliser ce serveur Vscan.
9. Cochez la case Afficher le journal **Windows installer** si vous souhaitez afficher les journaux d'installation.
10. Sélectionnez **Terminer** pour terminer l'installation et fermer l'assistant InstallShield. L'icône **Configure ONTAP LIFs** est enregistrée sur le bureau pour configurer les LIFs ONTAP.
11. Ajouter un SVM au antivirus Connector. Vous pouvez ajouter un SVM à l'antivirus Connector en ajoutant une LIF de gestion ONTAP, interrogée sur la liste des LIFs de données, ou en configurant directement la LIF de données. Si la LIF de gestion ONTAP est configurée, vous devez également fournir les informations d'interrogation et les informations d'identification du compte admin ONTAP.

- Vérifier que la LIF de management ou l'adresse IP du SVM est Enabled for `management-https`. Cela n'est pas nécessaire lorsque vous configurez uniquement les LIFs de données.
- Vérifiez que vous avez créé un compte d'utilisateur pour l'application HTTP et que vous avez attribué un rôle ayant (au moins en lecture seule) accès au système `/api/network/ip/interfaces` API REST. Pour plus d'informations sur la création d'un utilisateur, reportez-vous à la section "création d'un rôle de connexion de sécurité" et "création d'une connexion de sécurité" Pages de manuel ONTAP.

> Vous pouvez également utiliser l'utilisateur du domaine en tant que compte en ajoutant un SVM de tunnel d'authentification pour une SVM d'administration. Pour plus d'informations, reportez-vous à la section "connexion de sécurité domaine-tunnel créer" ONTAP ou utilisez `/api/security/acccounts` et `/api/security/roles` API REST pour configurer le compte et le rôle admin

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**.
2. Dans la boîte de dialogue Configure ONTAP LIFs, sélectionnez le type de configuration préféré, puis effectuez les actions suivantes :

Pour créer ce type de LIF…	Procédez comme suit…
LIF de données	a. Définissez « rôle » sur « données ». b. Définissez « protocole de données » sur « cifs ». c. Définissez la « politique de pare-feu » sur « données ». d. Définissez « stratégie de service » sur « fichiers-données-par-défaut ».
LIF de management	a. Définir « rôle* sur « données » b. Définissez « protocole de données » sur « aucun ». c. Définissez la « politique de pare-feu » sur « gestion ». d. Définissez « stratégie de service » sur « gestion par défaut ».

En savoir plus sur "Création d'une LIF".

Après avoir créé une LIF, entrer la LIF de données ou de gestion ou l'adresse IP du SVM que vous souhaitez ajouter. Vous pouvez également entrer dans la LIF de cluster management. Si vous spécifiez la LIF de cluster management, tous les SVM au sein de ce cluster qui servent SMB peuvent utiliser le serveur Vscan.

> Lorsque l'authentification Kerberos est requise pour les serveurs Vscan, chaque LIF de données du SVM doit avoir un nom DNS unique, et vous devez enregistrer ce nom en tant que nom principal du serveur (SPN) avec Windows Active Directory. Lorsqu'un nom DNS unique n'est pas disponible pour chaque LIF de données ou enregistré en tant que SPN, le serveur Vscan utilise le mécanisme NT LAN Manager pour l'authentification. Si vous ajoutez ou modifiez les noms DNS et les SPN après la connexion du serveur Vscan, vous devez redémarrer le service antivirus Connector sur le serveur Vscan pour appliquer les modifications.

3. Pour configurer une LIF de gestion, entrez la durée d'interrogation en secondes. La durée de l'interrogation est la fréquence à laquelle l'antivirus Connector recherche des modifications des SVM ou de la configuration LIF du cluster. L'intervalle d'interrogation par défaut est de 60 secondes.
4. Entrez le nom et le mot de passe du compte admin ONTAP pour configurer une LIF de gestion.
5. Cliquez sur **Test** pour vérifier la connectivité et l'authentification. L'authentification est uniquement vérifiée pour une configuration LIF de management.
6. Cliquez sur **mettre à jour** pour ajouter la LIF à la liste des LIFs à interroger ou à se connecter.
7. Cliquez sur **Enregistrer** pour enregistrer la connexion au registre.
8. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers un fichier d'importation de registre ou d'exportation de registre. Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Voir la "Configurez la page ONTAP antivirus Connector" pour les options de configuration.

Configurer ONTAP antivirus Connector

Configurer ONTAP antivirus Connector pour spécifier un ou plusieurs SVM (Storage Virtual machines) auxquels vous souhaitez vous connecter en entrant dans la LIF de gestion ONTAP, en interrotant qu'information et les informations d'identification du compte d'administrateur ONTAP, ou simplement dans la LIF de données. Vous pouvez également modifier les détails d'une connexion SVM ou supprimer une connexion SVM. Par défaut, ONTAP antivirus Connector utilise les API REST pour récupérer la liste des LIFs de données si le LIF de management ONTAP est configuré.

