À propos de la protection antivirus NetApp

ONTAP 9

NetApp
April 24, 2024

Sommaire

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.

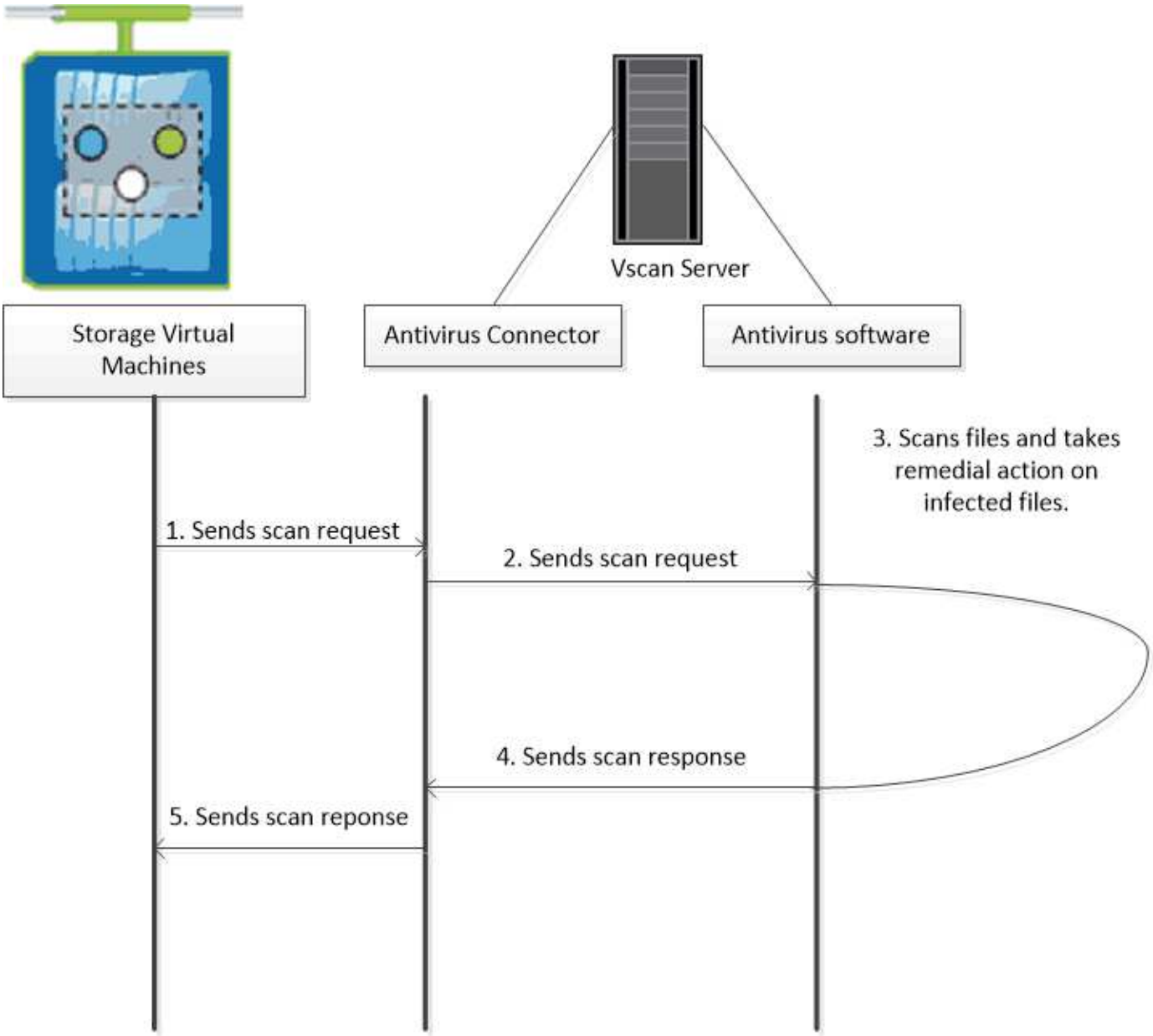
  L’analyse lors de l’accès n’est pas prise en charge par NFS.

- 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.

