Virenschutzkonfiguration

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

Virenschutzkonfiguration

Übersicht über die Virenschutzkonfiguration

Sie können die NetApp Virenprüfung (*Vscan*) verwenden, um Daten vor Viren oder anderem Schadcode zu schützen. Es zeigt Ihnen, wie Sie mittels Zugriffsscans nach Viren suchen, wenn Clients über SMB auf Dateien zugreifen, und wie Sie On-Demand-Scans nutzen, um sofort oder nach einem Zeitplan auf Viren zu überprüfen.

Die Verwendung von Vscan erfolgt über die Befehlszeilenschnittstelle (CLI) von ONTAP, nicht über den System Manager oder ein automatisiertes Scripting Tool. Vscan wird von System Manager nicht unterstützt.

Verwandte Informationen

"Trellix (ehemals McAfee) Endpoint Security Storage Protection"

"Technischer Bericht 4304: Antivirus Solution for Clustered Data ONTAP Symantec"

"Technischer Bericht 4312: Antivirus Solution for Clustered Data ONTAP Trend Micro"

Über den Virenschutz von NetApp

Informationen zur Virenprüfung von NetApp

Mit der integrierten Antivirenfunktion auf NetApp Storage-Systemen schützen Sie Daten vor Viren oder anderen schädlichen Codes. Die NetApp Virenprüfung (*Vscan*) kombiniert erstklassige Virenschutz-Software von Drittanbietern mit den ONTAP Funktionen. Sie können dann flexibel kontrollieren, welche Dateien wann gescannt werden.

So funktioniert die Virenprüfung

Storage-Systeme verlagern Scanvorgänge auf externe Server, auf denen Virenschutz-Software von Drittanbietern gehostet wird. Der von NetApp bereitgestellte und auf dem externen Server installierte ONTAP Antivirus Connector übernimmt die Kommunikation zwischen dem Storage-System und der Antivirensoftware.

- Sie können *On-Access Scanning* verwenden, um nach Viren zu suchen, wenn Clients Dateien über SMB öffnen, lesen, umbenennen oder schließen. Der Dateivorgang wird angehalten, bis der externe Server den Scanstatus der Datei meldet. Wenn die Datei bereits gescannt wurde, ermöglicht ONTAP den Dateivorgang. Andernfalls fordert er einen Scan vom Server an.

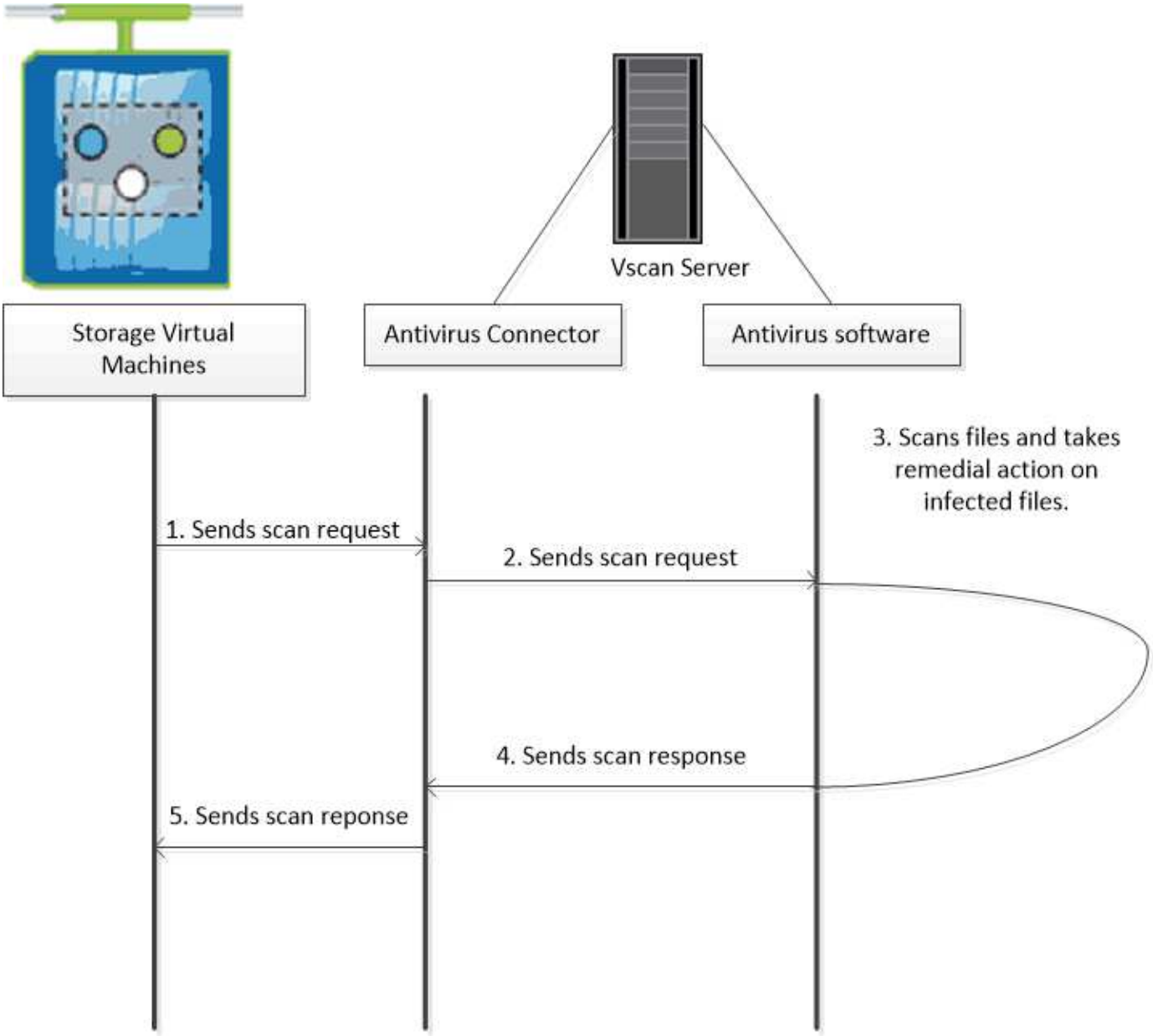
  Das Scannen beim Zugriff wird für NFS nicht unterstützt.