Modifier le détail d'une connexion SVM

Vous pouvez mettre à jour les détails d'une connexion SVM (Storage Virtual machine), qui a été ajoutée à l'antivirus Connector, en modifiant la LIF de gestion ONTAP et les informations d'interrogation. Une fois ajoutées, les LIF de données ne peuvent pas être mises à jour. Pour mettre à jour les LIF de données, vous devez d'abord les supprimer, puis les ajouter de nouveau avec la nouvelle LIF ou adresse IP.

Avant de commencer

Vérifiez que vous avez créé un compte d'utilisateur pour l'application HTTP et que vous avez attribué un rôle ayant (au moins en lecture seule) accès au système `/api/network/ip/interfaces` API REST. Pour plus d'informations sur la création d'un utilisateur, reportez-vous à la section "création d'un rôle de connexion de sécurité" et le "création d'une connexion de sécurité" commandes. Vous pouvez également utiliser l'utilisateur du domaine en tant que compte en ajoutant un SVM de tunnel d'authentification pour une SVM d'administration. Pour plus d'informations, reportez-vous à la section "connexion de sécurité domaine-tunnel créer" Page de manuel ONTAP.

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**. La boîte de dialogue Configure ONTAP LIFs s'ouvre.
2. Sélectionner l'adresse IP du SVM, puis cliquer sur **Update**.
3. Mettez à jour les informations, si nécessaire.
4. Cliquez sur **Enregistrer** pour mettre à jour les détails de la connexion dans le registre.
5. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers une importation de registre ou

un fichier d'exportation de registre. Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Retirer une connexion SVM du connecteur antivirus

Si vous n'avez plus besoin d'une connexion SVM, vous pouvez la supprimer.

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**. La boîte de dialogue Configure ONTAP LIFs s'ouvre.
2. Sélectionner une ou plusieurs adresses IP de SVM, puis cliquer sur **Supprimer**.
3. Cliquez sur **Enregistrer** pour mettre à jour les détails de la connexion dans le registre.
4. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers un fichier d'importation de registre ou d'exportation de registre. Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Résoudre les problèmes

Avant de commencer

Lorsque vous créez des valeurs de registre dans cette procédure, utilisez le volet droit.

Vous pouvez activer ou désactiver les journaux antivirus Connector à des fins de diagnostic. Par défaut, ces journaux sont désactivés. Pour améliorer les performances, vous devez conserver les journaux du connecteur antivirus désactivés et les activer uniquement pour les événements critiques.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, localisez la sous-clé suivante pour ONTAP antivirus Connector : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Créez des valeurs de registre en fournissant le type, le nom et les valeurs indiqués dans le tableau suivant :

Type	Nom	Valeurs
Chaîne	Chemin de traçabilité	c:\avshim.log

   Cette valeur de registre peut être n'importe quel autre chemin valide.

4. Créez une autre valeur de registre en fournissant le type, le nom, les valeurs et les informations de journalisation indiquées dans le tableau suivant :

Type	Nom	Journalisation critique	Journalisation intermédiaire	Journalisation détaillée
DWORD	TRACELEVEL	1	2 ou 3	4

   Cela active les journaux antivirus Connector qui sont enregistrés à la valeur de chemin fournie dans

TracePath à l'étape 3.

5. Désactivez les journaux du connecteur antivirus en supprimant les valeurs de registre que vous avez créées aux étapes 3 et 4.
6. Créez une autre valeur de registre de type "MULTI_SZ" avec le nom "LogRotation" (sans guillemets). Dans « LogRotation », Indiquez « logFileSize:1 » comme entrée pour la taille de rotation (où 1 représente 1 Mo) et dans la ligne suivante, indiquez « logFileCount:5 » comme entrée pour la limite de rotation (5 est la limite).

> Ces valeurs sont facultatives. Si elles ne sont pas fournies, les valeurs par défaut des fichiers 20 Mo et 10 sont utilisées respectivement pour la taille de rotation et la limite de rotation. Les valeurs entières fournies ne fournissent pas de valeurs décimales ou de fraction. Si vous indiquez des valeurs supérieures aux valeurs par défaut, les valeurs par défaut sont utilisées à la place.

7. Pour désactiver la rotation du journal configurée par l'utilisateur, supprimez les valeurs de registre que vous avez créées à l'étape 6.

Bannière personnalisable

Une bannière personnalisée vous permet de placer une déclaration juridiquement contraignante et une clause de non-responsabilité d'accès au système dans la fenêtre *Configure ONTAP LIF API*.

Étape

1. Modifiez la bannière par défaut en mettant à jour le contenu de l' `banner.txt` dans le répertoire d'installation, puis en enregistrant les modifications. Vous devez rouvrir la fenêtre configurer l'API LIF ONTAP pour voir les modifications reflétées dans la bannière.

