



Konfigurieren Sie das Scannen beim Zugriff

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

- Konfigurieren Sie das Scannen beim Zugriff 1
 - Erstellen einer Zugriffsrichtlinie 1
 - Aktivieren einer Zugriffsrichtlinie 2
 - Ändern Sie das Vscan-Dateibetriebsprofil für eine SMB-Freigabe 3
 - Befehle zum Managen von Zugriffsrichtlinien 4

Konfigurieren Sie das Scannen beim Zugriff

Erstellen einer Zugriffsrichtlinie

Eine Zugriffsrichtlinie definiert den Umfang eines Scans beim Zugriff. Sie können die maximale Größe der zu scannenden Dateien, die Erweiterungen der Dateien, die in den Scan aufgenommen werden sollen, sowie die Erweiterungen und Pfade der Dateien angeben, die vom Scan ausgeschlossen werden sollen. Sie können eine On-Access-Richtlinie für eine einzelne SVM oder für alle SVMs in einem Cluster erstellen.

Über diese Aufgabe

ONTAP erstellt standardmäßig eine Zugriffsrichtlinie mit dem Namen „default_CIFS“ und ermöglicht sie für alle SVMs in einem Cluster.

Sie können die einstellen `scan-mandatory` Option „aus“, um festzulegen, dass der Dateizugriff zulässig ist, wenn keine Vscan-Server für Virenprüfungen verfügbar sind. Beachten Sie, dass alle Dateien, die für den Scan-Ausschluss auf Basis des qualifiziert sind `paths-to-exclude`, `file-ext-to-exclude`, Oder `max-file-size` Parameter werden nicht für das Scannen berücksichtigt, auch wenn der `scan-mandatory` Die Option ist auf ein eingestellt.



Für potenzielle Probleme im Zusammenhang mit dem `scan-mandatory` Option, siehe [Mögliche Verbindungsprobleme bei der Option „Scannen erforderlich“](#).

Standardmäßig werden nur Lese- und Schreib-Volumes gescannt. Sie können Filter festlegen, die das Scannen von schreibgeschützten Volumes ermöglichen oder das Scannen auf Dateien beschränken, die mit dem Zugriff ausführen geöffnet wurden.

Schritte

1. Erstellen einer Richtlinie für den Zugriff:

```
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
```

- Legen Sie eine Daten-SVM für eine Richtlinie fest, die für eine einzelne SVM, einen Cluster-Admin-SVM für eine Richtlinie festgelegt ist, die für alle SVMs in einem Cluster definiert ist.
- Der `-file-ext-to-exclude` Die Einstellung überschreibt den `-file-ext-to-include` Einstellung.
- Einstellen `-scan-files-with-no-ext` Um Dateien ohne Erweiterungen zu scannen. Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen für den Zugriff erstellt `Policy1` Auf dem `vs1SVM`:

```
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. Überprüfen Sie, ob die Richtlinie für den Zugriff auf den Zugriff erstellt wurde: `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name policy_name`

Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

Mit dem folgenden Befehl werden die Details für das angezeigt Policy1 Richtlinie:

```
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
```

Aktivieren einer Zugriffsrichtlinie

Sie müssen eine Zugriffsrichtlinie auf einer SVM aktivieren, bevor deren Dateien gescannt werden können. Falls Sie eine Zugriffsrichtlinie für alle SVMs in einem Cluster erstellt haben, müssen Sie die Richtlinie für jede SVM einzeln aktivieren. Sie können jeweils nur eine Zugriffsrichtlinie für eine SVM aktivieren.

Schritte

1. Aktivieren einer Zugriffsrichtlinie:

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

Mit dem folgenden Befehl wird eine Richtlinie für den Zugriff mit dem Namen aktiviert Policy1 Auf dem vs1SVM:

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

2. Vergewissern Sie sich, dass die Zugriffsrichtlinie aktiviert ist: `vserver vscan on-access-policy show -instance data_SVM -policy-name policy_name`

Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

Mit dem folgenden Befehl werden die Details für das angezeigte `Policy1` Richtlinie für den Zugriff:

```
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
```

Ändern Sie das Vscan-Dateibetriebsprofil für eine SMB-Freigabe

Das Vscan-Dateibetriebsprofil für eine SMB-Freigabe definiert, welche Vorgänge auf der Freigabe das Scannen auslösen können. Standardmäßig ist der Parameter auf `standard` festgelegt. Sie können den Parameter beim Erstellen oder Ändern einer SMB-Freigabe nach Bedarf anpassen.

Über diese Aufgabe

Weitere Informationen zu den verfügbaren Werten für ein Vscan-Dateioperationen-Profil finden Sie unter „Vscan-Dateioperationen-Profil“.

["Vscan-Dateioperationen-Profil \(nur beim Scannen beim Zugriff\)"](#)



Der Virus-Scan wird nicht auf einer SMB-Freigabe durchgeführt, für die der `continuously-available` Parameter auf `Yes` festgelegt ist.

Schritt

1. Ändern Sie den Wert des Vscan-Dateibetriebsprofils für eine SMB-Freigabe: `vserver cifs share modify -vserver data_SVM -share-name share -path share_path -vscan-fileop -profile no-scan|standard|strict|writes-only`

Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

Mit dem folgenden Befehl wird das Vscan-Dateibetriebsprofil für eine SMB-Freigabe in geändert `strict`:

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

Befehle zum Managen von Zugriffsrichtlinien

Sie können eine Richtlinie für den Zugriff ändern, deaktivieren oder löschen. Sie können sich eine Zusammenfassung und Details der Richtlinie anzeigen lassen.

Ihr Ziel ist	Geben Sie den folgenden Befehl ein...
Ändern Sie eine Zugriffsrichtlinie	<code>vserver vscan on-access-policy modify</code>
Deaktivieren einer Zugriffsrichtlinie	<code>vserver vscan on-access-policy disable</code>
Löschen Sie eine Zugriffsrichtlinie	<code>vserver vscan on-access-policy delete</code>
Zusammenfassung und Details zu einer Zugriffsrichtlinie anzeigen	<code>vserver vscan on-access-policy show</code>
Fügen Sie zur Liste der auszuschließenden Pfade hinzu	<code>vscan on-access-policy paths-to-exclude add</code>
Löschen Sie die Liste der auszuschließenden Pfade	<code>vscan on-access-policy paths-to-exclude remove</code>
Zeigen Sie die Liste der auszuschließenden Pfade an	<code>vscan on-access-policy paths-to-exclude show</code>
Fügen Sie zur Liste der auszuschließenden Dateierweiterungen hinzu	<code>vscan on-access-policy file-ext-to-exclude add</code>
Löschen Sie aus der Liste der auszuschließenden Dateierweiterungen	<code>vscan on-access-policy file-ext-to-exclude remove</code>
Zeigen Sie die Liste der auszuschließenden Dateierweiterungen an	<code>vscan on-access-policy file-ext-to-exclude show</code>

Fügen Sie zur Liste der einzuschließen von Dateierweiterungen hinzu	<code>vscan on-access-policy file-ext-to-include add</code>
Löschen Sie aus der Liste der einzuschließen Dateiendungen	<code>vscan on-access-policy file-ext-to-include remove</code>
Die Liste der einzuschließen von Dateierweiterungen anzeigen	<code>vscan on-access-policy file-ext-to-include show</code>

Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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 IRGEND EINER 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.