Informazioni sulla protezione antivirus di NetApp

ONTAP 9

NetApp
April 24, 2024

Sommario

Informazioni sulla protezione antivirus di NetApp

Informazioni sulla scansione dei virus NetApp

Vscan è una soluzione di scansione antivirus sviluppata da NetApp che consente ai clienti di proteggere i propri dati da virus o altri codici dannosi. Combina il software antivirus fornito dal partner con le funzionalità ONTAP per offrire ai clienti la flessibilità necessaria per gestire la scansione dei file.

Come funziona la scansione virus

I sistemi storage trasferiscono le operazioni di scansione a server esterni che ospitano software antivirus di terze parti.

In base alla modalità di scansione attiva, ONTAP invia richieste di scansione quando i client accedono ai file tramite SMB (on-access) o accedono ai file in posizioni specifiche, in base a una pianificazione o immediatamente (on-demand).

- È possibile utilizzare *on-access scanning* per verificare la presenza di virus quando i client aprono, leggono, rinominano o chiudono i file su SMB. Le operazioni sui file vengono sospese fino a quando il server esterno non riporta lo stato di scansione del file. Se il file è già stato sottoposto a scansione, ONTAP consente l'operazione. In caso contrario, richiede una scansione dal server.

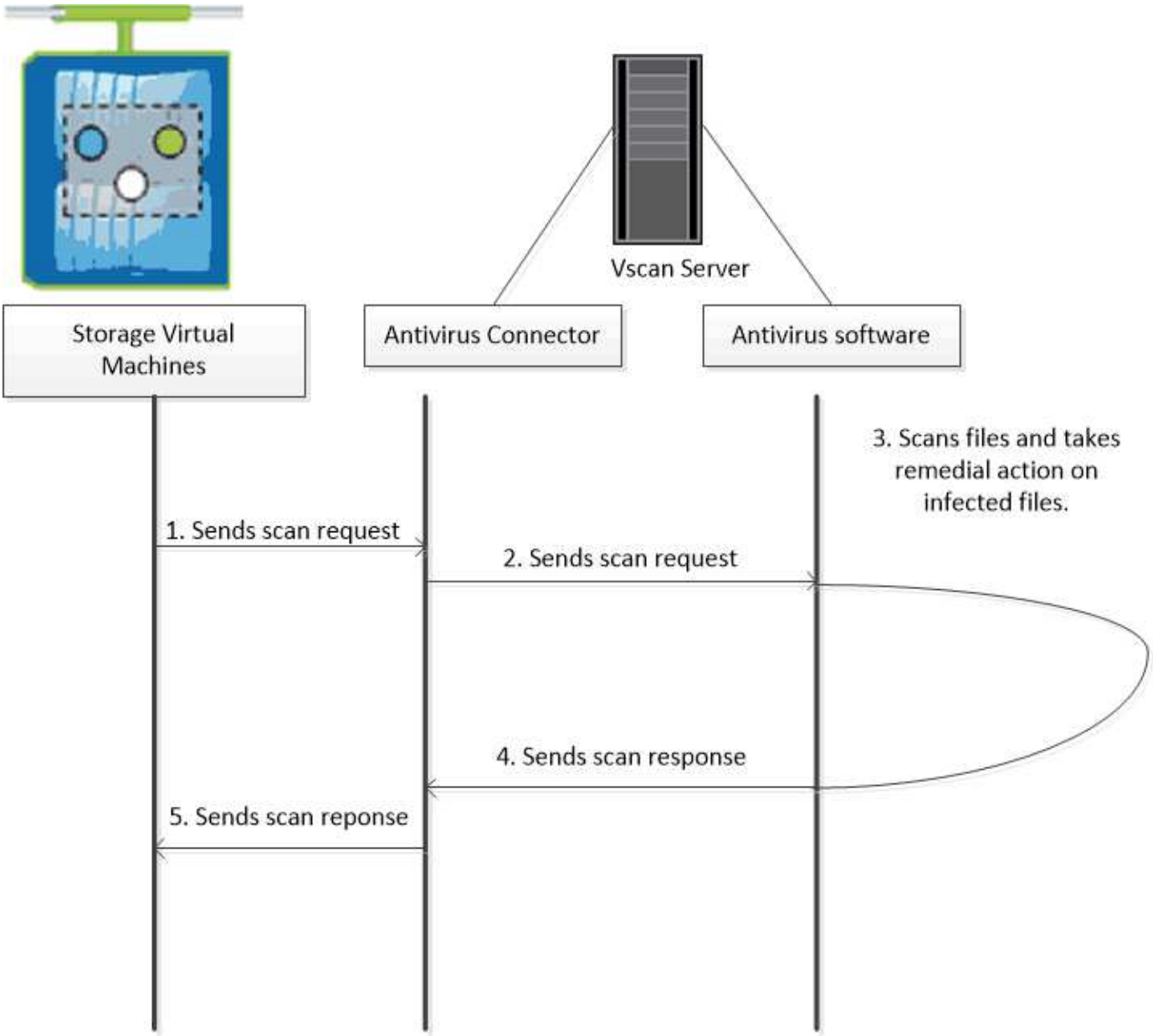
  La scansione on-access non è supportata per NFS.