Activer le mode Eo (Extended Ordinance)

Vous pouvez activer et désactiver le mode Extended Ordinance (EO) pour un fonctionnement sécurisé.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, localisez la sous-clé suivante pour ONTAP antivirus Connector : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Dans le volet de droite, créez une nouvelle valeur de registre de type "DWORD" avec le nom "EO_mode" (sans guillemets) et la valeur "1" (sans guillemets) pour activer le mode EO ou la valeur "0" (sans guillemets) pour désactiver le mode EO.

> Par défaut, si l' `EO_Mode` L'entrée de registre est absente, le mode EO est désactivé. Lorsque vous activez le mode EO, vous devez configurer à la fois le serveur syslog externe et l'authentification mutuelle des certificats.

Configurez le serveur syslog externe

Avant de commencer

Notez que lorsque vous créez des valeurs de registre dans cette procédure, utilisez le volet de droite.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, créez la sous-clé suivante pour ONTAP antivirus Connector pour la configuration syslog : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Créez une valeur de registre en fournissant le type, le nom et la valeur, comme indiqué dans le tableau suivant :

Type	Nom	Valeur
DWORD	syslog_enabled	1 ou 0

   Veuillez noter qu'une valeur « 1 » active le syslog et qu'une valeur « 0 » le désactive.

4. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Hôte_syslog

   Indiquez l'adresse IP ou le nom de domaine de l'hôte syslog pour le champ valeur.

5. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Syslog_port

   Indiquez le numéro de port sur lequel le serveur syslog s'exécute dans le champ valeur.

6. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Protocole_syslog

   Saisissez le protocole utilisé sur le serveur syslog, soit « tcp », soit « udp », dans le champ valeur.

7. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom	JOURNAL_CRIT	LOG_NOTICE	INFO_JOURNAL	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom	Valeur

DWORD	syslog_tls	1 ou 0

Notez qu'une valeur « 1 » active syslog avec TLS (transport Layer Security) et une valeur « 0 » désactive syslog avec TLS.

Assurez-vous qu'un serveur syslog externe configuré fonctionne correctement

- Si la clé est absente ou a une valeur nulle :
  - Le protocole par défaut est « tcp ».
  - Le port par défaut est "514" pour "tcp/udp" et par défaut "6514" pour TLS.
  - Par défaut, le niveau syslog est 5 (LOG_NOTICE).
- Vous pouvez confirmer que syslog est activé en vérifiant que le système `syslog_enabled` la valeur est « 1 ». Lorsque le `syslog_enabled` La valeur est "1", vous devriez pouvoir vous connecter au serveur distant configuré, que le mode EO soit activé ou non.
- Si le mode EO est réglé sur « 1 » et que vous modifiez le `syslog_enabled` valeur comprise entre « 1 » et « 0 », ce qui suit s'applique :
  - Vous ne pouvez pas démarrer le service si syslog n'est pas activé en mode EO.
  - Si le système fonctionne dans un état stable, un avertissement s'affiche indiquant que syslog ne peut pas être désactivé en mode EO et que syslog est fermement défini sur « 1 », que vous pouvez voir dans le registre. Si cela se produit, vous devez d'abord désactiver le mode EO, puis désactiver syslog.
- Si le serveur syslog ne peut pas fonctionner correctement lorsque le mode EO et syslog sont activés, le service s'arrête. Ceci peut se produire pour l'une des raisons suivantes :
  - Un hôte syslog_non valide ou non configuré.
  - Un protocole non valide, hormis UDP ou TCP, est configuré.
  - Un numéro de port n'est pas valide.
- Dans le cas d'une configuration TCP ou TLS sur TCP, si le serveur n'écoute pas le port IP, la connexion échoue et le service s'arrête.

Configurer l'authentification de certificat mutuel X.509

L'authentification mutuelle basée sur certificat X.509 est possible pour la communication SSL (Secure Sockets Layer) entre l'antivirus Connector et ONTAP dans le chemin de gestion. Si le mode EO est activé et que le certificat n'est pas trouvé, le connecteur AV se termine. Effectuez la procédure suivante sur l'antivirus Connector :

Étapes

1. Le connecteur antivirus recherche le certificat client du connecteur antivirus et le certificat de l'autorité de certification du serveur NetApp dans le chemin d'accès au répertoire à partir duquel le connecteur antivirus exécute le répertoire d'installation. Copiez les certificats dans ce chemin de répertoire fixe.
2. Intégrez le certificat client et sa clé privée au format PKCS12 et nommez-le « AV_client.P12 ».
3. Assurez-vous que le certificat de l'autorité de certification (ainsi que toute autorité de signature intermédiaire jusqu'à l'autorité de certification racine) utilisé pour signer le certificat du serveur NetApp est au format PEM (Privacy Enhanced Mail) et nommé ONTAP_CA.pem. Placez-le dans le répertoire d'installation de l'antivirus Connector. Sur le système NetApp ONTAP, installez le certificat de l'autorité de certification (ainsi que toute autorité de signature intermédiaire jusqu'à l'autorité de certification racine) utilisé pour signer le certificat client pour le connecteur antivirus à « ONTAP » en tant que certificat de type

« client-ca ».

