Protezione antivirus con Vscan

ONTAP 9

NetApp
August 31, 2024

Sommario

Protezione antivirus con Vscan

Panoramica della configurazione antivirus

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.

Vscan esegue scansioni virus quando i client accedono ai file tramite SMB. È possibile configurare Vscan per la scansione on-demand o in base a una pianificazione. È possibile interagire con Vscan utilizzando l'interfaccia a riga di comando (CLI) di ONTAP o le API (Application Programming Interface) di ONTAP.

Informazioni correlate

"Soluzioni partner di Vscan"

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.

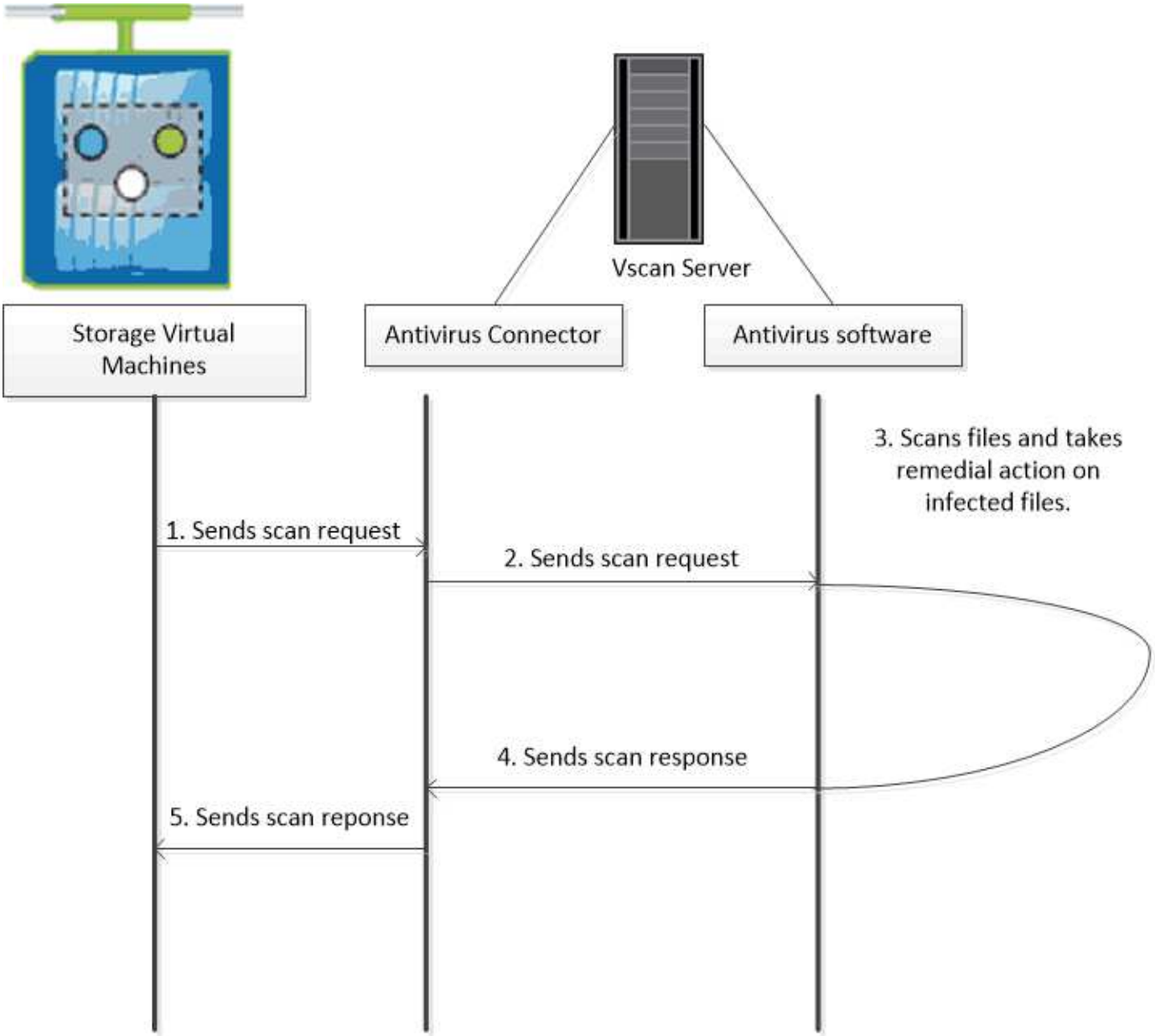
- È possibile utilizzare la *scansione on-demand* per controllare i file alla ricerca di virus immediatamente o in base a una pianificazione. Si consiglia di eseguire scansioni on-demand solo in ore non di punta per evitare di sovraccaricare l'infrastruttura AV esistente, che è normalmente dimensionata 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.

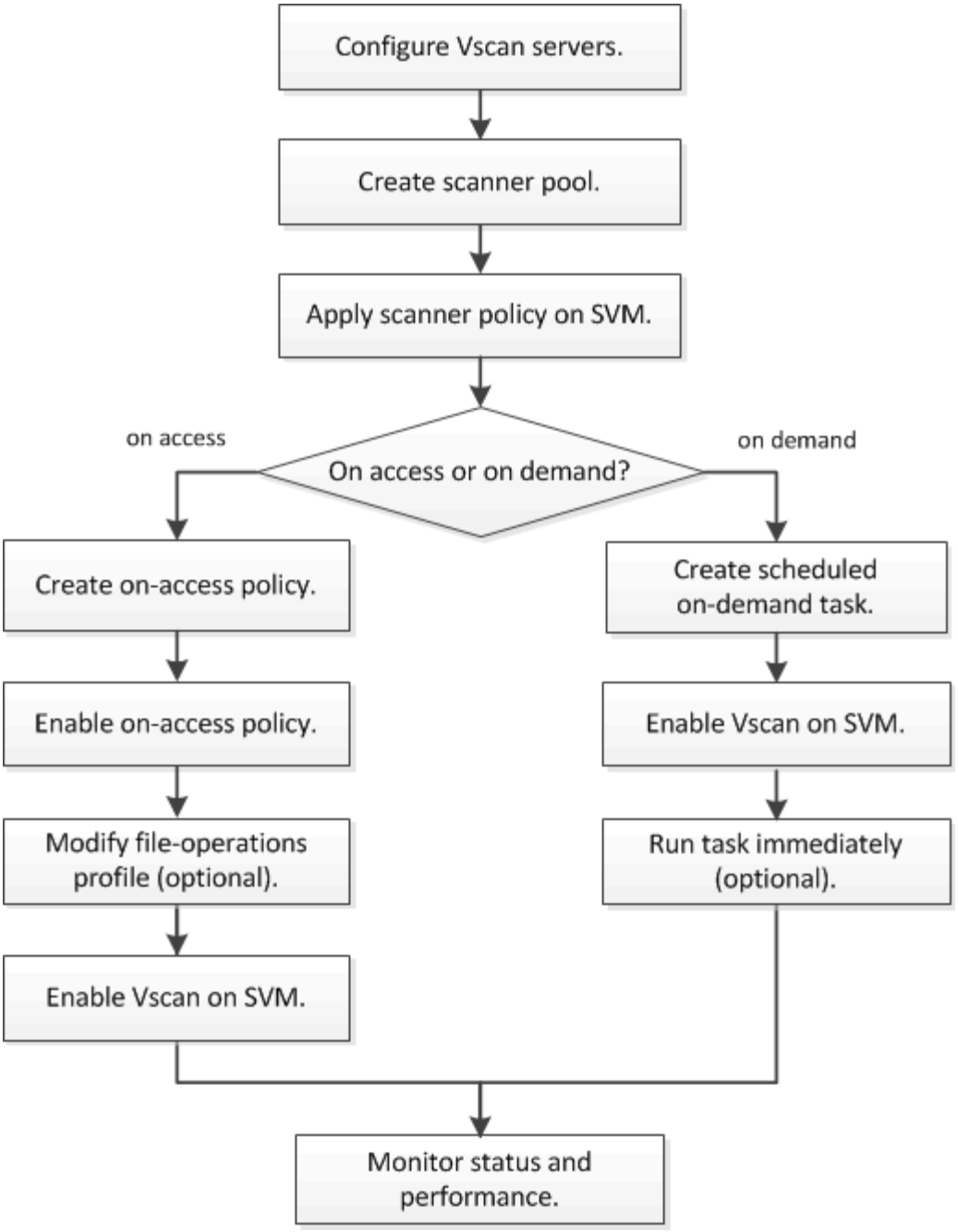
Il connettore antivirus ONTAP, fornito da NetApp e installato sul server esterno, gestisce la comunicazione tra il sistema di storage e il software antivirus.