- Sie können *On-Demand Scan* verwenden, um Dateien sofort oder nach Zeitplan auf Viren zu überprüfen. Möglicherweise sollten Sie Scans nur außerhalb der Stoßzeiten durchführen, z. B.. Der externe Server aktualisiert den Scanstatus der überprüften Dateien, sodass die Verzögerung beim Dateizugriff für diese Dateien (sofern sie nicht geändert wurden) in der Regel beim nächsten Zugriff über SMB reduziert wird.

  Der bedarfsorientierte Scan eignet sich für jeden Pfad im SVM Namespace. Dies gilt auch für Volumes, die nur über NFS exportiert werden.

Sie aktivieren normalerweise beide Scanmodi auf einer SVM. In beiden Modi übernimmt die Antivirus-Software

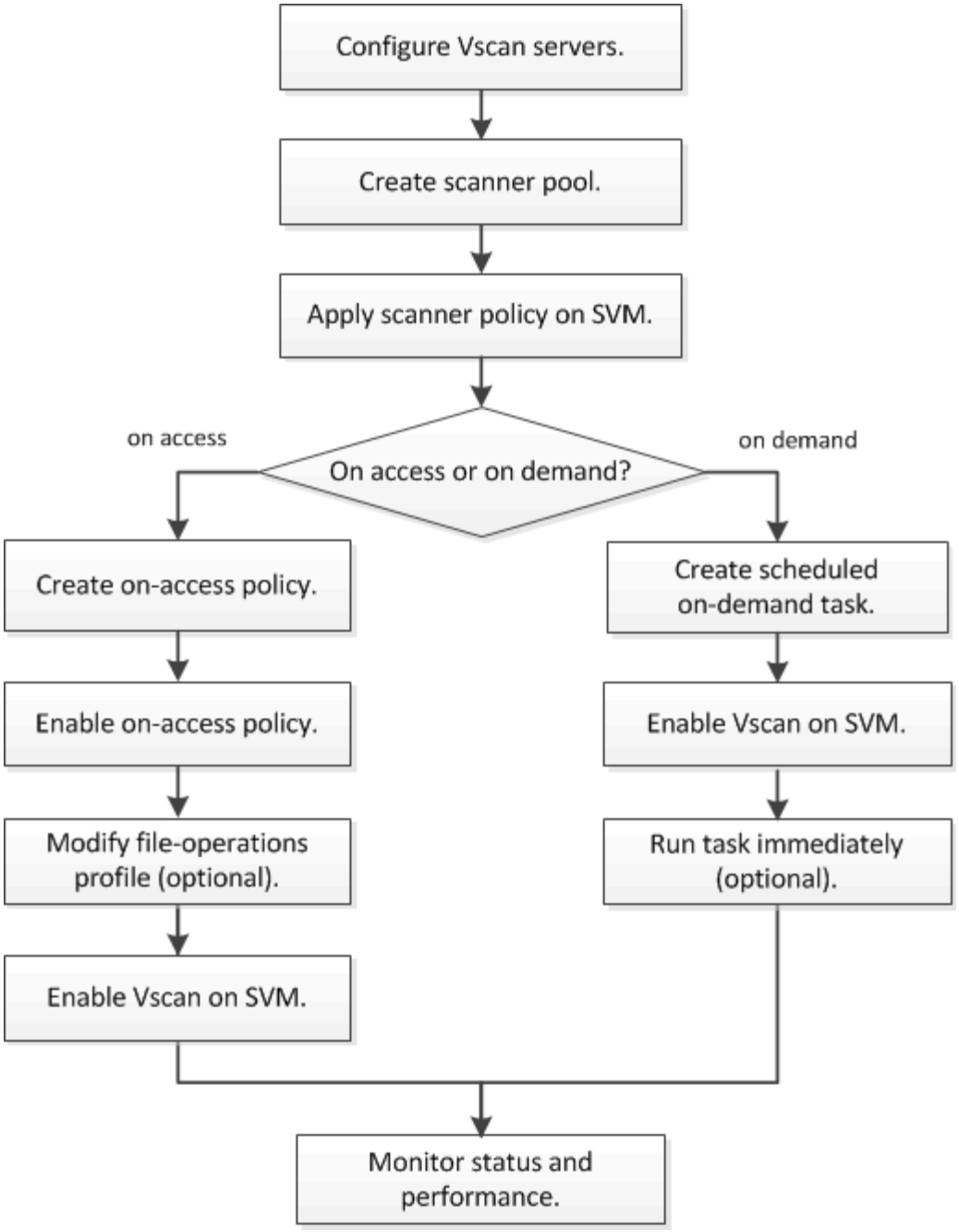
basierend auf Ihren Einstellungen in der Software eine Störungsbehebung bei infizierten Dateien.



Workflow für Virenprüfung

Sie müssen einen Scannerpool erstellen und eine Scannerrichtlinie anwenden, bevor Sie das Scannen aktivieren können. Sie aktivieren üblicherweise sowohl On-Access- als auch On-Demand-Scans auf einer SVM.