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, vous devez 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 ONTAP antivirus Connector avec la LIF de management du SVM ou la LIF de donnée du SVM.
- Pour les scanner-pool définis pour tous les SVM d'un cluster, vous devez avoir configuré ONTAP antivirus Connector avec la LIF cluster management.
- La liste des utilisateurs privilégiés doit inclure le compte d'utilisateur de domaine que le serveur Vscan utilise pour se connecter à la SVM.
- Une fois le scanner pool configuré, vérifiez l'état de la connexion aux serveurs.

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 ONTAP antivirus Connector avec la LIF de management du SVM ou la LIF de donnée du SVM.
- Pour les scanner-pool définis pour tous les SVM d'un cluster, vous devez avoir configuré ONTAP antivirus Connector avec la LIF cluster management.
- La liste des utilisateurs privilégiés doit inclure le compte d'utilisateur de domaine que le serveur Vscan

utilise pour se connecter à la SVM.

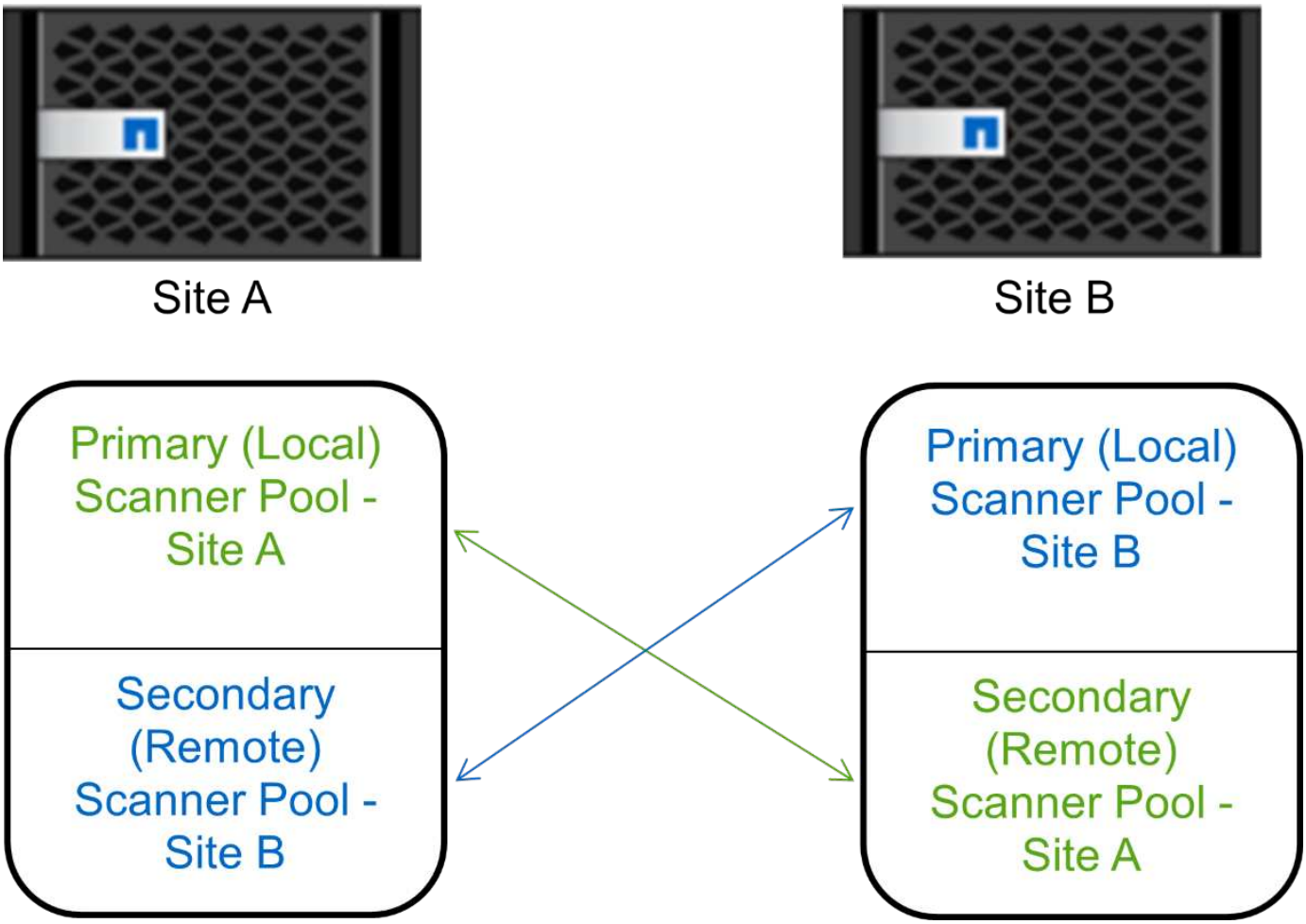
- Une fois le scanner pool configuré, vérifiez l'état de la connexion aux serveurs.