- È possibile utilizzare la *scansione on-demand* per controllare i file alla ricerca di virus immediatamente o in base a una pianificazione. Si consiglia di eseguire scansioni on-demand solo in ore non di punta per evitare di sovraccaricare l'infrastruttura AV esistente, che è normalmente dimensionata per la scansione on-access. Il server esterno aggiorna lo stato di scansione dei file selezionati, in modo da ridurre la latenza di accesso ai file su SMB. In caso di modifiche al file o aggiornamenti della versione software, viene richiesta una nuova scansione del file dal server esterno.

  È possibile utilizzare la scansione on-demand per qualsiasi percorso nello spazio dei nomi SVM, anche per i volumi esportati solo tramite NFS.

In genere, si abilitano le modalità di scansione on-access e on-demand su una SVM. In entrambe le modalità, il software antivirus esegue un'azione correttiva sui file infetti in base alle impostazioni del software.

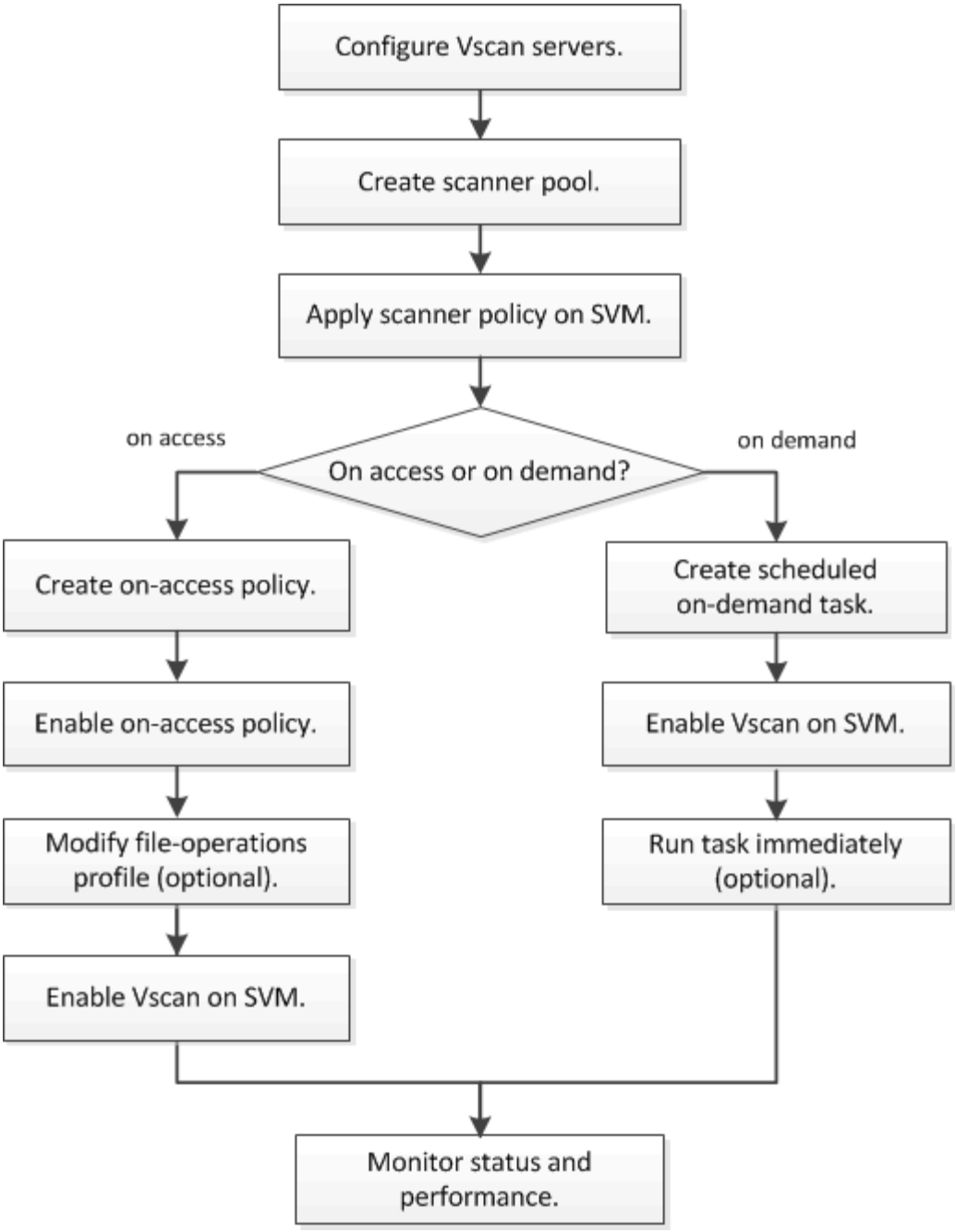
Il connettore antivirus ONTAP, fornito da NetApp e installato sul server esterno, gestisce la comunicazione tra il sistema di storage e il software antivirus.



