



Configurare la scansione on-access

ONTAP 9

NetApp
April 24, 2024

Sommario

- Configurare la scansione on-access 1
 - Creare una policy di accesso 1
 - Attivare un criterio di accesso 3
 - Modificare il profilo delle operazioni del file Vscan per una condivisione SMB 4
 - Comandi per la gestione delle policy di accesso 4

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	<code>vserver vscan on-access-policy create</code>
Modificare un criterio di accesso	<code>vserver vscan on-access-policy modify</code>
Attivare un criterio di accesso	<code>vserver vscan on-access-policy enable</code>
Disattiva un criterio di accesso	<code>vserver vscan on-access-policy disable</code>
Eliminare un criterio di accesso	<code>vserver vscan on-access-policy delete</code>

Visualizza riepilogo e dettagli per una policy di accesso	<code>vserver vscan on-access-policy show</code>
Aggiungere all'elenco di percorsi da escludere	<code>vserver vscan on-access-policy paths-to-exclude add</code>
Eliminare dall'elenco dei percorsi da escludere	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
Visualizzare l'elenco dei percorsi da escludere	<code>vserver vscan on-access-policy paths-to-exclude show</code>
Aggiungere all'elenco delle estensioni di file da escludere	<code>vserver vscan on-access-policy file-ext-to-exclude add</code>
Eliminare dall'elenco delle estensioni di file da escludere	<code>vserver vscan on-access-policy file-ext-to-exclude remove</code>
Visualizzare l'elenco delle estensioni di file da escludere	<code>vserver vscan on-access-policy file-ext-to-exclude show</code>
Aggiungere all'elenco delle estensioni di file da includere	<code>vserver vscan on-access-policy file-ext-to-include add</code>
Eliminare dall'elenco delle estensioni di file da includere	<code>vserver vscan on-access-policy file-ext-to-include remove</code>
Visualizzare l'elenco delle estensioni di file da includere	<code>vserver vscan on-access-policy file-ext-to-include show</code>

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

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.