On-Access-Scan konfigurieren

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/antivirus/create-on-access-policy-task.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

On-Access-Scan konfigurieren . . . 1
ONTAP Vscan On-Access-Richtlinien erstellen . . . 1
ONTAP Vscan On-Access-Richtlinien aktivieren . . . 3
Das ONTAP Vscan Dateioperationsprofil für SMB-Freigaben anpassen . . . 4
ONTAP Vscan Befehle zur Verwaltung von On-Access-Richtlinien . . . 4

On-Access-Scan konfigurieren

ONTAP Vscan On-Access-Richtlinien erstellen

Eine On-Access-Richtlinie definiert den Umfang eines On-Access-Scans. Es kann eine On-Access-Richtlinie für eine einzelne SVM oder für alle SVMs in einem Cluster erstellt werden. Wenn Sie eine On-Access-Richtlinie für alle SVMs in einem Cluster erstellt haben, muss die Richtlinie auf jeder SVM einzeln aktiviert werden.

Über diese Aufgabe

- Sie können die maximale Dateigröße für den Scan, die Dateierweiterungen und Pfade, die in den Scan einbezogen werden sollen, sowie die Dateierweiterungen und Pfade, die vom Scan ausgeschlossen werden sollen, angeben.
- Sie können die Option `scan-mandatory`auf „off“ setzen, um festzulegen, dass Dateizugriff erlaubt ist, wenn keine Vscan-Server für die Virenprüfung verfügbar sind.
- Standardmäßig erstellt ONTAP eine On-Access-Richtlinie mit dem Namen "default_CIFS" und aktiviert sie für alle SVMs in einem Cluster.
- Jede Datei, die aufgrund der `paths-to-exclude`, `file-ext-to-exclude` oder `max-file-size` Parameter für den Scan ausgeschlossen wird, wird nicht für das Scannen berücksichtigt, selbst wenn die `scan-mandatory` Option auf „Ein“ gesetzt ist. (In diesem "Fehlerbehebung" Abschnitt finden sich Hinweise zu Verbindungsproblemen im Zusammenhang mit der `scan-mandatory` Option.)
- Standardmäßig werden nur Lese-/Schreib-Volumes gescannt. Es können Filter festgelegt werden, die das Scannen von schreibgeschützten Volumes ermöglichen oder das Scannen auf Dateien beschränken, die mit Ausführungsrechten geöffnet wurden.
- Bei einer SMB-Freigabe, für die der Parameter "ständig verfügbar" auf "Ja" gesetzt ist, wird keine Virenprüfung durchgeführt.
- Einzelheiten zum Abschnitt "Antivirus Architektur" bezüglich des *Vscan file-operations profile*.
- Sie können maximal zehn (10) On-Access-Richtlinien pro SVM erstellen. Es kann jedoch immer nur eine On-Access-Richtlinie gleichzeitig aktiviert werden.
  - Sie können in einer On-Access-Richtlinie maximal einhundert (100) Pfade und Dateierweiterungen von der Virenprüfung ausschließen.
- Einige Empfehlungen zum Ausschluss von Dateien:
  - Es kann sinnvoll sein, große Dateien (die Dateigröße kann festgelegt werden) vom Virenscan auszuschließen, da dies bei CIFS-Benutzern zu langsamen Reaktionszeiten oder Zeitüberschreitungen bei Scan-Anfragen führen kann. Die Standarddateigröße für den Ausschluss beträgt 2GB.
  - Es kann sinnvoll sein, Dateiendungen wie `.vhd` und `.tmp` auszuschließen, da Dateien mit diesen Endungen möglicherweise nicht für das Scannen geeignet sind.
  - Es kann sinnvoll sein, Dateipfade wie das Quarantäneverzeichnis oder Pfade, in denen nur virtuelle Festplatten oder Datenbanken gespeichert sind, auszuschließen.
  - Stellen Sie sicher, dass alle Ausnahmen in derselben Richtlinie definiert sind, da immer nur eine Richtlinie gleichzeitig aktiviert sein kann. NetApp empfiehlt dringend, dass dieselben Ausnahmen in der Antiviren-Engine festgelegt werden.
  - Ab ONTAP 9.14.1 können Sie Wildcards verwenden, um Zugriffs-Pfade und Dateierweiterungen anzugeben, die ausgeschlossen werden sollen.

- Für eine On-Demand Scan-Zugriffsrichtlinie ist eine Richtlinie beim Zugriff erforderlich. Um das Scannen beim Zugriff zu vermeiden, sollte `-scan-files-with-no-ext` auf false und `-file-ext-to-exclude` auf * gesetzt werden, um alle Erweiterungen auszuschließen.