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 scanner pools principal et secondaire sur chaque cluster d'une configuration MetroCluster. Le pool secondaire devient actif lorsque le cluster commence à transmettre des données depuis le SVM secondaire. Pour la reprise sur incident, la configuration est similaire à celle de MetroCluster.

Cette figure présente une configuration MetroCluster/DR classique.



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 activer un scanner pool avant que les serveurs Vscan qu'il définit puissent 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.

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.
- Pour les configurations MetroCluster et de reprise après incident, vous devez appliquer une stratégie scanner à chaque pool de scanner du cluster local et distant.
- Dans la règle que vous créez pour le cluster local, vous devez spécifier le cluster local dans le `cluster` paramètre. Dans la stratégie que vous créez pour le cluster distant, vous devez spécifier le cluster distant dans `cluster` paramètre. Le cluster distant peut alors prendre le contrôle des 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.

> 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 également afficher des informations récapitulatives sur le 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. 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	`vserver vscan on-access-policy create`
Modifier une stratégie d'accès	`vserver vscan on-access-policy modify`
Activez une stratégie on-Access	`vserver vscan on-access-policy enable`
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	`vserver vscan on-access-policy paths-to-exclude add`
Supprimer de la liste des chemins à exclure	`vserver vscan on-access-policy paths-to-exclude remove`
Afficher la liste des chemins à exclure	`vserver vscan on-access-policy paths-to-exclude show`
Ajouter à la liste des extensions de fichier à exclure	`vserver vscan on-access-policy file-ext-to-exclude add`
Supprimer de la liste des extensions de fichier à exclure	`vserver vscan on-access-policy file-ext-to-exclude remove`
Afficher la liste des extensions de fichier à exclure	`vserver vscan on-access-policy file-ext-to-exclude show`
Ajouter à la liste des extensions de fichier à inclure	`vserver vscan on-access-policy file-ext-to-include add`
Supprimer de la liste des extensions de fichier à inclure	`vserver vscan on-access-policy file-ext-to-include remove`

Afficher la liste des extensions de fichier à inclure	`vserver 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.

À propos de cette rubrique

- Vous pouvez affecter un planning lorsque vous créez une tâche.
- 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.

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

> Pour créer une tâche à la demande, au moins une stratégie d'accès doit être activée. Il peut s'agir de la stratégie par défaut ou d'une stratégie d'accès créée par l'utilisateur.

Créer une tâche à la demande

Une tâche à la demande définit la portée de l'analyse antivirus 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.

Description de la tâche

- Dix (10) tâches à la demande au maximum peuvent être effectuées pour chaque SVM, mais une seule peut être active.
- Une tâche à la demande crée un rapport, qui contient des informations sur les statistiques relatives aux analyses. Ce rapport est accessible à l'aide d'une commande ou en téléchargeant le fichier de rapport créé par la tâche à l'emplacement défini.

Avant de commencer

- Vous devez avoir création d'une stratégie d'accès. La stratégie peut être créée par défaut ou par l'utilisateur. Sans la stratégie On-Access, vous ne pouvez pas activer la numérisation.

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`* `-file-ext-to -exclude` *`file_extensions`* `-file-ext-to-include` *`file_extensions`* `-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, reportez-vous au "référence de commande".

     La commande suivante crée une tâche à la demande nommée `Task1` Sur la `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