Sie müssen die CIFS-Konfiguration abgeschlossen haben.



Virenschutz-Architektur

Die Antiviren-Architektur von NetApp besteht aus einem Vscan Server und einer Reihe von ONTAP Konfigurationen.

Vscan-Server-Komponenten

Sie müssen die folgenden Komponenten auf dem Vscan-Server installieren.

- **ONTAP Antivirus Connector**

  Der von NetApp bereitgestellte Antivirus Connector ONTAP behandelt die Kommunikation zwischen ONTAP und dem Vscan Server.

- **Antivirus-Software**

  Die ONTAP-konforme Virenschutzsoftware anderer Anbieter überprüft Dateien auf Viren oder andere Malware. Sie geben die Abhilfemaßnahmen für infizierte Dateien an, wenn Sie die Software konfigurieren.

ONTAP-Konfigurationen

Sie müssen die folgenden Elemente auf dem NetApp Storage-System konfigurieren.

- **Scanner-Pool**

  Ein Scanner-Pool definiert die Vscan-Server und privilegierten Benutzer, die eine Verbindung zu SVMs herstellen können. Es definiert auch eine Zeitdauer für die Scan-Anforderung, nach der die Scan-Anforderung an einen alternativen Vscan-Server gesendet wird, wenn eine verfügbar ist.

  > Es empfiehlt sich, den Zeitraum für die Zeitüberschreitung in der Antivirensoftware auf dem Vscan-Server auf fünf Sekunden zu setzen, die unter dem Timeout-Zeitraum für die Scannerpoolanforderung liegen. Um Situationen zu vermeiden, in denen der Dateizugriff komplett verzögert oder verweigert wird, weil die Zeitdauer auf der Software größer ist als die Zeitdauer für die Scan-Anforderung.

- **Privilegierter Benutzer**

  Ein privilegierter Benutzer ist ein Domain-Benutzerkonto, das von einem Vscan-Server zur Verbindung mit der SVM verwendet wird. Das Konto muss in die Liste der privilegierten Benutzer enthalten sein, die im Scannerpool definiert sind.

- **Scanner-Richtlinie**

  Eine Scannerrichtlinie bestimmt, ob ein Scannerpool aktiv ist. Eine Scannerrichtlinie kann einen der folgenden Werte aufweisen:

  - `Primary` Gibt an, dass der Scannerpool aktiv ist.
  - `Secondary` Gibt an, dass der Scannerpool nur aktiv ist, wenn keiner der Vscan-Server im primären Scannerpool angeschlossen ist.
  - `Idle` Gibt an, dass der Scannerpool inaktiv ist. Die Scannerrichtlinien sind systemdefiniert. Sie können keine benutzerdefinierte Scannerrichtlinie erstellen.

- **Zugangsrichtlinie**

  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.

  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:

  - `scan-ro-volume` Ermöglicht das Scannen schreibgeschützter Volumes.
  - `scan-execute-access` Schränkt das Scannen auf Dateien ein, die durch Ausführen des Zugriffs geöffnet wurden.

„Execute Access“ ist nicht identisch mit „Execute Permission“. Ein bestimmter Client hat „Execute Access“ in einer ausführbaren Datei nur dann, wenn die Datei mit „Execute Intent“ geöffnet wurde.

Sie können die einstellen `scan-mandatory` Option „aus“, um festzulegen, dass der Dateizugriff zulässig ist, wenn keine Vscan-Server für Virenprüfungen verfügbar sind.

- **On-Demand Task**

  Ein On-Demand-Task definiert den Umfang eines Scans nach Bedarf. Sie können die maximale Größe der zu scannenden Dateien, die Erweiterungen und Pfade der Dateien angeben, die in den Scan aufgenommen werden sollen, sowie die Erweiterungen und Pfade der Dateien, die vom Scan ausgeschlossen werden sollen. Dateien in Unterverzeichnissen werden standardmäßig gescannt.

  Sie verwenden einen Cron-Zeitplan, um festzulegen, wann die Aufgabe ausgeführt wird. Sie können das verwenden `vserver vscan on-demand-task run` Befehl zum sofortigen Ausführen der Aufgabe.

- **Vscan-Dateioperationen-Profil (nur beim Scannen beim Zugriff)**

  Der `-vscan-fileop-profile` Parameter für das `vserver cifs share create` Der Befehl definiert, welche Vorgänge auf einer SMB-Freigabe einen Virus-Scan auslösen können. Standardmäßig ist der Parameter auf festgelegt `standard`, Das ist die NetApp Best Practice.

  Sie können diesen Parameter beim Erstellen oder Ändern einer SMB-Freigabe nach Bedarf anpassen:

  - `no-scan` Gibt an, dass Virenscans nie für die Freigabe ausgelöst werden.
  - `standard` Gibt an, dass Virenprüfungen durch Öffnen, Schließen und Umbenennen von Vorgängen ausgelöst werden können.
  - `strict` Gibt an, dass Virenprüfungen durch Öffnen, Lesen, Schließen und Umbenennen von Vorgängen ausgelöst werden können.

    Der `strict` Profil bietet erhöhte Sicherheit für Situationen, in denen mehrere Clients gleichzeitig auf eine Datei zugreifen. Wenn ein Client eine Datei schließt, nachdem ein Virus darauf geschrieben wurde, und die gleiche Datei weiterhin auf einem zweiten Client geöffnet bleibt, `strict` Stellt sicher, dass ein Lesevorgang auf dem zweiten Client einen Scan auslöst, bevor die Datei geschlossen wird.