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)"
Trend Micro	"Guida introduttiva di Trend Micro ServerProtect for Storage 6.0"	"Tool di matrice di interoperabilità NetApp"

Partner	Documentazione della soluzione	Dettagli sull'interoperabilità
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

Installazione e configurazione del server Vscan

Installazione e configurazione del server Vscan

Impostare uno o più server Vscan per verificare che i file sul sistema vengano sottoposti a scansione antivirus. Seguire le istruzioni fornite dal fornitore per installare e configurare il software antivirus sul server.

Seguire le istruzioni contenute nel file README fornito da NetApp per installare e configurare il connettore antivirus ONTAP. In alternativa, seguire le istruzioni sul "Pagina installare il connettore antivirus ONTAP".

Per le configurazioni di disaster recovery e MetroCluster, è necessario configurare server Vscan separati per i cluster ONTAP primario/locale e secondario/partner.

Requisiti del software antivirus

- Per informazioni sui requisiti del software antivirus, consultare la documentazione del vendor.
- Per informazioni su vendor, software e versioni supportate da Vscan, consultare "Soluzioni partner di Vscan" pagina.

Requisiti del connettore antivirus ONTAP

- È possibile scaricare il connettore antivirus ONTAP dalla pagina **Download software** sul sito di supporto NetApp. "Download NetApp: Software"
- Per informazioni sulle versioni di Windows supportate dal connettore antivirus ONTAP e sui requisiti di interoperabilità, vedere "Soluzioni partner di Vscan".

È possibile installare diverse versioni dei server Windows per diversi server Vscan in un cluster.

- Sul server Windows deve essere installato .NET 3.0 o versione successiva.
- SMB 2.0 deve essere attivato sul server Windows.

Installare il connettore antivirus ONTAP

Installare il connettore antivirus ONTAP sul server Vscan per abilitare la comunicazione tra il sistema che esegue ONTAP e il server Vscan. Una volta installato il connettore

antivirus ONTAP, il software antivirus è in grado di comunicare con una o più Storage Virtual Machine (SVM).

A proposito di questa attività

- Vedere "Soluzioni partner di Vscan" Per informazioni sui protocolli supportati, le versioni del software dei fornitori antivirus, le versioni di ONTAP, i requisiti di interoperabilità e i server Windows.
- È necessario installare .NET 4.5.1 o versione successiva.
- Il connettore antivirus ONTAP può essere eseguito su una macchina virtuale. Tuttavia, per ottenere prestazioni ottimali, NetApp consiglia di utilizzare una macchina virtuale dedicata per la scansione antivirus.
- SMB 2,0 deve essere attivato sul server Windows su cui si sta installando ed eseguendo il connettore antivirus ONTAP.

Prima di iniziare

- Scaricare il file di installazione di ONTAP Antivirus Connector dal sito di assistenza e salvarlo in una directory sul disco rigido.
- Verificare di soddisfare i requisiti per l'installazione del connettore antivirus ONTAP.
- Verificare di disporre dei privilegi di amministratore per installare il connettore antivirus.

Fasi

1. Avviare l'installazione guidata del connettore antivirus eseguendo il file di installazione appropriato.
2. Selezionare *Avanti*. Viene visualizzata la finestra di dialogo cartella di destinazione.
3. Selezionare *Avanti* per installare il connettore antivirus nella cartella elencata oppure selezionare *Cambia* per eseguire l'installazione in una cartella diversa.
4. Viene visualizzata la finestra di dialogo credenziali servizio Windows connettore AV ONTAP.
5. Immettere le credenziali del servizio Windows o selezionare **Aggiungi** per selezionare un utente. Per un sistema ONTAP, questo utente deve essere un utente di dominio valido e deve esistere nella configurazione del pool di scanner per la SVM.
6. Selezionare **Avanti**. Viene visualizzata la finestra di dialogo Pronto per l'installazione del programma.
7. Selezionare **Installa** per avviare l'installazione o selezionare **Indietro** se si desidera apportare modifiche alle impostazioni. Viene visualizzata una finestra di stato che illustra l'avanzamento dell'installazione, seguita dalla finestra di dialogo InstallShield Wizard Completed (Installazione guidata InstallShield completata).
8. Selezionare la casella di controllo Configura LIF ONTAP per continuare con la configurazione di LIF dati o gestione ONTAP. Devi configurare almeno una gestione ONTAP o un'interfaccia LIF dati prima che questo server Vscan possa essere utilizzato.
9. Selezionare la casella di controllo Mostra registro **Windows Installer** se si desidera visualizzare i registri di installazione.
10. Selezionare **fine** per terminare l'installazione e chiudere la procedura guidata InstallShield. L'icona **Configura LIF ONTAP** viene salvata sul desktop per configurare le LIF ONTAP.
11. Aggiungere una SVM al connettore antivirus. Puoi aggiungere una SVM al connettore antivirus aggiungendo una LIF di gestione ONTAP, che viene interrogata per recuperare l'elenco di LIF dati, oppure configurando direttamente la LIF o la LIF dati. Se la LIF di gestione ONTAP è configurata, devi anche fornire le informazioni di polling e le credenziali dell'account amministratore di ONTAP.
    - Verifica che la LIF di gestione o l'indirizzo IP della SVM sia abilitato per `management-https`. Non è necessario quando si configurano solo LIF dati.

- Verificare di aver creato un account utente per l'applicazione HTTP e di aver assegnato un ruolo con accesso (almeno di sola lettura) a `/api/network/ip/interfaces` API REST. Per ulteriori informazioni sulla creazione di un utente, vedere la "creazione del ruolo di accesso di sicurezza" e. "creazione dell'accesso di sicurezza" Pagine man di ONTAP.

> Puoi anche utilizzare l'utente di dominio come account aggiungendo una SVM con tunnel di autenticazione per una SVM amministrativa. Per ulteriori informazioni, consultare "login di sicurezza creazione del tunnel di dominio" Pagina man di ONTAP o utilizzare `/api/security/acccounts` e. `/api/security/roles` REST API per configurare l'account e il ruolo di amministratore.

Fasi

1. Fare clic con il pulsante destro del mouse sull'icona **Configure ONTAP LIF**, salvata sul desktop al termine dell'installazione di Antivirus Connector, quindi selezionare **Esegui come amministratore**.
2. Nella finestra di dialogo Configura LIF ONTAP, selezionare il tipo di configurazione preferito, quindi eseguire le seguenti operazioni:

Per creare questo tipo di LIF…	Eseguire questa procedura…
LIF dati	a. Impostare "ruolo" su "dati" b. Impostare "protocollo dati" su "cifs" c. Impostare "policy firewall" su "data" d. Impostare "politica di servizio" su "file-dati-predefiniti"
LIF di gestione	a. Impostare "ruolo* su "dati" b. Impostare "protocollo dati" su "nessuno" c. Impostare "policy firewall" su "Mgmt" d. Impostare "politica di servizio" su "gestione predefinita"

   Scopri di più "Creazione di una LIF".

   Dopo aver creato una LIF, inserisci i dati o l'indirizzo IP della LIF di gestione o della SVM che desideri aggiungere. Puoi anche inserire la LIF di gestione cluster. Se specifichi la LIF di gestione cluster, tutte le SVM del cluster che servono SMB potranno utilizzare il server Vscan.

> Quando è richiesta l'autenticazione Kerberos per i server Vscan, ogni LIF dati SVM deve avere un nome DNS univoco ed è necessario registrarlo come nome principale server (SPN) con Windows Active Directory. Quando non è disponibile un nome DNS univoco per ogni LIF dati o registrato come SPN, il server Vscan utilizza il meccanismo NT LAN Manager per l'autenticazione. Se si aggiungono o modificano i nomi DNS e gli SPN dopo la connessione del server Vscan, è necessario riavviare il servizio Antivirus Connector sul server Vscan per applicare le modifiche.

3. Per configurare una LIF di gestione, inserisci la durata del polling in secondi. La durata del poll è la frequenza con cui il connettore antivirus verifica le modifiche alle SVM o alla configurazione LIF del cluster. L'intervallo di polling predefinito è di 60 secondi.
4. Inserisci il nome dell'account e la password dell'amministratore ONTAP per configurare una LIF di gestione.

5. Fare clic su **Test** per controllare la connettività e verificare l'autenticazione. L'autenticazione viene verificata solo per una configurazione LIF di gestione.
6. Fare clic su **Update** (Aggiorna) per aggiungere la LIF all'elenco delle LIF a cui eseguire il polling o connettersi.
7. Fare clic su **Salva** per salvare la connessione al Registro di sistema.
8. Fare clic su **Esporta** se si desidera esportare l'elenco delle connessioni in un file di importazione del Registro di sistema o di esportazione del Registro di sistema. Ciò è utile se più server Vscan utilizzano lo stesso set di LIF di gestione o di dati.

Vedere "Configurare la pagina ONTAP Antivirus Connector" per le opzioni di configurazione.