Vous pouvez créer une tâche sans affecter de planification et utiliser le `vserver vscan on-demand-task schedule` pour attribuer un planning ou pour ajouter un planning lors de la création de 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.
```

Pour afficher l'état du travail, utilisez le `job show` commande. Le `job pause` et `job resume` les commandes, respectivement, permettent de suspendre et de redémarrer le travail ; le `job stop` la commande met 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.

Avant de commencer

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…
Créer une tâche à la demande	`vserver vscan on-demand-task create`
Modifier une tâche à la demande	`vserver vscan on-demand-task modify`
Supprimer une tâche à la demande	`vserver vscan on-demand-task delete`
Exécutez une tâche à la demande	`vserver vscan on-demand-task run`
Planifiez une tâche à la demande	`vserver vscan on-demand-task schedule`
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.

Bonnes pratiques de configuration de la fonctionnalité antivirus externe dans ONTAP

Envisagez les recommandations suivantes pour la configuration de la fonctionnalité externe dans ONTAP.

- Limiter les utilisateurs privilégiés aux opérations d'analyse antivirus. Les utilisateurs normaux doivent être déconseillés d'utiliser des informations d'identification d'utilisateur privilégiées. Cette restriction peut être obtenue en désactivant les droits de connexion pour les utilisateurs privilégiés sur Active Directory.
- Les utilisateurs privilégiés ne sont pas tenus de faire partie d'un groupe d'utilisateurs disposant d'un grand nombre de droits dans le domaine, tels que le groupe d'administrateurs ou le groupe d'opérateurs de sauvegarde. Les utilisateurs privilégiés doivent être validés uniquement par le système de stockage de sorte qu'ils soient autorisés à créer des connexions au serveur Vscan et à accéder aux fichiers pour l'analyse antivirus.
- Utiliser les ordinateurs exécutant des serveurs Vscan uniquement à des fins d'analyse antivirus. Pour décourager l'utilisation générale, désactivez les services de terminal Windows et les autres dispositions d'accès à distance sur ces ordinateurs et accordez le droit d'installer de nouveaux logiciels sur ces ordinateurs uniquement aux administrateurs.
- Dédiez les serveurs Vscan à l'analyse antivirus et ne les utilisez pas pour d'autres opérations, telles que les sauvegardes. Vous pouvez décider d'exécuter le serveur Vscan en tant que machine virtuelle (VM). Si vous exécutez le serveur Vscan en tant que VM, assurez-vous que les ressources allouées à la VM ne sont pas partagées et suffisantes pour effectuer une analyse antivirus.
- Fournir le CPU, la mémoire et la capacité disque appropriés au serveur Vscan pour éviter toute sur-allocation des ressources La plupart des serveurs Vscan sont conçus pour utiliser plusieurs serveurs CPU core et pour répartir la charge entre les CPU.
- NetApp recommande d'utiliser un réseau dédié avec un VLAN privé pour la connexion de la SVM au serveur Vscan de sorte que le trafic de scan n'est pas affecté par d'autres trafic réseau client. Créer une carte d'interface réseau (NIC) distincte dédiée au VLAN antivirus sur le serveur Vscan et à la LIF de données sur la SVM Cette étape simplifie l'administration et le dépannage en cas de problèmes réseau. Le trafic antivirus doit être isolé à l'aide d'un réseau privé. Le serveur antivirus doit être configuré pour communiquer avec le contrôleur de domaine (DC) et ONTAP de l'une des manières suivantes :
  - Le DC doit communiquer avec les serveurs antivirus via le réseau privé utilisé pour isoler le trafic.
  - Le serveur DC et antivirus doivent communiquer via un autre réseau (pas le réseau privé mentionné précédemment), qui n'est pas le même que le réseau client CIFS.
  - Pour activer l'authentification Kerberos pour la communication antivirus, créez une entrée DNS pour les LIFs privées et un nom principal de service sur le DC correspondant à l'entrée DNS créée pour la LIF privée. Utiliser ce nom lors de l'ajout d'une LIF au antivirus Connector. Le DNS doit pouvoir renvoyer un nom unique pour chaque LIF privée connectée au connecteur antivirus.

> Si la LIF du trafic Vscan est configurée sur un port différent de la LIF pour le trafic client, la LIF Vscan peut basculer vers un autre nœud en cas de défaillance de port. La modification rend le serveur Vscan inaccessible depuis le nouveau nœud et les notifications de scan pour les opérations de fichier sur le nœud échouent. Vérifier que le serveur Vscan est accessible via au moins une LIF sur un nœud de sorte qu'il puisse traiter les demandes de scan pour les opérations de fichier effectuées sur ce nœud.

- Connecter le système de stockage NetApp et le serveur Vscan en utilisant au moins un réseau 1GbE.
- Pour un environnement avec plusieurs serveurs Vscan, connectez tous les serveurs qui ont des connexions réseau hautes performances similaires. La connexion des serveurs Vscan améliore les performances en permettant le partage de charge.
- Pour les sites distants et les succursales, NetApp recommande d'utiliser un serveur Vscan local plutôt qu'un serveur Vscan distant, car le premier est le candidat idéal à une latence élevée. Si le coût est un facteur, utilisez un ordinateur portable ou un PC pour une protection antivirus modérée. Vous pouvez planifier des analyses complètes périodiques du système de fichiers en partageant les volumes ou les qtrees et en les analysant à partir de n'importe quel système du site distant.
- Utiliser plusieurs serveurs Vscan pour scanner les données sur la SVM à des fins d'équilibrage de charge et de redondance La quantité de charge de travail CIFS et le trafic antivirus résultant varient selon les SVM. Surveillez la latence CIFS et l'analyse antivirus sur le contrôleur de stockage. Surveiller la tendance des résultats au fil du temps. Si la latence CIFS et la latence de l'analyse antivirus augmentent en raison des files d'attente des processeurs ou des applications sur les serveurs Vscan, les clients CIFS peuvent rencontrer de longs délais d'attente. Ajouter des serveurs Vscan supplémentaires pour distribuer la charge.
- Installez la dernière version de ONTAP antivirus Connector.
- Maintenez les moteurs antivirus et les définitions à jour. Consultez vos partenaires pour obtenir des recommandations sur la fréquence de mise à jour.
- Dans un environnement multi-tanancy, un pool de scanner (pool de serveurs Vscan) peut être partagé avec plusieurs SVM à condition que les serveurs Vscan et les SVM fassent partie du même domaine ou du même domaine de confiance.
- La stratégie de logiciel antivirus pour les fichiers infectés doit être définie sur « delete » ou « quarantine », qui est la valeur par défaut définie par la plupart des fournisseurs d'antivirus. Si le « vscan-fileop-profile » est défini sur « write_only » et si un fichier infecté est trouvé, le fichier reste dans le partage et peut être ouvert car l'ouverture d'un fichier ne déclenche pas de scan. Le scan antivirus est déclenché uniquement après la fermeture du fichier.
- Le `scan-engine timeout` la valeur doit être inférieure à `scanner-pool request-timeout` valeur. Si la valeur est supérieure, l'accès aux fichiers peut être retardé et peut éventuellement prendre du temps. Pour éviter cela, configurez le `scan-engine timeout` à 5 secondes de moins que le `scanner-pool request-timeout` valeur. Reportez-vous à la documentation du fournisseur du moteur de numérisation pour obtenir des instructions sur la façon de modifier le `scan-engine timeout` paramètres. Le `scanner-pool timeout` peut être modifié à l'aide de la commande suivante en mode avancé et en fournissant la valeur appropriée pour `request-timeout` paramètre : `vserver vscan scanner-pool modify`.
- Pour un environnement dimensionné pour les charges de travail d'analyse à l'accès et nécessitant l'analyse à la demande, NetApp recommande de planifier la tâche d'analyse à la demande en dehors des heures de pointe afin d'éviter toute charge supplémentaire sur l'infrastructure antivirus existante.

Pour en savoir plus sur les meilleures pratiques propres à nos partenaires, rendez-vous sur "Solutions partenaires Vscan".

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.

Étapes

1. Activer l'analyse antivirus sur un SVM :

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

> Vous pouvez utiliser le `vserver vscan disable` pour 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.

Ce dont vous aurez besoin

Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. 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.

Avant de commencer

Des privilèges avancés sont requis pour afficher le journal des événements Vscan.

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.
   ```