    Sie sollten vorsichtig sein, die zu beschränken `strict` Profil für Freigaben, die Dateien enthalten, auf die Sie erwarten, wird gleichzeitig zugegriffen. Da das Profil mehr Scananforderungen generiert als die anderen, kann es sich negativ auf die Leistung auswirken.

  - `writes-only` Gibt an, dass Virenprüfungen nur ausgelöst werden können, wenn eine geänderte Datei geschlossen wurde.

    Wenn eine Client-Anwendung einen Umbenennung durchführt, wird die Datei mit dem neuen Namen geschlossen und nicht gescannt. Wenn ein solcher Betrieb in Ihrer Umgebung Sicherheitsaspekte mit sich bringt, sollten Sie den verwenden `standard` Oder `strict` Profil:

    Weil `writes-only` Generiert weniger Scananforderungen als die anderen Profile (außer `no-scan`), es verbessert in der Regel die Leistung.

Beachten Sie jedoch, dass der Scanner konfiguriert werden muss, wenn Sie dieses Profil für eine Freigabe

verwenden, um eine nicht pairable infizierte Datei zu löschen oder zu isolieren, damit später keine Clients darauf zugreifen können. Wenn z. B. ein Client eine Datei nach dem Schreiben eines Virus schließt und die Datei nicht repariert, gelöscht oder isoliert wird, wird jeder Client, der auf die Datei zugreift, infiziert.

Installation und Konfiguration des Vscan-Servers

Sie müssen einen oder mehrere Vscan-Server einrichten, um sicherzustellen, dass Dateien auf Ihrem System nach Viren gescannt werden. Befolgen Sie die Anweisungen Ihres Anbieters, um die Antivirensoftware auf dem Server zu installieren und zu konfigurieren. Befolgen Sie die Anweisungen in der Infodatei von NetApp, um den ONTAP Antivirus Connector zu installieren und zu konfigurieren.

Für Disaster Recovery- und MetroCluster-Konfigurationen müssen separate Vscan-Server für lokale und Partner-Cluster eingerichtet werden.

Anforderungen an die Virenschutz-Software

- Informationen zu den Anforderungen an Antivirensoftware finden Sie in der Dokumentation des Anbieters.
- Informationen zu den von Vscan unterstützten Anbietern, Software und Versionen finden Sie in der NetAppInteroperabilitätsmatrix.

  "mysupport.netapp.com/matrix"

Anforderungen für den Antivirus Connector von ONTAP

- Sie können den Antiviren-Connector für ONTAP von der Seite für Software-Download auf der NetApp Support-Website herunterladen. "NetApp Downloads: Software"
- Informationen zu den vom ONTAP Antivirus Connector unterstützten Windows-Versionen finden Sie in der NetAppInteroperabilitätsmatrix.

  "mysupport.netapp.com/matrix"

  Sie können verschiedene Versionen von Windows-Servern für verschiedene Vscan-Server in einem Cluster installieren.

- .NET 3.0 oder höher muss auf dem Windows-Server installiert sein.
- SMB 2.0 muss auf dem Windows Server aktiviert sein.

Konfigurieren von Scannerpools

Konfigurieren Sie die Übersicht über Scannerpools

Ein Scanner-Pool definiert die Vscan-Server und privilegierten Benutzer, die eine Verbindung zu SVMs herstellen können. Eine Scannerrichtlinie bestimmt, ob ein Scannerpool aktiv ist.

Wenn Sie eine Exportrichtlinie auf einem SMB-Server verwenden, müssen Sie jeden Vscan-Server zur Exportrichtlinie hinzufügen.

Erstellen Sie einen Scanner-Pool auf einem einzelnen Cluster

Ein Scanner-Pool definiert die Vscan-Server und privilegierten Benutzer, die eine Verbindung zu SVMs herstellen können. Sie können einen Scanner-Pool für eine einzelne SVM oder für alle SVMs in einem Cluster erstellen.

Was Sie benötigen

- SVMs und Vscan-Server müssen sich in derselben Domäne oder in vertrauenswürdigen Domänen befinden.
- Für Scannerpools, die für eine einzelne SVM definiert sind, müssen Sie den ONTAP Antivirus Connector mit der SVM Management LIF oder der SVM Daten-LIF konfiguriert haben.
- Für alle in einem Cluster definierten Scannerpools muss der ONTAP Antivirus Connector mit der Cluster-Management-LIF konfiguriert sein.

Über diese Aufgabe

Die Liste der privilegierten Benutzer muss das Domain-Benutzerkonto enthalten, das der Vscan-Server zur Verbindung mit der SVM verwendet.

Schritte

1. Erstellen eines Scannerpools:

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - Legen Sie eine Daten-SVM für einen Pool fest, der für eine einzelne SVM definiert ist, und geben Sie eine Cluster-Admin-SVM für einen Pool an, der für alle SVMs in einem Cluster definiert ist.
   - Geben Sie für jeden Host-Namen des Vscan-Servers eine IP-Adresse oder einen FQDN an.
   - Geben Sie die Domäne und den Benutzernamen für jeden privilegierten Benutzer an. Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

     Mit dem folgenden Befehl wird ein Scannerpool mit dem Namen erstellt `SP` Auf dem `vs1`SVM:

   ```
   cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
   SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
   cifs\u1,cifs\u2
   ```

2. Überprüfen Sie, ob der Scannerpool erstellt wurde: `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner-pool` *`scanner_pool`*

