Konfigurieren Sie das Scannen beim Zugriff

ONTAP 9

NetApp
April 24, 2024

Inhalt

Konfigurieren Sie das Scannen beim Zugriff

Erstellen einer Zugriffsrichtlinie

Eine Zugriffsrichtlinie definiert den Umfang eines Scans beim Zugriff. Sie können eine On-Access-Richtlinie für eine einzelne SVM oder für alle SVMs in einem Cluster erstellen. Falls Sie eine Zugriffsrichtlinie für alle SVMs in einem Cluster erstellt haben, müssen Sie die Richtlinie für jede SVM einzeln aktivieren.

Über diese Aufgabe

- Sie können die maximale Dateigröße für den Scan, Dateierweiterungen und Pfade für den Scan sowie Dateierweiterungen und -Pfade für den Scan angeben.
- Sie können die einstellen `scan-mandatory` Option „aus“, um festzulegen, dass der Dateizugriff zulässig ist, wenn keine Vscan-Server für Virenprüfungen verfügbar sind.
- Standardmäßig erstellt ONTAP eine Zugriffsrichtlinie mit dem Namen „Default_CIFS“ und ermöglicht sie für alle SVMs in einem Cluster.
- Jede Datei, die auf der Grundlage des für den Scanausschluss qualifiziert ist `paths-to-exclude`, `file-ext-to-exclude`, Oder `max-file-size` Parameter werden für das Scannen nicht berücksichtigt, auch wenn der `scan-mandatory` Die Option ist auf ein eingestellt. (Prüfen Sie dies "Fehlerbehebung" Abschnitt für Konnektivitätsprobleme im Zusammenhang mit `scan-mandatory` Option.)
- 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.
- Ein Virus-Scan wird nicht auf einer SMB-Freigabe durchgeführt, für die der kontinuierlich verfügbare Parameter auf Ja gesetzt ist.
- Siehe "Virenschutz-Architektur" Abschnitt für Details zum *Vscan file-Operations Profil*.
- Sie können maximal zehn (10) Zugriffsrichtlinien pro SVM erstellen. Sie können jedoch jeweils nur eine Richtlinie für den Zugriff aktivieren.
  - Sie können in einer Richtlinie für den Zugriff maximal hundert (100) Pfade und Dateierweiterungen von der Virenüberprüfung ausschließen.
- Einige Empfehlungen zum Dateiausschluss:
  - Ziehen Sie es in Erwägung, große Dateien (Dateigröße kann angegeben werden) von Virus-Scans auszuschließen, da sie zu einer langsamen Antwortzeit oder Scan-Anfrage-Timeouts für CIFS-Benutzer führen können. Die Standarddateigröße für Ausschluss beträgt 2 GB.
  - Es empfiehlt sich, Dateierweiterungen wie z. B. auszuschließen `.vhd` Und `.tmp` Weil Dateien mit diesen Erweiterungen möglicherweise nicht zum Scannen geeignet sind.
  - Es empfiehlt sich, Dateipfade wie das Quarantäneverzeichnis oder Pfade auszuschließen, in denen nur virtuelle Festplatten oder Datenbanken gespeichert sind.
  - Vergewissern Sie sich, dass alle Ausschlüsse in derselben Richtlinie angegeben sind, da jeweils nur eine Richtlinie aktiviert werden kann. NetApp empfiehlt dringend, die gleichen Ausschlüsse zu verwenden, die in der Antiviren-Engine angegeben sind.
- Für einen ist eine Zugangsrichtlinie erforderlich On-Demand-Scan. Um das Scannen beim Zugriff auf zu vermeiden, sollten Sie die Einstellung festlegen `-scan-files-with-no-ext` Zu false und `-file-ext-to-exclude` Um * auszuschließen, um alle Nebenstellen auszuschließen.

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 `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. 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` *`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

Eine Zugriffsrichtlinie definiert den Umfang eines Scans beim Zugriff. 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 `vs1` SVM:

   ```
   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 angezeigt `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 Profil *Vscan file-Operations* für eine SMB-Freigabe definiert die Vorgänge auf der Freigabe, die einen Scan auslösen können. Standardmäßig ist der Parameter auf festgelegt `standard`. Sie können den Parameter beim Erstellen oder Ändern einer SMB-Freigabe nach Bedarf anpassen.

Siehe "Virenschutz-Architektur" Abschnitt für Details zum *Vscan file-Operations Profil*.

> Der Virus-Scan wird nicht auf einer SMB-Freigabe durchgeführt, die über den verfügt `continuously-available` Parameter auf gesetzt `Yes`.

Schritt

1. Ändern Sie den Wert des Vscan-Dateioperationsprofils 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 Profil der Vscan-Dateivorgänge 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…
Erstellen einer Zugriffsrichtlinie	`vserver vscan on-access-policy create`
Ändern Sie eine Zugriffsrichtlinie	`vserver vscan on-access-policy modify`
Aktivieren einer Zugriffsrichtlinie	`vserver vscan on-access-policy enable`
Deaktivieren einer Zugriffsrichtlinie	`vserver vscan on-access-policy disable`
Löschen Sie eine Zugriffsrichtlinie	`vserver vscan on-access-policy delete`

Zusammenfassung und Details zu einer Zugriffsrichtlinie anzeigen	`vserver vscan on-access-policy show`
Fügen Sie zur Liste der auszuschließenden Pfade hinzu	`vserver vscan on-access-policy paths-to-exclude add`
Löschen Sie die Liste der auszuschließenden Pfade	`vserver vscan on-access-policy paths-to-exclude remove`
Zeigen Sie die Liste der auszuschließenden Pfade an	`vserver vscan on-access-policy paths-to-exclude show`
Fügen Sie zur Liste der auszuschließenden Dateierweiterungen hinzu	`vserver vscan on-access-policy file-ext-to-exclude add`
Löschen Sie aus der Liste der auszuschließenden Dateierweiterungen	`vserver vscan on-access-policy file-ext-to-exclude remove`
Zeigen Sie die Liste der auszuschließenden Dateierweiterungen an	`vserver vscan on-access-policy file-ext-to-exclude show`
Fügen Sie zur Liste der einzuschließen von Dateierweiterungen hinzu	`vserver vscan on-access-policy file-ext-to-include add`
Löschen Sie aus der Liste der einzuschließen Dateiendungen	`vserver vscan on-access-policy file-ext-to-include remove`
Die Liste der einzuschließen von Dateierweiterungen anzeigen	`vserver vscan on-access-policy file-ext-to-include show`

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