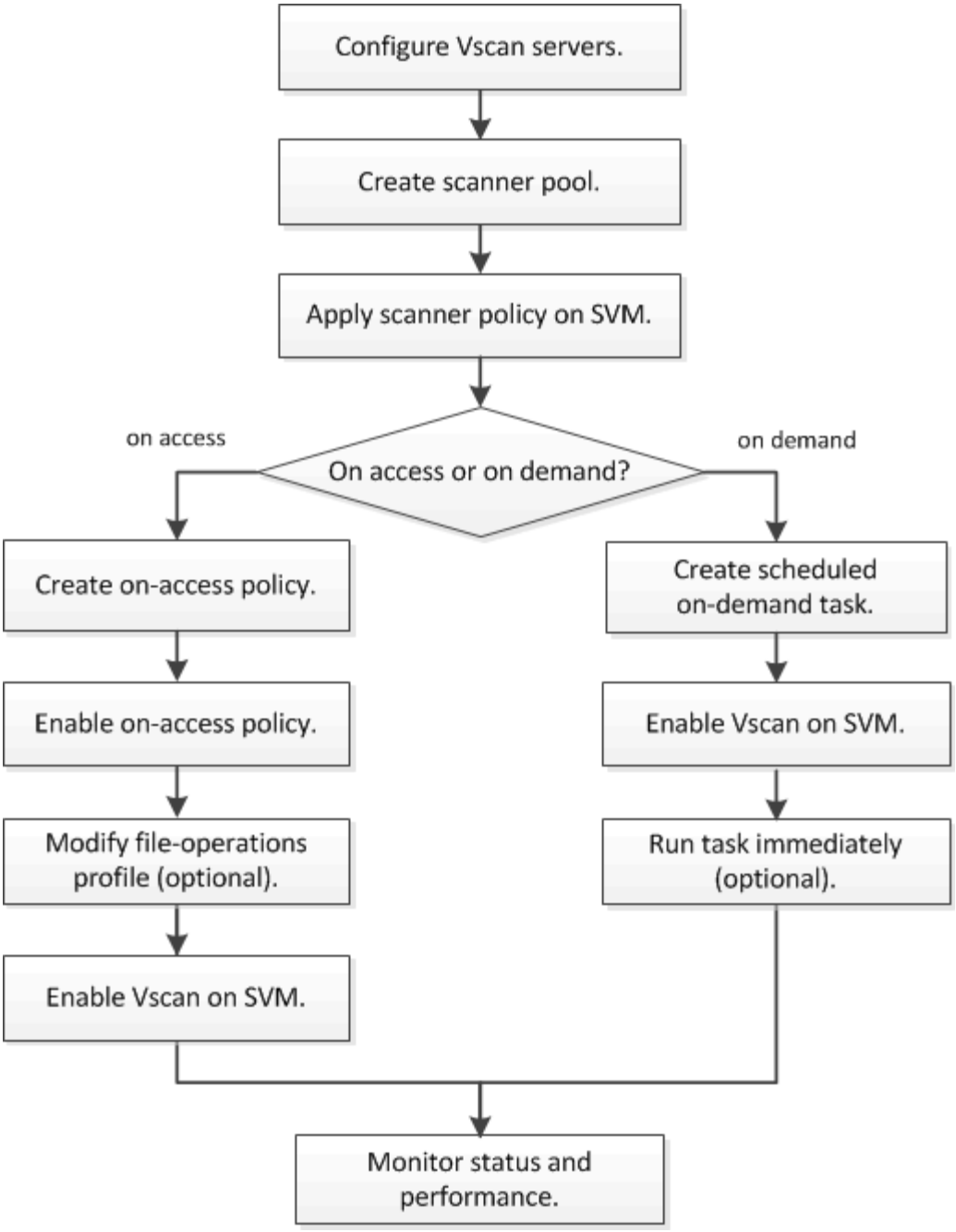
Le connecteur antivirus ONTAP, fourni par NetApp et installé sur le serveur externe, gère la communication entre le système de stockage et le logiciel antivirus.



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)"

En tant que partenaire	Documentation de la solution	Détails sur l'interopérabilité
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)"
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