Installazione e configurazione del server Vscan

ONTAP 9

NetApp
April 24, 2024

Sommario

Installazione e configurazione del server Vscan 1
Installazione e configurazione del server Vscan 1
Installare il connettore antivirus ONTAP 1
Configurare il connettore antivirus ONTAP 4

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".