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

   Mit dem folgenden Befehl werden die Details für das angezeigt `SP` Scanner-Pool:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                                Scanner Pool: SP
                              Applied Policy: idle
                              Current Status: off
          Cluster on Which Policy Is Applied: -
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
```

Sie können auch die verwenden `vserver vscan scanner-pool show` Befehl zum Anzeigen aller Scannerpools auf einer SVM. Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

Erstellen von Scannerpools in MetroCluster-Konfigurationen

Sie müssen primäre und sekundäre Scannerpools auf jedem Cluster einer MetroCluster Konfiguration erstellen, die den primären und sekundären SVMs im Cluster entsprechen.

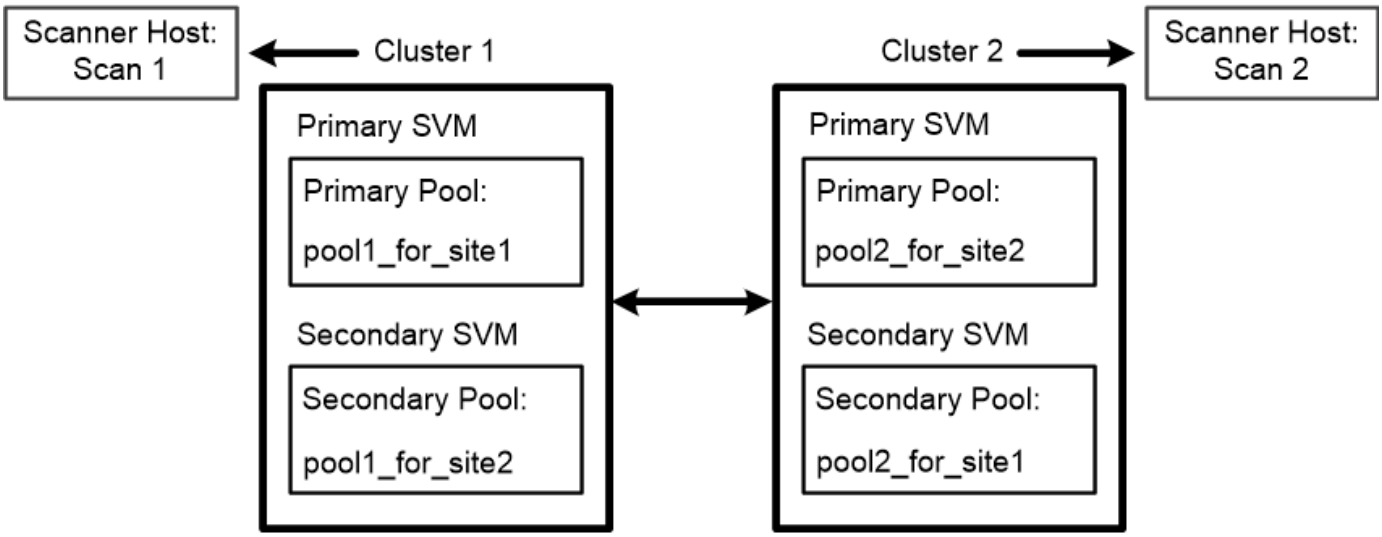
Was Sie benötigen

- SVMs und Vscan-Server müssen sich in derselben Domäne oder in vertrauenswürdigen Domänen befinden.
- Für Scannerpools, die für eine einzelne SVM definiert sind, müssen Sie den ONTAP Antivirus Connector mit der SVM Management LIF oder der SVM Daten-LIF konfiguriert haben.
- Für alle in einem Cluster definierten Scannerpools muss der ONTAP Antivirus Connector mit der Cluster-Management-LIF konfiguriert sein.

Über diese Aufgabe

MetroCluster Konfigurationen sichern Daten, indem zwei physisch getrennte gespiegelte Cluster implementiert werden. Jedes Cluster repliziert die Daten synchron zur SVM-Konfiguration des anderen. Eine primäre SVM auf dem lokalen Cluster stellt Daten bereit, wenn das Cluster online ist. Eine sekundäre SVM auf dem lokalen Cluster stellt Daten bereit, wenn das Remote-Cluster offline ist.

Das bedeutet, dass Sie primäre und sekundäre Scanner-Pools auf jedem Cluster einer MetroCluster Konfiguration erstellen müssen, die den primären und sekundären SVMs im Cluster entsprechen. Der sekundäre Pool wird aktiv, wenn das Cluster mit der Bereitstellung von Daten von der sekundären SVM beginnt. Die folgende Abbildung zeigt eine typische MetroCluster-Konfiguration.



Die Liste der privilegierten Benutzer muss das Domain-Benutzerkonto enthalten, das der Vscan-Server zur Verbindung mit der SVM verwendet.

Schritte

1. Erstellen eines Scannerpools:

   `vserver vscan scanner-pool create -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`* `-hostnames` *`Vscan_server_hostnames`* `-privileged-users` *`privileged_users`*

   - Legen Sie eine Daten-SVM für einen Pool fest, der für eine einzelne SVM definiert ist, und geben Sie eine Cluster-Admin-SVM für einen Pool an, der für alle SVMs in einem Cluster definiert ist.
   - Geben Sie für jeden Host-Namen des Vscan-Servers eine IP-Adresse oder einen FQDN an.
   - Geben Sie die Domäne und den Benutzernamen für jeden privilegierten Benutzer an.

     Sie müssen alle Scannerpools aus dem Cluster erstellen, das die primäre SVM enthält.

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

     Mit den folgenden Befehlen werden primäre und sekundäre Scannerpools auf jedem Cluster in einer MetroCluster-Konfiguration erstellt:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Überprüfen Sie, ob die Scannerpools erstellt wurden: `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner-pool` *`scanner_pool`*

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

   Mit dem folgenden Befehl werden die Details für den Scannerpool angezeigt `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: idle
                              Current Status: off
          Cluster on Which Policy Is Applied: -
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                     List of Privileged Users: cifs\u1,cifs\u2
```

   Sie können auch die verwenden `vserver vscan scanner-pool show` Befehl zum Anzeigen aller Scannerpools auf einer SVM. Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

Wenden Sie eine Scannerrichtlinie auf einem einzelnen Cluster an

Eine Scannerrichtlinie bestimmt, ob ein Scannerpool aktiv ist. Sie müssen einen Scannerpool aktiv machen, bevor die im Scannerpool definierten Vscan-Server eine Verbindung zu einer SVM herstellen können.