Workflow di scansione dei virus

Prima di attivare la scansione, è necessario creare un pool di scanner e applicare un criterio scanner. In genere, si abilitano le modalità di scansione on-access e on-demand su una SVM.

È necessario aver completato la configurazione CIFS.



Passi successivi

- Creare un pool di scanner su un singolo cluster
- Applicare un criterio scanner a un singolo cluster
- Creare una policy di accesso

Architettura antivirus

L'architettura antivirus di NetApp è costituita dal software del server Vscan e dalle relative impostazioni.

Software del server Vscan

È necessario installare questo software sul server Vscan.

- **Connettore antivirus ONTAP**

  Si tratta di un software fornito da NetApp che gestisce le comunicazioni di risposta e richiesta di scansione tra le SVM e il software antivirus. Può essere eseguito su una macchina virtuale, ma per ottenere le migliori performance utilizza una macchina fisica. È possibile scaricare questo software dal sito del supporto NetApp (richiede l'accesso).

- **Software antivirus**

  Si tratta di un software fornito dal partner che esegue la scansione dei file alla ricerca di virus o altro codice dannoso. Specificare le azioni correttive da intraprendere sui file infetti durante la configurazione del software.

Impostazioni del software Vscan

È necessario configurare queste impostazioni software sul server Vscan.

- **Scanner pool**

  Questa impostazione definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. Definisce inoltre un periodo di timeout della richiesta di scansione, trascorso il quale la richiesta di scansione viene inviata a un server Vscan alternativo, se disponibile.

  > Impostare il periodo di timeout nel software antivirus sul server Vscan su un valore inferiore di cinque secondi rispetto al periodo di timeout della richiesta di scansione del pool di scanner. In questo modo si evitano situazioni in cui l'accesso al file viene ritardato o negato del tutto perché il periodo di timeout sul software è superiore al periodo di timeout per la richiesta di scansione.

- **Utente con privilegi**

  Questa impostazione è un account utente di dominio utilizzato da un server Vscan per connettersi a SVM. L'account deve essere presente nell'elenco degli utenti con privilegi nel pool di scanner.

- **Criterio scanner**

  Questa impostazione determina se un pool di scanner è attivo. I criteri dello scanner sono definiti dal sistema, pertanto non è possibile creare policy personalizzate dello scanner. Sono disponibili solo queste tre policy:

  - `Primary` specifica che il pool di scanner è attivo.
  - `Secondary` Specifica che il pool di scanner è attivo, solo quando nessuno dei server Vscan nel pool di scanner primario è connesso.
  - `Idle` specifica che il pool di scanner non è attivo.

- **Policy di accesso**

  Questa impostazione definisce l'ambito di una scansione all'accesso. È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e

le estensioni e i percorsi dei file da escludere dalla scansione.

Per impostazione predefinita, viene eseguita la scansione solo dei volumi di lettura/scrittura. È possibile specificare i filtri che consentono la scansione di volumi di sola lettura o che limitano la scansione ai file aperti con accesso di esecuzione:

- `scan-ro-volume` consente la scansione di volumi di sola lettura.
- `scan-execute-access` limita la scansione ai file aperti con accesso di esecuzione.

> “Execute access” è diverso da “Execute permission”. Un determinato client avrà “Execute Access” su un file eseguibile solo se il file è stato aperto con “Execute Intent”.

È possibile impostare `scan-mandatory` Selezionare Off per specificare che l’accesso al file è consentito quando non sono disponibili server Vscan per la scansione dei virus. Nella modalità on-access è possibile scegliere tra queste due opzioni che si escludono a vicenda:

- Obbligatorio: Con questa opzione, Vscan tenta di inviare la richiesta di scansione al server fino alla scadenza del periodo di timeout. Se la richiesta di scansione non viene accettata dal server, la richiesta di accesso client viene negata.
- Non obbligatorio: Con questa opzione, Vscan consente sempre l’accesso al client, indipendentemente dal fatto che sia disponibile un server Vscan per la scansione dei virus.