Configurare il connettore antivirus ONTAP

Configurare il connettore antivirus ONTAP per specificare una o più Storage Virtual Machine (SVM) a cui connettersi inserendo la LIF di gestione ONTAP, le informazioni di polling e le credenziali dell'account amministratore ONTAP o solo la LIF dati. Puoi anche modificare i dettagli di una connessione SVM o rimuovere una connessione SVM. Per impostazione predefinita, il connettore antivirus ONTAP utilizza le API REST per recuperare l'elenco di LIF di dati, se la LIF di gestione ONTAP è configurata.

Modificare i dettagli di una connessione SVM

Puoi aggiornare i dettagli di una connessione SVM (Storage Virtual Machine), che è stata aggiunta al connettore antivirus, modificando la LIF di gestione ONTAP e le informazioni di polling. Non puoi aggiornare le LIF dati dopo che sono state aggiunte. Per aggiornare le LIF dati, devi prima rimuoverle e poi aggiungerle di nuovo con il nuovo indirizzo LIF o IP.

Prima di iniziare

Verificare di aver creato un account utente per l'applicazione HTTP e di aver assegnato un ruolo con accesso (almeno di sola lettura) a `/api/network/ip/interfaces` API REST. Per ulteriori informazioni sulla creazione di un utente, vedere la "creazione del ruolo di accesso di sicurezza" e a. "creazione dell'accesso di sicurezza" comandi. Puoi anche utilizzare l'utente di dominio come account aggiungendo una SVM con tunnel di autenticazione per una SVM amministrativa. Per ulteriori informazioni, consultare "login di sicurezza creazione del tunnel di dominio" Pagina man di ONTAP.

Fasi

1. Fare clic con il pulsante destro del mouse sull'icona **Configura LIF ONTAP**, salvata sul desktop al termine dell'installazione di Antivirus Connector, quindi selezionare **Esegui come amministratore**. Viene visualizzata la finestra di dialogo Configura LIF ONTAP.
2. Selezionare l'indirizzo IP della SVM, quindi fare clic su **Aggiorna**.
3. Aggiornare le informazioni secondo necessità.
4. Fare clic su **Salva** per aggiornare i dettagli della connessione nel registro.
5. Fare clic su **Esporta** se si desidera esportare l'elenco delle connessioni in un'importazione del Registro di sistema o in un file di esportazione del Registro di sistema. Ciò è utile se più server Vscan utilizzano lo stesso set di LIF di gestione o di dati.

Rimuovere una connessione SVM dal connettore antivirus

Se non ti serve più una connessione SVM, puoi rimuoverla.

Fasi

1. Fare clic con il pulsante destro del mouse sull'icona **Configura LIF ONTAP**, salvata sul desktop al termine dell'installazione di Antivirus Connector, quindi selezionare **Esegui come amministratore**. Viene visualizzata la finestra di dialogo Configura LIF ONTAP.
2. Selezionare uno o più indirizzi IP SVM, quindi fare clic su **Rimuovi**.
3. Fare clic su **Salva** per aggiornare i dettagli della connessione nel registro.
4. Fare clic su **Esporta** se si desidera esportare l'elenco delle connessioni in un file di importazione del Registro di sistema o di esportazione del Registro di sistema. Ciò è utile se più server Vscan utilizzano lo stesso set di LIF di gestione o di dati.

Risolvere i problemi

Prima di iniziare

Quando si creano i valori del Registro di sistema in questa procedura, utilizzare il riquadro a destra.

È possibile attivare o disattivare i registri dei connettori antivirus per scopi diagnostici. Per impostazione predefinita, questi registri sono disattivati. Per migliorare le prestazioni, è necessario disattivare i registri del connettore antivirus e attivarli solo per gli eventi critici.

Fasi

1. Selezionare **Start**, digitare "regedit" nella casella di ricerca, quindi selezionare `regedit.exe` Nell'elenco programmi.
2. In **Editor del Registro di sistema**, individuare la seguente sottochiave per il connettore antivirus ONTAP: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Creare i valori del Registro di sistema specificando il tipo, il nome e i valori indicati nella tabella seguente:

Tipo	Nome	Valori
Stringa	Tracepath	c:\avshim.log

   Questo valore del Registro di sistema potrebbe essere qualsiasi altro percorso valido.

4. Creare un altro valore del Registro di sistema fornendo il tipo, il nome, i valori e le informazioni di registrazione mostrate nella tabella seguente:

Tipo	Nome	Registrazione critica	Registrazione intermedia	Registrazione dettagliata
DWORD	TRACELEVEL	1	2 o 3	4

   In questo modo si attivano i registri del connettore antivirus salvati al valore del percorso fornito in TracePath nel passaggio 3.

5. Disattivare i registri del connettore antivirus eliminando i valori del Registro di sistema creati nei passaggi 3 e 4.
6. Creare un altro valore di registro di tipo "MULTI_SZ" con il nome "LogRotation" (senza virgolette). In "LogRotation", Fornire "logFileSize:1" come voce per la dimensione di rotazione (dove 1 rappresenta 1MB) e nella riga successiva fornire "logFileCount:5" come un immissione del limite di rotazione (5 è il limite).

Questi valori sono facoltativi. Se non vengono forniti, vengono utilizzati i valori predefiniti dei file 20MB e 10 rispettivamente per la dimensione di rotazione e il limite di rotazione. I valori interi forniti non forniscono valori decimali o frazioni. Se si forniscono valori superiori ai valori predefiniti, vengono utilizzati i valori predefiniti.

7. Per disattivare la rotazione del registro configurata dall'utente, eliminare i valori del Registro di sistema creati nel passaggio 6.

Banner personalizzabile

Un banner personalizzato ti consente di inserire un'istruzione legale e un'esclusione di responsabilità per l'accesso al sistema nella finestra *Configure ONTAP LIF API*.

Fase

1. Modificare l'intestazione predefinita aggiornando il contenuto della `banner.txt` nella directory di installazione, quindi salvare le modifiche. Riapri la finestra Configura API LIF ONTAP per vedere le modifiche riflesse nel banner.

Attivare la modalità Extended Ordinance (EO)

È possibile attivare e disattivare la modalità Extended Ordinance (EO) per garantire un funzionamento sicuro.

Fasi

1. Selezionare **Start**, digitare "regedit" nella casella di ricerca, quindi selezionare `regedit.exe` Nell'elenco programmi.
2. In **Editor del Registro di sistema**, individuare la seguente sottochiave per ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Nel riquadro a destra, creare un nuovo valore del Registro di sistema di tipo "DWORD" con il nome "EO_Mode" (senza virgolette) e il valore "1" (senza virgolette) per attivare la modalità EO o il valore "0" (senza virgolette) per disattivare la modalità EO.

Per impostazione predefinita, se `EO_Mode` La voce del Registro di sistema è assente, la modalità EO è disattivata. Quando si attiva la modalità EO, è necessario configurare sia il server syslog esterno che l'autenticazione dei certificati reciproci.

Configurare il server syslog esterno

Prima di iniziare

Tenere presente che quando si creano i valori del Registro di sistema in questa procedura, utilizzare il riquadro a destra.

Fasi

1. Selezionare **Start**, digitare "regedit" nella casella di ricerca, quindi selezionare `regedit.exe` Nell'elenco programmi.
2. In **Editor del Registro di sistema**, creare la seguente sottochiave per ONTAP Antivirus Connector per la configurazione syslog: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Creare un valore del Registro di sistema specificando il tipo, il nome e il valore come illustrato nella tabella seguente:

Tipo	Nome	Valore
DWORD	syslog_enabled	1 o 0

Si noti che un valore "1" attiva il syslog e un valore "0" lo disattiva.

4. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome
REG_SZ	Syslog_host

Fornire l'indirizzo IP dell'host syslog o il nome di dominio per il campo valore.

5. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome
REG_SZ	Porta_syslog

Specificare il numero della porta su cui viene eseguito il server syslog nel campo Value.

6. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome
REG_SZ	Syslog_Protocol

Immettere il protocollo in uso sul server syslog, "tcp" o "udp", nel campo valore.

7. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome	Valore
DWORD	syslog_tls	1 o 0

Si noti che un valore "1" abilita syslog con TLS (Transport Layer Security) e un valore "0" disabilita syslog con TLS.

Garantire il corretto funzionamento di un server syslog esterno configurato

- Se la chiave è assente o ha un valore nullo:

- L’impostazione predefinita del protocollo è "tcp".
- L’impostazione predefinita della porta è "514" per "tcp/udp" e "6514" per TLS.
- Il livello syslog predefinito è 5 (LOG_NOTICE).