Surveillez et résolvez 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, reportez-vous au "Pages de manuel ONTAP".

Résolution des problèmes liés à l'analyse antivirus

Pour les problèmes courants d'analyse antivirus, il existe des causes possibles et des moyens de les résoudre. L'analyse antivirus est également appelée Vscan.

Problème	Comment le résoudre
Les serveurs Vscan ne peuvent pas se connecter à Système de stockage clustered ONTAP.	Vérifier si la configuration scanner pool spécifie l'adresse IP du serveur Vscan. Vérifiez également si les utilisateurs privilégiés autorisés dans la liste scanner pool sont actifs. Pour vérifier le scanner pool, exécutez le `vserver vscan scanner-pool show` dans l'invite de commande du système de stockage. Si les serveurs Vscan ne peuvent toujours pas se connecter, il peut y avoir un problème au niveau du réseau.
Les clients observent une latence élevée.	Il est probablement temps d'ajouter d'autres serveurs Vscan au pool de scanner.
Trop d'acquisitions sont déclenchées.	Modifier la valeur du `vscan-fileop-profile` paramètre permettant de limiter le nombre d'opérations de fichiers surveillées pour l'analyse antivirus.
Certains fichiers ne sont pas numérisés.	Vérifiez la stratégie d'accès. Il est possible que le chemin de ces fichiers ait été ajouté à la liste d'exclusion de chemin ou que leur taille dépasse la valeur configurée pour les exclusions. Pour vérifier la stratégie On-Access, exécutez `vserver vscan on-access-policy show` dans l'invite de commande du système de stockage.
Accès au fichier refusé.	Vérifiez si le paramètre *scan-obligatoire* est spécifié dans la configuration de la stratégie. Ce paramètre refuse l'accès aux données si aucun serveur Vscan n'est connecté. Modifiez le paramètre si nécessaire.

Surveiller l'état et les activités de performance

Vous pouvez surveiller les aspects critiques du module Vscan, tels que le statut de connexion du serveur Vscan, La santé des serveurs Vscan et le nombre de fichiers analysés. Ces informations sont utiles Vous diagnostiquez les problèmes liés au serveur Vscan.

Afficher les informations de connexion au serveur Vscan

Vous pouvez afficher le statut de connexion des serveurs Vscan pour gérer les connexions qui sont déjà utilisées et les connexions disponibles. Diverses commandes affichent des informations À propos du statut de connexion des serveurs Vscan.