- **Attività on-demand**

  Questa impostazione definisce l’ambito di una scansione on-demand. È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e le estensioni e i percorsi dei file da escludere dalla scansione. Per impostazione predefinita, i file nelle sottodirectory vengono sottoposti a scansione.

  Si utilizza una pianificazione cron per specificare quando eseguire l’attività. È possibile utilizzare `vserver vscan on-demand-task run` per eseguire l’attività immediatamente.

- **Profilo delle operazioni del file Vscan (solo scansione all’accesso)**

  Il `vscan-fileop-profile` parametro per `vserver cifs share create` Il comando definisce quali operazioni di file SMB attivano la scansione dei virus. Per impostazione predefinita, il parametro è impostato su `standard`, Che è la Best practice di NetApp. È possibile regolare questo parametro in base alle necessità quando si crea o si modifica una condivisione SMB:

  - `no-scan` specifica che le scansioni antivirus non vengono mai attivate per la condivisione.
  - `standard` specifica che le scansioni antivirus vengono attivate da operazioni di apertura, chiusura e ridenominazione.
  - `strict` specifica che le scansioni antivirus vengono attivate da operazioni di apertura, lettura, chiusura e ridenominazione.

    Il `strict` profile offre una maggiore sicurezza per le situazioni in cui più client accedono a un file contemporaneamente. Se un client chiude un file dopo averlo scritto e lo stesso file rimane aperto su un secondo client, `strict` garantisce che un’operazione di lettura sul secondo client attivi una scansione prima della chiusura del file.

    Fare attenzione a limitare il `strict` il profilo alle condivisioni contenenti file che prevedi sia accessibile contemporaneamente. Poiché questo profilo genera più richieste di scansione, potrebbe

avere un impatto sulle performance.

- `writes-only` specifica che le scansioni antivirus vengono attivate solo quando i file modificati vengono chiusi.

  Da `writes-only` genera meno richieste di scansione, in genere migliora le performance.

Se si utilizza questo profilo, lo scanner deve essere configurato per eliminare o mettere in quarantena i file infetti non riparabili, in modo che non sia possibile accedervi. Se, ad esempio, un client chiude un file dopo la scrittura di un virus e il file non viene riparato, eliminato o messo in quarantena, qualsiasi client che accede al file `without` la scrittura su di esso sarà infetto.

> Se un'applicazione client esegue un'operazione di ridenominazione, il file viene chiuso con il nuovo nome e non viene sottoposto a scansione. Se tali operazioni rappresentano un problema di sicurezza nell'ambiente in uso, è necessario utilizzare `standard` oppure `strict` profilo.

Soluzioni partner di Vscan

NetApp collabora con Trellix, Symantec, Trend Micro e Sentinel One per offrire soluzioni anti-malware e anti-virus leader del settore basate sulla tecnologia ONTAP Vscan. Queste soluzioni consentono di eseguire la scansione dei file per rilevare la presenza di malware e correggere eventuali file interessati.

Come mostrato nella tabella seguente, i dettagli relativi all'interoperabilità per Trellix, Symantec e Trend Micro sono conservati nella matrice di interoperabilità NetApp. I dettagli sull'interoperabilità per Trellix e Symantec sono disponibili anche sui siti Web dei partner. I dettagli sull'interoperabilità di Sentinel One e degli altri nuovi partner verranno gestiti dal partner sui propri siti Web.

Partner	Documentazione della soluzione	Dettagli sull'interoperabilità
Trellix (precedentemente McAfee)	"Documentazione del prodotto Trellix"	• "Tool di matrice di interoperabilità NetApp" • "Piattaforme supportate per Endpoint Security Storage Protection (trellix.com)"
Symantec	"Symantec Protection Engine 9.0.0"	• "Tool di matrice di interoperabilità NetApp" • "Matrice di supporto per dispositivi partner certificati con Symantec Protection Engine (SPE) per NAS (Network Attached Storage) 9.x.x" • "Matrice di supporto per i dispositivi partner certificata con Symantec Protection Engine (SPE) per NAS (Network Attached Storage) 8.x (broadcom.com)"

Partner	Documentazione della soluzione	Dettagli sull'interoperabilità
Trend Micro	"Guida introduttiva di Trend Micro ServerProtect for Storage 6.0"	"Tool di matrice di interoperabilità NetApp"
Sentinel One	• "SentinelOne Singularity Cloud Data Security" • "Supporto SentinelOne" Questo collegamento richiede l'accesso dell'utente. È possibile richiedere l'accesso da Sentinel One.	Istinto profondo