Über diese Aufgabe

- Sie können nur eine Scannerrichtlinie auf einen Scannerpool anwenden.
- Falls Sie einen Scanner-Pool für alle SVMs in einem Cluster erstellt haben, müssen Sie jeweils eine Scannerrichtlinie auf jede SVM anwenden.
- Für Disaster Recovery- und MetroCluster-Konfigurationen müssen Sie eine Scannerrichtlinie auf die Scannerpools für das lokale Cluster und das Partner-Cluster anwenden.

  In der Richtlinie, die Sie für das lokale Cluster erstellen, müssen Sie das lokale Cluster in angeben `cluster` Parameter. In der Richtlinie, die Sie für das Partner-Cluster erstellen, müssen Sie im das Partner-Cluster angeben `cluster` Parameter. Im Notfall kann der Partner-Cluster Virenprüfungen durchführen.

Schritte

1. Anwendung einer Scannerrichtlinie:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Eine Scannerrichtlinie kann einen der folgenden Werte aufweisen:

   - `Primary` Gibt an, dass der Scannerpool aktiv ist.
   - `Secondary` Gibt an, dass der Scannerpool nur aktiv ist, wenn keiner der Vscan-Server im primären Scannerpool angeschlossen ist.
   - `Idle` Gibt an, dass der Scannerpool inaktiv ist.

     Das folgende Beispiel zeigt, dass der Scanner-Pool mit dem Namen `SP` Auf dem `vs1` SVM ist aktiv:

   ```
   cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
   -scanner-pool SP  -scanner-policy primary
   ```

2. Vergewissern Sie sich, dass der Scanner-Pool aktiv ist:

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

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

   Mit dem folgenden Befehl werden die Details für das angezeigt `SP` Scanner-Pool:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                                Scanner Pool: SP
                              Applied Policy: primary
                              Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

Sie können das verwenden `vserver vscan scanner-pool show-active` Befehl zum Anzeigen der aktiven Scannerpools auf einer SVM. Die vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

Wenden Sie die Scannerrichtlinien in MetroCluster-Konfigurationen an

Eine Scannerrichtlinie bestimmt, ob ein Scannerpool aktiv ist. Sie müssen eine Scannerrichtlinie auf die primären und sekundären Scannerpools in jedem Cluster einer MetroCluster-Konfiguration anwenden.

Über diese Aufgabe

- Sie können nur eine Scannerrichtlinie auf einen Scannerpool anwenden.
- Falls Sie einen Scanner-Pool für alle SVMs in einem Cluster erstellt haben, müssen Sie jeweils eine Scannerrichtlinie auf jede SVM anwenden.

Schritte

1. Anwendung einer Scannerrichtlinie:

   `vserver vscan scanner-pool apply-policy -vserver` *`data_SVM`* `-scanner-pool` *`scanner_pool`* `-scanner-policy primary|secondary|idle -cluster` *`cluster_to_apply_policy_on`*

   Eine Scannerrichtlinie kann einen der folgenden Werte aufweisen:

   - `Primary` Gibt an, dass der Scannerpool aktiv ist.
   - `Secondary` Gibt an, dass der Scannerpool nur aktiv ist, wenn keiner der Vscan-Server im primären Scannerpool angeschlossen ist.
   - `Idle` Gibt an, dass der Scannerpool inaktiv ist.

   > Sie müssen alle Scannerrichtlinien auf dem Cluster anwenden, das die primäre SVM enthält.

Mit den folgenden Befehlen werden die Scannerrichtlinien auf die primären und sekundären Scannerpools in jedem Cluster in einer MetroCluster-Konfiguration angewendet:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Vergewissern Sie sich, dass der Scanner-Pool aktiv ist:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

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

   Mit dem folgenden Befehl werden die Details für den Scannerpool angezeigt `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: primary
                              Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   Sie können das verwenden `vserver vscan scanner-pool show-active` Befehl zum Anzeigen der aktiven Scannerpools auf einer SVM. Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

Befehle zum Verwalten von Scannerpools

Sie können Scannerpools ändern und löschen und privilegierte Benutzer und Vscan-

Server für einen Scannerpool verwalten. Sie können die Zusammenfassung und Details eines Scannerpools anzeigen.

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Ändern eines Scannerpools	`vserver vscan scanner-pool modify`
Löschen eines Scannerpools	`vserver vscan scanner-pool delete`
Fügen Sie privilegierte Benutzer zu einem Scanner-Pool hinzu	`vserver vscan scanner-pool privileged-users add`
Löschen Sie privilegierte Benutzer aus einem Scannerpool	`vserver vscan scanner-pool privileged-users remove`
Fügen Sie Vscan-Server einem Scanner-Pool hinzu	`vserver vscan scanner-pool servers add`
Löschen Sie Vscan-Server aus einem Scannerpool	`vserver vscan scanner-pool servers remove`
Zeigen Sie die Zusammenfassung und Details für einen Scannerpool an	`vserver vscan scanner-pool show`
Zeigen Sie privilegierte Benutzer für einen Scannerpool an	`vserver vscan scanner-pool privileged-users show`
Zeigen Sie Vscan-Server für alle Scannerpools an	`vserver vscan scanner-pool servers show`

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

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 `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 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 `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 Vscan-Dateibetriebsprofil für eine SMB-Freigabe definiert, welche Vorgänge auf der Freigabe das Scannen auslösen können. Standardmäßig ist der Parameter auf festgelegt `standard`. 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 ist auf festgelegt `Yes`.