- Puoi confermare che syslog è attivato verificando che `syslog_enabled` il valore è "1". Quando il `syslog_enabled` Il valore è "1", dovrebbe essere possibile accedere al server remoto configurato indipendentemente dall’attivazione o meno della modalità EO.
- Se la modalità EO è impostata su "1" e si modifica la `syslog_enabled` valore compreso tra "1" e "0", vale quanto segue:
  - Non è possibile avviare il servizio se syslog non è abilitato in modalità EO.
  - Se il sistema è in esecuzione in modalità regolare, viene visualizzato un avviso che indica che syslog non può essere disattivato in modalità EO e che syslog è impostato con forza su "1", che è possibile vedere nel Registro di sistema. In questo caso, è necessario disattivare prima la modalità EO e poi disabilitare syslog.
- Se il server syslog non è in grado di funzionare correttamente quando la modalità EO e syslog sono attivati, il servizio si arresta. Questo può verificarsi per uno dei seguenti motivi:
  - È stato configurato un syslog_host non valido o non esistente.
  - È stato configurato un protocollo non valido tranne UDP o TCP.
  - Un numero di porta non è valido.
- Per una configurazione TCP o TLS su TCP, se il server non è in ascolto sulla porta IP, la connessione non riesce e il servizio si arresta.

Configurare l’autenticazione reciproca dei certificati X,509

L’autenticazione reciproca basata su certificati X,509 è possibile per la comunicazione SSL (Secure Sockets Layer) tra il connettore antivirus e ONTAP nel percorso di gestione. Se la modalità EO è attivata e il certificato non viene trovato, il connettore AV termina. Eseguire la seguente procedura sul connettore dell’antivirus:

Fasi

1. Il connettore antivirus ricerca il certificato client del connettore antivirus e il certificato dell’autorità di certificazione (CA) per il server NetApp nel percorso di directory da cui il connettore antivirus esegue la directory di installazione. Copiare i certificati in questo percorso di directory fisso.
2. Incorporare il certificato client e la relativa chiave privata nel formato PKCS12 e denominarlo "AV_client.P12".
3. Verificare che il certificato CA (insieme a qualsiasi autorità di firma intermedia fino alla CA principale) utilizzato per firmare il certificato per il server NetApp sia in formato PEM (Privacy Enhanced Mail) e denominato "ONTAP_CA.pem". Posizionarlo nella directory di installazione di Antivirus Connector. Sul sistema NetApp ONTAP, installare il certificato CA (insieme a qualsiasi autorità di firma intermedia fino alla CA principale) utilizzato per firmare il certificato client per il connettore antivirus in "ONTAP" come certificato di tipo "client-ca".

Configurare i pool di scanner

Panoramica sulla configurazione dei pool di scanner

Un pool di scanner definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. Un criterio dello scanner determina se un pool di scanner è attivo.

Se si utilizza un criterio di esportazione su un server SMB, è necessario aggiungere ciascun server Vscan al criterio di esportazione.

Creare un pool di scanner su un singolo cluster

Un pool di scanner definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. È possibile creare un pool di scanner per una singola SVM o per tutte le SVM in un cluster.

Di cosa hai bisogno

- I server SVM e Vscan devono trovarsi nello stesso dominio o in domini attendibili.
- Per i pool di scanner definiti per una singola SVM, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione SVM o la LIF dei dati SVM.
- Per i pool di scanner definiti per tutte le SVM in un cluster, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione del cluster.
- L'elenco degli utenti con privilegi deve includere l'account utente di dominio utilizzato dal server Vscan per connettersi a SVM.
- Una volta configurato il pool di scanner, controllare lo stato della connessione ai server.

Fasi

1. Creazione di un pool di scanner:

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

   - Specificare una SVM di dati per un pool definito per una singola SVM e specificare una SVM amministrativa del cluster per un pool definito per tutte le SVM in un cluster.
   - Specificare un indirizzo IP o un FQDN per ciascun nome host del server Vscan.
   - Specificare il dominio e il nome utente per ciascun utente con privilegi. Per un elenco completo delle opzioni, vedere la pagina man del comando.

     Il seguente comando crea un pool di scanner denominato `SP` su `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. Verificare che il pool di scanner sia stato creato:

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

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `SP` pool di scanner:

```
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
```

È inoltre possibile utilizzare `vserver vscan scanner-pool show` Per visualizzare tutti i pool di scanner su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

Creazione di pool di scanner nelle configurazioni MetroCluster

È necessario creare pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster, corrispondente alle SVM primarie e secondarie sul cluster.

Di cosa hai bisogno

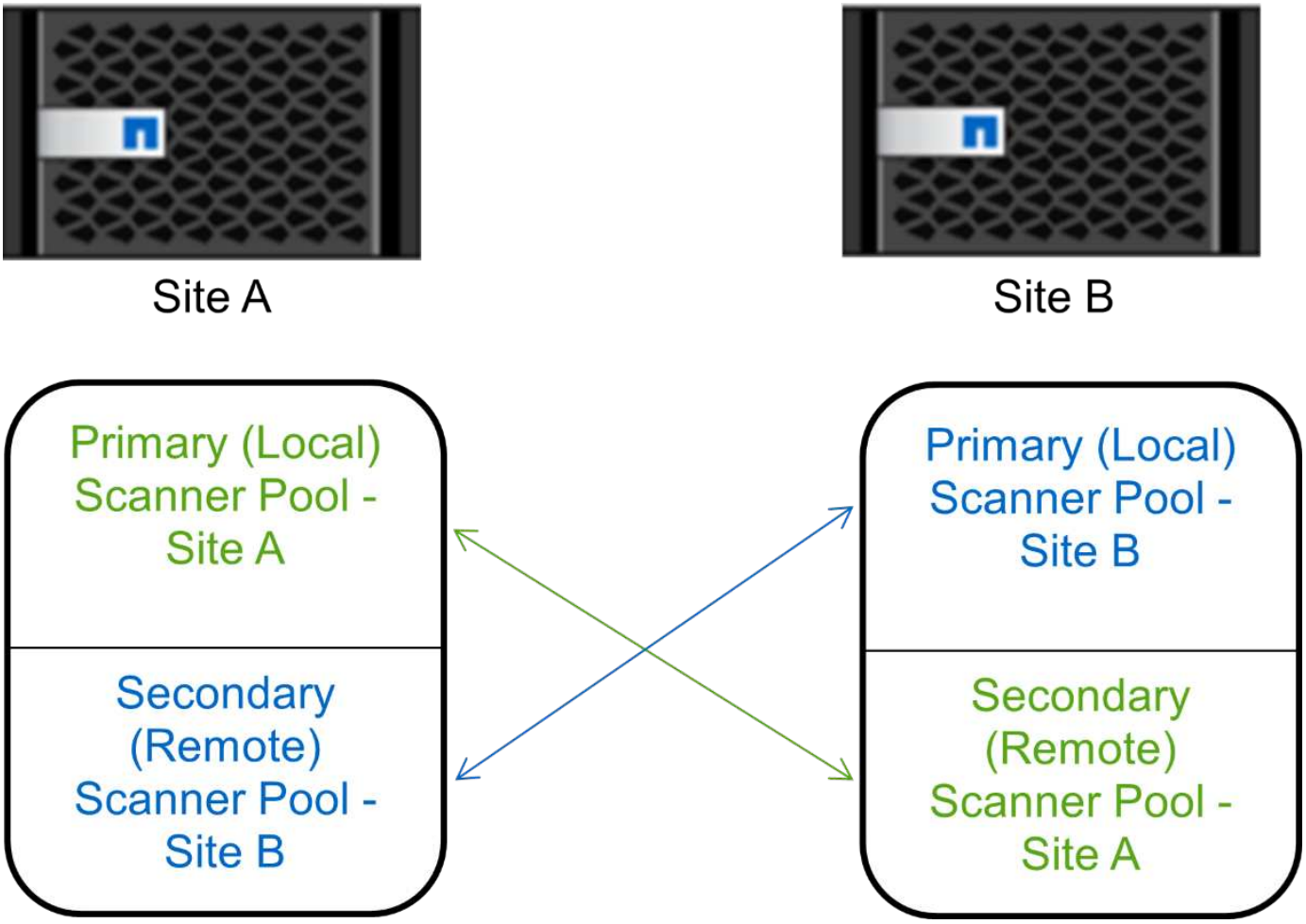
- I server SVM e Vscan devono trovarsi nello stesso dominio o in domini attendibili.
- Per i pool di scanner definiti per una singola SVM, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione SVM o la LIF dei dati SVM.
- Per i pool di scanner definiti per tutte le SVM in un cluster, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione del cluster.
- L'elenco degli utenti con privilegi deve includere l'account utente di dominio utilizzato dal server Vscan per connettersi a SVM.
- Una volta configurato il pool di scanner, controllare lo stato della connessione ai server.

A proposito di questa attività

Le configurazioni MetroCluster proteggono i dati implementando due cluster mirrorati fisicamente separati. Ciascun cluster replica in modo sincrono i dati e la configurazione SVM dell'altro. Una SVM primaria sul cluster locale serve i dati quando il cluster è online. Una SVM secondaria sul cluster locale serve i dati quando il cluster remoto non è in linea.