Commande…	Informations affichées…
`vserver vscan connection-status show`	Résumé de l'état de la connexion
`vserver vscan connection-status show-all`	Informations détaillées sur l'état de la connexion
`vserver vscan connection-status show-not-connected`	État des connexions disponibles mais non connectées
`vserver vscan connection-status show-connected`	Informations sur le serveur Vscan connecté

Pour plus d'informations sur ces commandes, reportez-vous au "pages de manuel".

Afficher les statistiques du serveur Vscan

Vous pouvez afficher les statistiques spécifiques au serveur Vscan pour surveiller les performances et diagnostiquer les problèmes liés à analyse antivirus Vous devez collecter un échantillon de données avant de pouvoir utiliser le `statistics show` commande à Afficher les statistiques du serveur Vscan. Pour compléter un échantillon de données, procédez comme suit :

Étape

1. Exécutez le `statistics start` commande et le `optional statistics` commande d'arrêt.

Afficher les statistiques des requêtes et des latences du serveur Vscan

Vous pouvez utiliser ONTAP `offbox_vscan` Compteurs par SVM pour surveiller le taux de Vscan Requêtes de serveur envoyées et reçues par seconde et latences de serveur dans tous les Vscan serveurs. Pour afficher ces statistiques, procédez comme suit :

Étape

1. Exécutez les statistiques show `object offbox_vscan -instance SVM` commande avec compteurs suivants :

Compteur…	Informations affichées…
`scan_request_dispatched_rate`	Nombre de requêtes antivirus envoyées par ONTAP aux serveurs Vscan par seconde
`scan_noti_received_rate`	Nombre de requêtes antivirus reçues par ONTAP des serveurs Vscan par seconde
`dispatch_latency`	Latence dans ONTAP pour identifier un serveur Vscan disponible et envoyer la demande à ce serveur Vscan
`scan_latency`	Latence aller-retour de ONTAP au serveur Vscan, y compris le temps que le scan doit s'exécuter

Exemple de statistiques générées à partir d'un compteur ONTAP externe vscan

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
---------------------------------------------------------------
```

Afficher les statistiques des requêtes et des latences individuelles du serveur Vscan

Vous pouvez utiliser ONTAP `offbox_vscan_server` Compteurs sur un serveur Vscan par SVM, par serveur Vscan externe, Et par nœud pour surveiller le taux des requêtes du serveur Vscan expédiées et la latence du serveur sur Chaque serveur Vscan individuellement. Pour collecter ces informations, procédez comme suit :

Étape

1. Exécutez le `statistics show -object offbox_vscan -instance SVM:servername:nodename` avec les compteurs suivants :

Compteur…	Informations affichées…
`scan_request_dispatched_rate`	Nombre de demandes d'analyse antivirus envoyées par ONTAP
`scan_latency`	Latence aller-retour de ONTAP au serveur Vscan, y compris le temps que le scan doit s'exécuter Vers les serveurs Vscan par seconde

Exemple de statistiques générées à partir d'un compteur ONTAP offbox_vscan_Server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-----------------------------------------------------------------
```

Afficher les statistiques d'utilisation du serveur Vscan

Vous pouvez également utiliser ONTAP `offbox_vscan_server` Compteurs pour la collecte de l'utilisation Vscan côté serveur statistiques. Ces statistiques sont suivies par SVM, par serveur Vscan externe et par nœud. Ils Inclure l'utilisation des CPU sur le serveur Vscan, la profondeur de file d'attente pour les opérations de scan sur le serveur Vscan (actuel et maximal), mémoire utilisée et réseau utilisé. Ces statistiques sont transmises par l'antivirus Connector aux compteurs statistiques de ONTAP. Ils sont basées sur des données interrogées toutes les 20 secondes et doivent être collectées plusieurs fois pour plus de précision ; sinon, les valeurs affichées dans les statistiques reflètent uniquement la dernière interrogation. L'utilisation du processeur et les files d'attente sont il est particulièrement important de surveiller et d'analyser. Une valeur élevée pour une file d'attente moyenne peut indiquer que l' Le serveur Vscan présente un goulet d'étranglement. Pour collecter les statistiques d'utilisation du serveur Vscan sur un SVM, un serveur Vscan par—serveur externe, et par—nœud basis, effectuez l'étape suivante :

Étape

1. Collectez les statistiques d'utilisation du serveur Vscan

   Exécutez le `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` avec les commandes suivantes `offbox_vscan_server` compteurs :

Compteur…	Informations affichées…
`scanner_stats_pct_cpu_used`	Utilisation du CPU sur le serveur Vscan
`scanner_stats_pct_input_queue_avg`	File d'attente moyenne des requêtes de scan sur le serveur Vscan
`scanner_stats_pct_input_queue_hiwatermark`	File d'attente de pointe des requêtes de scan sur le serveur Vscan
`scanner_stats_pct_mem_used`	Mémoire utilisée sur le serveur Vscan
`scanner_stats_pct_network_used`	Réseau utilisé sur le serveur Vscan

Exemple de statistiques d'utilisation pour le serveur Vscan

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```