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

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

Konfigurieren Sie das Scannen nach Bedarf

Konfigurieren Sie die Übersicht über das Scannen nach Bedarf

Mithilfe des On-Demand-Scans können Sie Dateien sofort oder nach einem Zeitplan auf Viren überprüfen. Möglicherweise möchten Sie Scans beispielsweise außerhalb der Stoßzeiten durchführen oder sehr große Dateien scannen, die von einem Scan beim Zugriff ausgeschlossen wurden.

Sie können einen Cron-Zeitplan verwenden, um festzulegen, wann die Aufgabe ausgeführt wird:

- Sie können beim Erstellen einer Aufgabe einen Zeitplan zuweisen.
- Sie können eine Aufgabe erstellen, ohne einen Zeitplan zuzuweisen, und verwenden Sie den `vserver vscan on-demand-task schedule` Befehl zum Zuweisen eines Zeitplans.
- Sie können das verwenden `vserver vscan on-demand-task run` Befehl zum sofortigen Ausführen einer Aufgabe, unabhängig davon, ob Sie einen Zeitplan zugewiesen haben.

Es kann jeweils nur eine Aufgabe gleichzeitig für eine SVM geplant werden.

Das Scannen nach Bedarf unterstützt keine Suche nach symbolischen Links oder Stream-Dateien.

Erstellen Sie eine On-Demand-Aufgabe

Ein On-Demand-Task definiert den Umfang eines Scans nach Bedarf. Sie können die maximale Größe der zu scannenden Dateien, die Erweiterungen und Pfade der Dateien angeben, die in den Scan aufgenommen werden sollen, sowie die Erweiterungen und Pfade der Dateien, die vom Scan ausgeschlossen werden sollen. Dateien in Unterverzeichnissen werden standardmäßig gescannt.

Schritte

1. On-Demand-Aufgabe erstellen:

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude
paths_of_files_to_exclude -file-ext-to-exclude extensions_of_files_to_exclude
-file-ext-to-include extensions_of_files_to_include -scan-files-with-no-ext
true|false -directory-recursion true|false
```

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

     Mit dem folgenden Befehl wird eine Aufgabe mit dem Namen für den Zugriff erstellt `Task1` Auf dem `vs1`SVM:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

Sie können das verwenden `job show` Befehl zum Anzeigen des Status des Jobs. Sie können das verwenden `job pause` Und `job resume` Befehle zum Anhalten und Neustarten des Jobs oder `job stop` Befehl zum Beenden des Jobs.

2. Überprüfen Sie, ob die Aufgabe On-Demand erstellt wurde: `vserver vscan on-demand-task show -instance data_SVM -task-name task_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 `Task1` Aufgabe:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                 List of Scan Paths: /vol1/, /vol2/cifs/
               Report Directory Path: /report
                        Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
              File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
            File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
            Request Service Timeout: 5m
                     Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
        Expiration Time for Report: -
```

Nachdem Sie fertig sind

Sie müssen den Scan auf der SVM aktivieren, bevor die Aufgabe geplant werden soll.

On-Demand-Aufgabe planen

Wenn Sie eine On-Demand-Aufgabe erstellt haben, ohne einen Zeitplan zuzuweisen, oder wenn Sie einer Aufgabe einen anderen Zeitplan zuweisen möchten, können Sie das verwenden `vserver vscan on-demand-task schedule` Befehl zum Zuweisen eines Zeitplans zu der Aufgabe.

Über diese Aufgabe

Der mit dem zugewiesene Zeitplan `vserver vscan on-demand-task schedule` Der Befehl überschreibt einen Zeitplan, der bereits dem zugewiesen ist `vserver vscan on-demand-task create` Befehl.

Schritte

1. Planung einer On-Demand-Aufgabe:

   ```
   vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name
   -schedule cron_schedule
   ```

   Der folgende Befehl plant eine Aufgabe mit dem Namen „On Access“ `Task2` Auf dem `vs2`SVM:

   ```
   cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
   -name Task2 -schedule daily
   [Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
   command to view the status.
   ```

   Sie können das verwenden `job show` Befehl zum Anzeigen des Status des Jobs. Sie können das verwenden `job pause` Und `job resume` Befehle zum Anhalten und Neustarten des Jobs oder `job stop` Befehl zum Beenden des Jobs.