Ciò significa che è necessario creare pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster, il pool secondario diventa attivo quando il cluster inizia a servire i dati dalla SVM secondaria. Per il disaster recovery (DR), la configurazione è simile a quella di MetroCluster.

Questa figura mostra una tipica configurazione MetroCluster/DR.



Fasi

1. Creazione di un pool di scanner:

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

   - Specificare una SVM di dati per un pool definito per una singola SVM e specificare una SVM amministrativa del cluster per un pool definito per tutte le SVM in un cluster.
   - Specificare un indirizzo IP o un FQDN per ciascun nome host del server Vscan.
   - Specificare il dominio e il nome utente per ciascun utente con privilegi.

     È necessario creare tutti i pool di scanner dal cluster contenente la SVM primaria.

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   I seguenti comandi creano pool di scanner primari e secondari su ciascun cluster in una configurazione 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. Verificare che i pool di scanner siano stati creati:

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

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli del pool di scanner `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
```

   È inoltre possibile utilizzare `vserver vscan scanner-pool show` Per visualizzare tutti i pool di scanner su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

Applicare un criterio scanner a un singolo cluster

Un criterio dello scanner determina se un pool di scanner è attivo. È necessario attivare un pool di scanner prima che i server Vscan definiti possano connettersi a una SVM.

A proposito di questa attività

- È possibile applicare un solo criterio scanner a un pool di scanner.
- Se è stato creato un pool di scanner per tutte le SVM in un cluster, è necessario applicare un criterio di scanner a ciascuna SVM singolarmente.

Fasi

1. Applicare un criterio 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
   ```

   Un criterio dello scanner può avere uno dei seguenti valori:

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

     Nell'esempio seguente viene indicato il nome del pool di scanner `SP` su `vs1` SVM è attivo:

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

2. Verificare che il pool di scanner sia attivo:

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

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `SP` pool di scanner:

   ```
   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
   ```

È possibile utilizzare `vserver vscan scanner-pool show-active` Per visualizzare i pool di scanner attivi su una SVM. Per la sintassi completa del comando, vedere la pagina man del comando.

Applicare i criteri dello scanner nelle configurazioni MetroCluster

Un criterio dello scanner determina se un pool di scanner è attivo. È necessario applicare un criterio dello scanner ai pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster.

A proposito di questa attività

- È possibile applicare un solo criterio scanner a un pool di scanner.
- Se è stato creato un pool di scanner per tutte le SVM in un cluster, è necessario applicare un criterio di scanner a ciascuna SVM singolarmente.
- Per le configurazioni di disaster recovery e MetroCluster, è necessario applicare un criterio dello scanner a ogni pool di scanner nel cluster locale e nel cluster remoto.
- Nel criterio creato per il cluster locale, è necessario specificare il cluster locale in `cluster` parametro. Nel criterio creato per il cluster remoto, è necessario specificare il cluster remoto in `cluster` parametro. Il cluster remoto può quindi rilevare le operazioni di scansione dei virus in caso di disastro.

Fasi

1. Applicare un criterio 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`*

   Un criterio dello scanner può avere uno dei seguenti valori:

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

     È necessario applicare tutti i criteri dello scanner dal cluster contenente la SVM primaria.

   I seguenti comandi applicano i criteri dello scanner ai pool di scanner primari e secondari su ciascun cluster in una configurazione 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 pool2_for_site2 -scanner-policy primary -cluster cluster2

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

2. Verificare che il pool di scanner sia attivo:

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

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli del pool di scanner `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
```

   È possibile utilizzare `vserver vscan scanner-pool show-active` Per visualizzare i pool di scanner attivi su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

Comandi per la gestione dei pool di scanner

È possibile modificare ed eliminare i pool di scanner e gestire gli utenti con privilegi e i server Vscan per un pool di scanner. È inoltre possibile visualizzare informazioni riepilogative sul pool di scanner.

Se si desidera…	Immettere il seguente comando…
Modificare un pool di scanner	`vserver vscan scanner-pool modify`
Eliminare un pool di scanner	`vserver vscan scanner-pool delete`
Aggiungere utenti con privilegi a un pool di scanner	`vserver vscan scanner-pool privileged-users add`
Eliminare gli utenti con privilegi da un pool di scanner	`vserver vscan scanner-pool privileged-users remove`
Aggiungere server Vscan a un pool di scanner	`vserver vscan scanner-pool servers add`
Eliminare i server Vscan da un pool di scanner	`vserver vscan scanner-pool servers remove`
Visualizza riepilogo e dettagli di un pool di scanner	`vserver vscan scanner-pool show`
Visualizzare gli utenti con privilegi per un pool di scanner	`vserver vscan scanner-pool privileged-users show`
Visualizzare i server Vscan per tutti i pool di scanner	`vserver vscan scanner-pool servers show`

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Configurare la scansione on-access

Creare una policy di accesso

Un criterio di accesso definisce l'ambito di una scansione all'accesso. È possibile creare una policy di accesso per una singola SVM o per tutte le SVM in un cluster. Se è stata creata una policy di accesso per tutte le SVM in un cluster, è necessario attivare la policy su ogni SVM singolarmente.

A proposito di questa attività

- 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.
- 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.
- Per impostazione predefinita, ONTAP crea una policy di accesso denominata "default_CIFS" e la abilita per tutte le SVM in un cluster.
- Qualsiasi file idoneo per l'esclusione della scansione in base a. `paths-to-exclude`, `file-ext-to-exclude`, o. `max-file-size` i parametri non vengono presi in considerazione per la scansione, anche se `scan-mandatory` l'opzione è impostata su on. (Selezionare questa opzione "risoluzione dei problemi"

sezione per i problemi di connettività relativi a. `scan-mandatory` opzione).

- 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.
- La scansione virus non viene eseguita su una condivisione SMB per la quale il parametro Continuously-Available è impostato su Yes.
- Vedere "Architettura antivirus" Per ulteriori informazioni sul profilo *Vscan file-Operations*.
- È possibile creare un massimo di dieci (10) criteri di accesso per SVM. Tuttavia, è possibile attivare un solo criterio di accesso alla volta.
  - È possibile escludere un massimo di cento (100) percorsi ed estensioni di file dalla scansione virus in una policy di accesso.
- Alcuni consigli sull'esclusione dei file:
  - Considerare l'esclusione di file di grandi dimensioni (è possibile specificare le dimensioni del file) dalla scansione dei virus perché possono causare un rallentamento della risposta o timeout delle richieste di scansione per gli utenti CIFS. La dimensione predefinita del file per l'esclusione è 2 GB.
  - Considerare l'esclusione di estensioni di file come `.vhd` e. `.tmp` perché i file con queste estensioni potrebbero non essere appropriati per la scansione.
  - Considerare l'esclusione di percorsi di file come la directory di quarantena o i percorsi in cui sono memorizzati solo i dischi rigidi o i database virtuali.
  - Verificare che tutte le esclusioni siano specificate nello stesso criterio, in quanto è possibile attivare un solo criterio alla volta. NetApp consiglia di utilizzare lo stesso set di esclusioni specificato nel motore antivirus.
- Per un è necessario un criterio di accesso scansione su richiesta. Per evitare la scansione all'accesso per, è necessario impostare `-scan-files-with-no-ext` a false e. `-file-ext-to-exclude` a * per escludere tutte le estensioni.

Fasi

1. Creare una policy di accesso:

   ```
   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
   ```

   - Specificare una SVM di dati per una policy definita per una singola SVM, una SVM amministrativa del cluster per una policy definita per tutte le SVM in un cluster.
   - Il `-file-ext-to-exclude` l'impostazione ha la precedenza su `-file-ext-to-include` impostazione.
   - Impostare `-scan-files-with-no-ext` a true per eseguire la scansione dei file senza estensioni. Il comando seguente crea una policy di accesso denominata `Policy1` su `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. Verificare che il criterio di accesso sia stato creato: `vserver vscan on-access-policy show -instance` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`name`*

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `Policy1` policy:

```
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
```

Attivare un criterio di accesso

Un criterio di accesso definisce l’ambito di una scansione all’accesso. È necessario attivare un criterio di accesso su una SVM prima di poter eseguire la scansione dei relativi file.

Se è stata creata una policy di accesso per tutte le SVM in un cluster, è necessario attivare la policy su ogni SVM singolarmente. È possibile attivare un solo criterio di accesso su una SVM alla volta.

Fasi

1. Attivare una policy di accesso:

   ```
   vserver vscan on-access-policy enable -vserver data_SVM -policy-name
   policy_name
   ```

   Il comando seguente attiva un criterio di accesso denominato `Policy1` su `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. Verificare che il criterio di accesso sia attivato:

   `vserver vscan on-access-policy show -instance` *`data_SVM`* `-policy-name` *`policy_name`*

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `Policy1` policy di accesso:

```
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
```

Modificare il profilo delle operazioni del file Vscan per una condivisione SMB

Il *profilo delle operazioni del file Vscan* per una condivisione SMB definisce le operazioni sulla condivisione che possono attivare la scansione. Per impostazione predefinita, il parametro è impostato su `standard`. È possibile regolare il parametro in base alle necessità quando si crea o si modifica una condivisione SMB.

Vedere "Architettura antivirus" Per ulteriori informazioni sul profilo *Vscan file-Operations*.

> La scansione antivirus non viene eseguita su una condivisione SMB che dispone di `continuously-available` parametro impostato su `Yes`.

Fase

1. Modificare il valore del profilo delle operazioni del file Vscan per una condivisione SMB:

   `vserver cifs share modify -vserver` *`data_SVM`* `-share-name` *`share`* `-path` *`share_path`* `-vscan-fileop-profile no-scan|standard|strict|writes-only`

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando modifica il profilo delle operazioni del file Vscan per una condivisione SMB in `strict`:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

Comandi per la gestione delle policy di accesso

È possibile modificare, disattivare o eliminare un criterio di accesso. È possibile visualizzare un riepilogo e i dettagli della policy.

Se si desidera…	Immettere il seguente comando…
Creare una policy di accesso	`vserver vscan on-access-policy create`
Modificare un criterio di accesso	`vserver vscan on-access-policy modify`
Attivare un criterio di accesso	`vserver vscan on-access-policy enable`
Disattiva un criterio di accesso	`vserver vscan on-access-policy disable`
Eliminare un criterio di accesso	`vserver vscan on-access-policy delete`
Visualizza riepilogo e dettagli per una policy di accesso	`vserver vscan on-access-policy show`
Aggiungere all'elenco di percorsi da escludere	`vserver vscan on-access-policy paths-to-exclude add`
Eliminare dall'elenco dei percorsi da escludere	`vserver vscan on-access-policy paths-to-exclude remove`
Visualizzare l'elenco dei percorsi da escludere	`vserver vscan on-access-policy paths-to-exclude show`
Aggiungere all'elenco delle estensioni di file da escludere	`vserver vscan on-access-policy file-ext-to-exclude add`
Eliminare dall'elenco delle estensioni di file da escludere	`vserver vscan on-access-policy file-ext-to-exclude remove`

Visualizzare l'elenco delle estensioni di file da escludere	`vserver vscan on-access-policy file-ext-to-exclude show`
Aggiungere all'elenco delle estensioni di file da includere	`vserver vscan on-access-policy file-ext-to-include add`
Eliminare dall'elenco delle estensioni di file da includere	`vserver vscan on-access-policy file-ext-to-include remove`
Visualizzare l'elenco delle estensioni di file da includere	`vserver vscan on-access-policy file-ext-to-include show`

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Configurare la scansione on-demand

Configurare una panoramica della scansione on-demand

È possibile utilizzare la scansione on-demand per controllare i file alla ricerca di virus immediatamente o in base a una pianificazione.

Ad esempio, è possibile eseguire scansioni solo in ore non di punta oppure eseguire la scansione di file di grandi dimensioni esclusi da una scansione all'accesso. È possibile utilizzare una pianificazione cron per specificare quando eseguire l'attività.

A proposito di questo argomento

- È possibile assegnare una pianificazione quando si crea un'attività.
- È possibile pianificare una sola attività alla volta su una SVM.
- La scansione on-demand non supporta la scansione di collegamenti simbolici o file di flusso.

> La scansione on-demand non supporta la scansione di collegamenti simbolici o file di flusso.

> Per creare un'attività on-demand, è necessario abilitare almeno una policy di accesso. Può essere il criterio predefinito o un criterio di accesso creato dall'utente.

Crea un'attività on-demand

Un'attività su richiesta definisce l'ambito della scansione antivirus su richiesta. 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.

A proposito di questa attività

- È possibile eseguire un massimo di dieci (10) task on-demand per ogni SVM, ma è possibile attivarne solo una.

- Un'attività on-demand crea un report contenente informazioni relative alle statistiche relative alle scansioni. Questo report è accessibile con un comando o scaricando il file di report creato dall'attività nella posizione definita.

Prima di iniziare

- Devi avere creazione di un criterio di accesso. Il criterio può essere predefinito o creato dall'utente. Senza il criterio di accesso, non è possibile attivare la scansione.

Fasi

1. Crea un'attività on-demand:

   ```
   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
   ```

   - Il `-file-ext-to-exclude` l'impostazione ha la precedenza su `-file-ext-to-include` impostazione.
   - Impostare `-scan-files-with-no-ext` a true per eseguire la scansione dei file senza estensioni.

     Per un elenco completo delle opzioni, consultare la "riferimento al comando".

     Il seguente comando crea un'attività on-demand denominata `Task1` Sulla `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.
   ```

   +

   > È possibile utilizzare `job show` per visualizzare lo stato del lavoro. È possibile utilizzare `job pause` e. `job resume` comandi per mettere in pausa e riavviare il lavoro o l' `job stop` per terminare il lavoro.

2. Verificare che l'attività on-demand sia stata creata:

   ```
   vserver vscan on-demand-task show -instance data_SVM -task-name task_name
   ```

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `Task1` attività:

```
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: -
```

Al termine

Prima di pianificare l'esecuzione dell'operazione, è necessario attivare la scansione sulla SVM.

Pianificare un'attività on-demand

È possibile creare un'attività senza assegnare una pianificazione e utilizzare `vserver vscan on-demand-task schedule` comando per assegnare un programma o aggiungere un programma durante la creazione dell'attività.

A proposito di questa attività

La pianificazione assegnata con `vserver vscan on-demand-task schedule` il comando sovrascrive un programma già assegnato con `vserver vscan on-demand-task create` comando.

Fasi

1. Pianificare un'attività on-demand:

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

   Il seguente comando pianifica un'attività di accesso denominata `Task2` su `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.
```

Per visualizzare lo stato del lavoro, utilizzare `job show` comando. Il `job pause` e. `job resume` i comandi, rispettivamente mettere in pausa e riavviare il lavoro; la `job stop` il comando termina il lavoro.

2. Verificare che l'attività on-demand sia stata pianificata:

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `Task 2` attività:

```
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
```

Al termine

Prima di pianificare l'esecuzione dell'operazione, è necessario attivare la scansione sulla SVM.

Eseguire immediatamente un'attività on-demand

È possibile eseguire un'attività on-demand immediatamente, indipendentemente dal fatto che sia stata assegnata o meno una pianificazione.

Prima di iniziare

È necessario aver attivato la scansione su SVM.

Fase

1. Eseguire immediatamente un'attività on-demand:

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

   Il seguente comando esegue un'attività di accesso denominata `Task1` su `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.
```

> È possibile utilizzare `job show` per visualizzare lo stato del lavoro. È possibile utilizzare `job pause` e. `job resume` comandi per mettere in pausa e riavviare il lavoro o l' `job stop` per terminare il lavoro.

Comandi per la gestione delle attività on-demand

È possibile modificare, eliminare o annullare la pianificazione di un'attività on-demand. È possibile visualizzare un riepilogo e i dettagli dell'attività e gestire i report per l'attività.

Se si desidera…	Immettere il seguente comando…
Crea un'attività on-demand	`vserver vscan on-demand-task create`
Modificare un'attività on-demand	`vserver vscan on-demand-task modify`
Eliminare un'attività on-demand	`vserver vscan on-demand-task delete`
Eseguire un'attività on-demand	`vserver vscan on-demand-task run`
Pianificare un'attività on-demand	`vserver vscan on-demand-task schedule`
Annulla pianificazione di un'attività on-demand	`vserver vscan on-demand-task unschedule`
Visualizza riepilogo e dettagli per un'attività on-demand	`vserver vscan on-demand-task show`
Visualizza report on-demand	`vserver vscan on-demand-task report show`
Elimina i report on-demand	`vserver vscan on-demand-task report delete`

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Procedure consigliate per la configurazione della funzionalità antivirus off-box in ONTAP

Prendere in considerazione i seguenti consigli per configurare la funzionalità off-box in ONTAP.