Schritte

1. Eine On-Access-Richtlinie erstellen:

   `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`

   - Eine Daten-SVM ist für eine Richtlinie anzugeben, die für eine einzelne SVM definiert ist, eine Cluster-Admin-SVM für eine Richtlinie, die für alle SVMs in einem Cluster definiert ist.
   - Die `-file-ext-to-exclude`Einstellung überschreibt die `-file-ext-to-include`Einstellung.
   - Set `-scan-files-with-no-ext` auf „true“, um Dateien ohne Dateiendung zu scannen. Der folgende Befehl erstellt eine On-Access-Richtlinie mit dem Namen `Policy1` auf der `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. Es wird überprüft, ob die On-Access-Richtlinie erstellt wurde: `vserver vscan on-access-policy show -instance` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`name`*

   Weitere Informationen zu `vserver vscan on-access-policy` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die Details für die `Policy1`Richtlinie an:

```
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
```

ONTAP Vscan On-Access-Richtlinien aktivieren

Eine On-Access-Richtlinie definiert den Umfang eines On-Access-Scans. Eine On-Access-Richtlinie muss auf einer SVM aktiviert werden, bevor deren Dateien gescannt werden können.

Wenn Sie eine On-Access-Richtlinie für alle SVMs in einem Cluster erstellt haben, muss die Richtlinie auf jeder SVM einzeln aktiviert werden. Auf einer SVM kann jeweils nur eine On-Access-Richtlinie aktiviert werden.

Schritte

1. Eine On-Access-Richtlinie aktivieren:

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

   Der folgende Befehl aktiviert eine On-Access-Richtlinie namens `Policy1` auf der `vs1` SVM:

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

2. Es sollte überprüft werden, ob die On-Access-Richtlinie aktiviert ist:

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

   Weitere Informationen zu `vserver vscan on-access-policy show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die Details der `Policy1`On-Access-Richtlinie an:

   ```
   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
```

Das ONTAP Vscan Dateioperationsprofil für SMB-Freigaben anpassen

Das *Vscan-Dateioperationsprofil* für eine SMB-Freigabe definiert die Operationen auf der Freigabe, die einen Scan auslösen können. Standardmäßig ist der Parameter auf `standard` gesetzt. Der Parameter kann bei Bedarf angepasst werden, wenn eine SMB-Freigabe erstellt oder geändert wird.

Einzelheiten zum Abschnitt "Antivirus Architektur" bezüglich des *Vscan file-operations profile*.

> Die Virenprüfung wird auf einer SMB-Freigabe, bei der der `continuously-available` Parameter auf `Yes` gesetzt ist, nicht durchgeführt.

Schritt

1. Den Wert des Vscan Dateioperationsprofils für eine SMB-Freigabe anpassen:

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

   Weitere Informationen zu `vserver cifs share modify` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl ändert das Vscan-Dateioperationsprofil für eine SMB-Freigabe zu `strict`:

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

ONTAP Vscan Befehle zur Verwaltung von On-Access-Richtlinien

Sie können eine On-Access-Richtlinie ändern, deaktivieren oder löschen. Eine Zusammenfassung und Details zur Richtlinie sind einsehbar.

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Eine On-Access-Richtlinie erstellen	`vserver vscan on-access-policy create`
Eine On-Access-Richtlinie ändern	`vserver vscan on-access-policy modify`
Eine On-Access-Richtlinie aktivieren	`vserver vscan on-access-policy enable`
Eine On-Access-Richtlinie deaktivieren	`vserver vscan on-access-policy disable`
Eine On-Access-Richtlinie löschen	`vserver vscan on-access-policy delete`
Zusammenfassung und Details zu einer On-Access-Richtlinie anzeigen	`vserver vscan on-access-policy show`

Zur Liste der auszuschließenden Pfade hinzufügen	`vserver vscan on-access-policy paths-to-exclude add`
Aus der Liste der auszuschließenden Pfade löschen	`vserver vscan on-access-policy paths-to-exclude remove`
Liste der auszuschließenden Pfade anzeigen	`vserver vscan on-access-policy paths-to-exclude show`
Zur Liste der auszuschließenden Dateierweiterungen hinzufügen	`vserver vscan on-access-policy file-ext-to-exclude add`
Aus der Liste der auszuschließenden Dateierweiterungen entfernen	`vserver vscan on-access-policy file-ext-to-exclude remove`
Liste der auszuschließenden Dateierweiterungen anzeigen	`vserver vscan on-access-policy file-ext-to-exclude show`
Zur Liste der einzuschließenden Dateierweiterungen hinzufügen	`vserver vscan on-access-policy file-ext-to-include add`
Aus der Liste der einzuschließenden Dateierweiterungen entfernen	`vserver vscan on-access-policy file-ext-to-include remove`
Liste der einzuschließenden Dateierweiterungen anzeigen	`vserver vscan on-access-policy file-ext-to-include show`

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.