- Limitare gli utenti con privilegi alle operazioni di scansione antivirus. Gli utenti normali devono essere scoraggiati dall'utilizzo di credenziali utente con privilegi. Questa restrizione può essere ottenuta disattivando i diritti di accesso per gli utenti con privilegi in Active Directory.
- Gli utenti con privilegi non devono far parte di alcun gruppo di utenti con un elevato numero di diritti nel dominio, ad esempio il gruppo Administrators o il gruppo di operatori di backup. Gli utenti con privilegi devono essere convalidati solo dal sistema di archiviazione in modo che possano creare connessioni al server Vscan e accedere ai file per la scansione antivirus.
- Utilizzare i computer su cui sono in esecuzione i server Vscan solo a scopo di scansione antivirus. Per scoraggiare l'uso generale, disattivare i servizi terminal di Windows e altre disposizioni di accesso remoto su questi computer e concedere il diritto di installare nuovo software su questi computer solo agli amministratori.
- Dedicare i server Vscan alla scansione antivirus e non utilizzarli per altre operazioni, ad esempio i backup. Si potrebbe decidere di eseguire il server Vscan come macchina virtuale (VM). Se si esegue il server Vscan come macchina virtuale, assicurarsi che le risorse assegnate alla macchina virtuale non siano condivise e siano sufficienti per eseguire la scansione antivirus.
- Fornire CPU, memoria e capacità del disco adeguate al server Vscan per evitare un'allocazione eccessiva delle risorse. La maggior parte dei server Vscan è progettata per utilizzare più server core CPU e per distribuire il carico tra le CPU.
- NetApp consiglia di utilizzare una rete dedicata con una VLAN privata per la connessione dalla SVM al server Vscan, in modo che il traffico di scansione non sia influenzato da altro traffico di rete client. Creare una scheda di interfaccia di rete (NIC) separata dedicata alla VLAN antivirus sul server Vscan e alla LIF dati sulla SVM. Questo passaggio semplifica l'amministrazione e la risoluzione dei problemi in caso di problemi di rete. Il traffico antivirus deve essere segregato utilizzando una rete privata. Il server antivirus deve essere configurato per comunicare con il controller di dominio (DC) e ONTAP in uno dei seguenti modi:
  - Il controller di dominio deve comunicare con i server antivirus tramite la rete privata utilizzata per separare il traffico.
  - Il DC e il server antivirus devono comunicare attraverso una rete diversa (non la rete privata menzionata in precedenza), che non è la stessa della rete client CIFS.
  - Per attivare l'autenticazione Kerberos per la comunicazione antivirus, creare una voce DNS per la LIF privata e un nome dell'entità di servizio sul controller di dominio corrispondente alla voce DNS creata per la LIF privata. Usare questo nome quando si aggiunge una LIF al connettore antivirus. Il DNS dovrebbe essere in grado di restituire un nome univoco per ogni LIF privato collegato al connettore antivirus.

> Se la LIF per il traffico Vscan è configurata su una porta diversa dalla LIF per il traffico client, in caso di guasto a una porta la LIF Vscan potrebbe essere sottoposta a failover su un altro nodo. La modifica rende il server Vscan non raggiungibile dal nuovo nodo e le notifiche di scansione per le operazioni sui file sul nodo non riescono. Verificare che il server Vscan sia raggiungibile tramite almeno una LIF su un nodo in modo da poter elaborare le richieste di scansione per le operazioni su file eseguite su quel nodo.

- Collegare il sistema storage NetApp e il server Vscan utilizzando almeno una rete 1GbE.
- Per un ambiente con più server Vscan, collegare tutti i server con connessioni di rete simili ad alte prestazioni. La connessione dei server Vscan migliora le performance consentendo la condivisione del carico.
- Per i siti remoti e le filiali, NetApp consiglia di utilizzare un server Vscan locale piuttosto che un server Vscan remoto, poiché il primo è il candidato ideale per ottenere una latenza elevata. Se il costo è un fattore, utilizzare un notebook o un PC per una protezione antivirus moderata. È possibile pianificare scansioni periodiche e complete del file system condividendo i volumi o i qtree ed eseguendone la scansione da qualsiasi sistema del sito remoto.
- Utilizzare più server Vscan per eseguire la scansione dei dati sulla SVM a scopo di bilanciamento del carico e ridondanza. La quantità di carico di lavoro CIFS e il conseguente traffico antivirus varia in base alla SVM. Monitorare la latenza di scansione virus e CIFS sullo storage controller. Monitorare l'andamento dei risultati nel tempo. Se la latenza CIFS e la latenza della scansione virus aumentano a causa delle code della CPU o delle applicazioni sui server Vscan oltre le soglie di trend, i client CIFS potrebbero riscontrare lunghi tempi di attesa. Aggiungere altri server Vscan per distribuire il carico.
- Installare la versione più recente del connettore antivirus ONTAP.
- Mantenere aggiornati i motori e le definizioni antivirus. Consulta i partner per consigli sulla frequenza di aggiornamento.
- In un ambiente multi-tenancy, è possibile condividere un pool di scanner (pool di server Vscan) con più SVM, a condizione che i server Vscan e le SVM facciano parte dello stesso dominio o dominio attendibile.
- Il criterio del software antivirus per i file infetti deve essere impostato su "elimina" o "quarantena", che è il valore predefinito impostato dalla maggior parte dei fornitori di antivirus. Se "vscan-fileop-profile" è impostato su "write_only" e se viene trovato un file infetto, il file rimane nella condivisione e può essere aperto perché l'apertura di un file non attiva una scansione. La scansione antivirus viene attivata solo dopo la chiusura del file.
- Il `scan-engine timeout` il valore deve essere inferiore a. `scanner-pool request-timeout` valore. Se è impostato su un valore più alto, l'accesso ai file potrebbe subire un ritardo e alla fine potrebbe scadere. Per evitare questo problema, configurare `scan-engine timeout` a 5 secondi in meno di `scanner-pool request-timeout` valore. Fare riferimento alla documentazione del fornitore del motore di scansione per le istruzioni su come cambiare `scan-engine timeout` impostazioni. Il `scanner-pool timeout` può essere modificato utilizzando il seguente comando in modalità avanzata e fornendo il valore appropriato per `request-timeout` parametro: `vserver vscan scanner-pool modify`.
- Per un ambiente dimensionato per i carichi di lavoro di scansione ad accesso e che richiede l'utilizzo di una scansione su richiesta, NetApp consiglia di pianificare il lavoro di scansione su richiesta in orari non di punta per evitare carichi aggiuntivi sull'infrastruttura antivirus esistente.

Scopri di più sulle Best practice specifiche per i partner all'indirizzo "Soluzioni partner di Vscan".

Abilitare la scansione virus su una SVM

È necessario attivare la scansione virus su una SVM prima di eseguire una scansione on-access o on-demand.

Fasi

1. Abilitare la scansione virus su una SVM:

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

È possibile utilizzare `vserver vscan disable` comando per disattivare la scansione virus, se necessario.

Il seguente comando attiva la scansione virus su `vs1` SVM:

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

2. Verificare che la scansione virus sia attivata su SVM:

   `vserver vscan show -vserver data_SVM`

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza lo stato Vscan di `vs1` SVM:

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

                          Vserver: vs1
                     Vscan Status: on
```

Ripristinare lo stato dei file sottoposti a scansione

Talvolta, è possibile ripristinare lo stato di scansione dei file sottoposti a scansione su una SVM utilizzando `vserver vscan reset` per eliminare le informazioni memorizzate nella cache per i file. È possibile utilizzare questo comando per riavviare l'elaborazione della scansione virus, ad esempio in caso di una scansione non configurata correttamente.

A proposito di questa attività

Dopo aver eseguito il `vserver vscan reset` comando, tutti i file idonei verranno sottoposti a scansione al successivo accesso.

Questo comando può influire negativamente sulle prestazioni, a seconda del numero e delle dimensioni dei file da ripetere.

Prima di iniziare

Per questa attività sono richiesti privilegi avanzati.

Fasi

1. Passare al livello di privilegio avanzato:

   `set -privilege advanced`

2. Ripristinare lo stato dei file sottoposti a scansione:

   `vserver vscan reset -vserver data_SVM`

Il seguente comando ripristina lo stato dei file sottoposti a scansione su `vs1` SVM:

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

Visualizzare le informazioni del registro eventi di Vscan

È possibile utilizzare `vserver vscan show-events` Comando per visualizzare le informazioni del registro eventi relative ai file infetti, agli aggiornamenti dei server Vscan e simili. È possibile visualizzare le informazioni sugli eventi per il cluster o per dati nodi, SVM o server Vscan.

Prima di iniziare

Per visualizzare il registro eventi Vscan sono necessari privilegi avanzati.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Visualizzare le informazioni del registro eventi di Vscan:

   ```
   vserver vscan show-events
   ```

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il comando seguente visualizza le informazioni del registro eventi per il 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.
   ```

Monitoraggio e risoluzione dei problemi di connettività

Potenziali problemi di connettività che coinvolgono l'opzione di scansione obbligatoria

È possibile utilizzare `vserver vscan connection-status show` Comandi per visualizzare informazioni sulle connessioni del server Vscan che potrebbero essere utili per la risoluzione dei problemi di connettività.

Per impostazione predefinita, il `scan-mandatory` L'opzione per la scansione all'accesso nega l'accesso ai file quando non è disponibile una connessione al server Vscan per la scansione. Sebbene questa opzione offra importanti funzioni di sicurezza, può causare problemi in alcune situazioni.

- Prima di abilitare l'accesso client, è necessario assicurarsi che almeno un server Vscan sia connesso a una SVM su ciascun nodo che dispone di una LIF. Se è necessario connettere i server alle SVM dopo aver attivato l'accesso client, è necessario disattivare `scan-mandatory` Opzione su SVM per garantire che l'accesso al file non venga negato perché non è disponibile una connessione al server Vscan. È possibile riattivare l'opzione dopo aver collegato il server.
- Se una LIF di destinazione ospita tutte le connessioni del server Vscan per una SVM, la connessione tra il server e la SVM andrà persa se la LIF viene migrata. Per garantire che l'accesso al file non venga negato perché non è disponibile una connessione al server Vscan, è necessario disattivare `scan-mandatory` Prima di migrare LIF. È possibile riattivare l'opzione dopo la migrazione del LIF.

A ciascuna SVM devono essere assegnati almeno due server Vscan. Si consiglia di collegare i server Vscan al sistema storage su una rete diversa da quella utilizzata per l'accesso client.

Comandi per visualizzare lo stato di connessione del server Vscan

È possibile utilizzare `vserver vscan connection-status show` Comandi per visualizzare informazioni riepilogative e dettagliate sullo stato di connessione del server Vscan.

Se si desidera…	Immettere il seguente comando…
Visualizza un riepilogo delle connessioni del server Vscan	`vserver vscan connection-status show`
Visualizza i dettagli delle connessioni al server Vscan	`vserver vscan connection-status show-all`
Visualizza i dettagli dei server Vscan connessi	`vserver vscan connection-status show-connected`
Visualizza i dettagli dei server Vscan disponibili non connessi	`vserver vscan connection-status show-not-connected`

Per ulteriori informazioni su questi comandi, consultare la "Pagine man di ONTAP".

Risolvere i problemi relativi alla scansione antivirus

Per i problemi più comuni di scansione dei virus, esistono possibili cause e modi per

risolverli. La scansione dei virus è nota anche come Vscan.

Problema	Come risolverlo
I server Vscan non sono in grado di connettersi a. Il sistema storage Clustered ONTAP.	Verificare se la configurazione del pool di scanner specifica l'indirizzo IP del server Vscan. Controllare inoltre se gli utenti con privilegi consentiti nell'elenco dei pool di scanner sono attivi. Per controllare il pool di scanner, eseguire `vserver vscan scanner-pool show` al prompt dei comandi del sistema di storage. Se i server Vscan non riescono ancora a connettersi, potrebbe esserci un problema di rete.
I client osservano una latenza elevata.	È probabilmente giunto il momento di aggiungere altri server Vscan al pool di scanner.
Troppe scansioni attivate.	Modificare il valore di `vscan-fileop-profile` parametro per limitare il numero di operazioni sui file monitorate per la scansione antivirus.
Alcuni file non vengono sottoposti a scansione.	Verificare la policy di accesso. È possibile che il percorso di questi file sia stato aggiunto all'elenco di esclusione del percorso o che la loro dimensione superi il valore configurato per le esclusioni. Per verificare il criterio di accesso, eseguire `vserver vscan on-access-policy show` al prompt dei comandi del sistema di storage.
Accesso al file negato.	Controllare se l'impostazione *scan-Mandatory* è specificata nella configurazione dei criteri. Questa impostazione nega l'accesso ai dati se non sono connessi server Vscan. Modificare l'impostazione come necessario.

Monitorare lo stato e le attività delle performance

È possibile monitorare gli aspetti critici del modulo Vscan, ad esempio lo stato di connessione del server Vscan, Lo stato dei server Vscan e il numero di file sottoposti a scansione. Queste informazioni sono utili Si diagnosticano i problemi relativi al server Vscan.

Visualizzare le informazioni di connessione del server Vscan

È possibile visualizzare lo stato di connessione dei server Vscan per gestire le connessioni già in uso e le connessioni disponibili per l'utilizzo. I vari comandi visualizzano informazioni Informazioni sullo stato di connessione dei server Vscan.

Comando…	Informazioni visualizzate…

`vserver vscan connection-status show`	Riepilogo dello stato della connessione
`vserver vscan connection-status show-all`	Informazioni dettagliate sullo stato della connessione
`vserver vscan connection-status show-not-connected`	Stato delle connessioni disponibili ma non connesse
`vserver vscan connection-status show-connected`	Informazioni sul server Vscan collegato

Per ulteriori informazioni su questi comandi, consultare la "Riferimento al comando ONTAP".

Visualizzare le statistiche del server Vscan

È possibile visualizzare le statistiche specifiche del server Vscan per monitorare le prestazioni e diagnosticare i problemi relativi a. scansione virus. È necessario raccogliere un campione di dati prima di poter utilizzare `statistics show` comando a. Visualizzare le statistiche del server Vscan. Per completare un campione di dati, completare la seguente fase:

Fase

1. Eseguire `statistics start` e il `optional statistics` comando di arresto.

Visualizzare le statistiche per le richieste e le latenze del server Vscan

È possibile utilizzare ONTAP `offbox_vscan` Contatori per SVM per monitorare la velocità di Vscan Le richieste del server inviate e ricevute al secondo e le latenze del server in tutte le Vscan server. Per visualizzare queste statistiche, completare la seguente fase:

Fase

1. Eseguire la visualizzazione delle statistiche `object offbox_vscan –instance SVM` con il contatori seguenti:

Contatore…	Informazioni visualizzate…
`scan_request_dispatched_rate`	Numero di richieste di scansione virus inviate da ONTAP ai server Vscan al secondo
`scan_noti_received_rate`	Numero di richieste di scansione virus ricevute da ONTAP dai server Vscan al secondo
`dispatch_latency`	Latenza all'interno di ONTAP per identificare un server Vscan disponibile e inviare la richiesta a tale server Vscan
`scan_latency`	Latenza di andata e ritorno da ONTAP al server Vscan, compreso il tempo di esecuzione della scansione

Esempio di statistiche generate da un contatore vscan ONTAP offbox

```
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
-------------------------------------------------------------------
```

Visualizzare le statistiche per le singole richieste e latenze del server Vscan

È possibile utilizzare ONTAP `offbox_vscan_server` Contatori su un server Vscan per-SVM, per-off-box, E per nodo per monitorare il tasso di richieste del server Vscan inviate e la latenza del server su Ciascun server Vscan singolarmente. Per raccogliere queste informazioni, completare la seguente fase:

Fase

1. Eseguire `statistics show –object offbox_vscan –instance SVM:servername:nodename` comando con i seguenti contatori:

Contatore…	Informazioni visualizzate…
`scan_request_dispatched_rate`	Numero di richieste di scansione virus inviate da ONTAP
`scan_latency`	Latenza di andata e ritorno da ONTAP al server Vscan, compreso il tempo di esecuzione della scansione Ai server Vscan al secondo

Esempio di statistiche generate da un contatore 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
-------------------------------------------------------------------
```

Visualizzare le statistiche per l'utilizzo del server Vscan

È anche possibile utilizzare ONTAP `offbox_vscan_server` Contatori per raccogliere l'utilizzo del server Vscan statistiche. Queste statistiche vengono monitorate per SVM, per server Vscan off-box e per nodo. Loro Includere l'utilizzo della CPU sul server Vscan, la profondità della coda per le operazioni di scansione sul server Vscan (corrente e massima), memoria utilizzata e rete utilizzata. Queste statistiche vengono inoltrate dal connettore antivirus ai contatori delle statistiche all'interno di ONTAP. Loro sono basati su dati che vengono interrogati ogni 20 secondi e devono essere raccolti più volte per la precisione; in caso contrario, i valori visualizzati nelle statistiche riflettono solo l'ultimo polling. L'utilizzo della CPU e le code sono particolarmente importante per il monitoraggio e l'analisi. Un valore elevato per una coda media può indicare che Il server Vscan presenta un collo di bottiglia. Per raccogliere le statistiche di utilizzo per il server Vscan su un server Vscan per SVM, per server Vscan e per nodo di base, completare il seguente passaggio:

Fase

1. Raccogliere le statistiche di utilizzo per il server Vscan

   Eseguire `statistics show –object offbox_vscan_server –instance SVM:servername:nodename` con i seguenti comandi `offbox_vscan_server` contatori:

Contatore…	Informazioni visualizzate…
`scanner_stats_pct_cpu_used`	Utilizzo della CPU sul server Vscan
`scanner_stats_pct_input_queue_avg`	Coda media di richieste di scansione sul server Vscan
`scanner_stats_pct_input_queue_hiwaterma rk`	Coda di picco delle richieste di scansione sul server Vscan
`scanner_stats_pct_mem_used`	Memoria utilizzata sul server Vscan
`scanner_stats_pct_network_used`	Rete utilizzata sul server Vscan

Esempio di statistiche di utilizzo per il server 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
---------------------------------------------------------------
```