2. Vergewissern Sie sich, dass die On-Demand-Aufgabe geplant ist: `vserver vscan on-demand-task show -instance data_SVM -task-name task_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 `Task 2` Aufgabe:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
```

Nachdem Sie fertig sind

Sie müssen den Scan auf der SVM aktivieren, bevor die Aufgabe geplant werden soll.

Führen Sie eine On-Demand-Aufgabe sofort aus

Sie können eine On-Demand-Aufgabe sofort ausführen, unabhängig davon, ob Sie einen Zeitplan zugewiesen haben.

Was Sie benötigen

Sie müssen das Scannen auf der SVM aktiviert haben.

Schritt

1. Führen Sie eine On-Demand-Aufgabe sofort aus:

   ```
   vserver vscan on-demand-task run -vserver data_SVM -task-name task_name
   ```

   Mit dem folgenden Befehl wird eine Aufgabe mit dem Namen für den Zugriff ausgeführt `Task1` Auf dem `vs1`SVM:

   ```
   cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
   Task1
   [Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
   command to view the status.
   ```

Sie können das verwenden `job show` Befehl zum Anzeigen des Status des Jobs. Sie können das verwenden `job pause` Und `job resume` Befehle zum Anhalten und Neustarten des Jobs oder `job stop` Befehl zum Beenden des Jobs.

Befehle für das Managen von On-Demand-Aufgaben

Sie können eine On-Demand-Aufgabe ändern, löschen oder aufheben. Sie können eine Zusammenfassung und Details für die Aufgabe anzeigen und Berichte für die Aufgabe verwalten.

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Ändern Sie eine Aufgabe nach Bedarf	`vserver vscan on-demand-task modify`
Löschen Sie eine On-Demand-Aufgabe	`vserver vscan on-demand-task delete`
Aufheben der Planung einer On-Demand-Aufgabe	`vserver vscan on-demand-task unschedule`
Zusammenfassung und Details für eine On-Demand-Aufgabe anzeigen	`vserver vscan on-demand-task show`
On-Demand-Berichte anzeigen	`vserver vscan on-demand-task report show`
On-Demand-Berichte löschen	`vserver vscan on-demand-task report delete`

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

Aktivieren Sie das Virensuchen auf einer SVM

Sie müssen den Virenscan auf einer SVM aktivieren, bevor ein Zugriff oder On-Demand-Scan ausgeführt werden kann. Die Vscan-Konfiguration muss vorhanden sein.

Schritte

1. Virenprüfung auf einer SVM aktivieren:

```
vserver vscan enable -vserver data_SVM
```

Sie können das verwenden `vserver vscan disable` Befehl zum Deaktivieren der Virenprüfung, falls erforderlich.

Mit dem folgenden Befehl wird das Scannen von Viren auf der aktiviert `vs1`SVM:

```
cluster1::> vserver vscan enable -vserver vs1
```

2. Vergewissern Sie sich, dass der Virus-Scan auf der SVM aktiviert ist:

   `vserver vscan show -vserver data_SVM`

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

   Mit dem folgenden Befehl wird der Vscan-Status des angezeigt `vs1`SVM:

```
cluster1::> vserver vscan show -vserver vs1

                            Vserver: vs1
                        Vscan Status: on
```

Setzen Sie den Status der gescannten Dateien zurück

Gelegentlich möchten Sie den Scanstatus erfolgreich gescannter Dateien auf einer SVM mithilfe von zurücksetzen `vserver vscan reset` Befehl zum Verwerfen der zwischengespeicherten Informationen für die Dateien. Mit diesem Befehl können Sie beispielsweise die Virenüberprüfung neu starten, wenn ein falsch konfigurierter Scan durchgeführt wird.

Über diese Aufgabe

Nachdem Sie den ausgeführt haben `vserver vscan reset` Befehl: Alle geeigneten Dateien werden beim nächsten Zugriff gescannt.

> Dieser Befehl kann sich nachteilig auf die Performance auswirken, abhängig von der Anzahl und Größe der neu zu speicherenden Dateien.

Schritt

1. Status der gescannten Dateien zurücksetzen:

   `vserver vscan reset -vserver data_SVM`

   Mit dem folgenden Befehl wird der Status der gescannten Dateien auf dem zurückgesetzt `vs1`SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

Zeigen Sie Vscan-Ereignisprotokollinformationen an

Sie können das verwenden `vserver vscan show-events` Befehl zum Anzeigen von Ereignisprotokollinformationen zu infizierten Dateien, Aktualisierungen auf Vscan-Servern

und dergleichen. Sie können Ereignisinformationen für das Cluster oder bestimmte Nodes, SVMs oder Vscan-Server anzeigen.

Was Sie benötigen

Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Anzeigen von Vscan-Ereignisprotokollinformationen:

   ```
   vserver vscan show-events
   ```

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

   Mit dem folgenden Befehl werden Ereignisprotokollinformationen für das Cluster angezeigt `cluster1`:

   ```
   cluster1::*> vserver vscan show-events

   Vserver     Node            Server          Event Type         Event Time
   ----------- --------------- --------------- -----------------
   -----------------
   vs1         Cluster-01      192.168.1.1     file-infected      9/5/2014
   11:37:38
   vs1         Cluster-01      192.168.1.1     scanner-updated    9/5/2014
   11:37:08
   vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
   11:34:55
   3 entries were displayed.
   ```

Behebung von Konnektivitätsproblemen

Mögliche Verbindungsprobleme bei der Option „Scannen erforderlich“

Sie können das verwenden `vserver vscan connection-status show` Befehle zum Anzeigen von Informationen über Vscan-Serververbindungen, die bei der Behebung von Verbindungsproblemen hilfreich sein könnten.

Standardmäßig wird der verwendet `scan-mandatory` Option für das Scannen beim Zugriff verweigert den Dateizugriff, wenn keine Vscan-Serververbindung zum Scannen verfügbar ist. Obwohl diese Option wichtige Sicherheitsfunktionen bietet, kann sie in einigen Situationen zu Problemen führen.

- Bevor Sie den Client-Zugriff aktivieren, müssen Sie sicherstellen, dass mindestens ein Vscan-Server mit einer SVM auf jedem Node mit einer LIF verbunden ist. Wenn Sie nach Aktivierung des Client-Zugriffs Server mit SVMs verbinden müssen, müssen Sie den deaktivieren `scan-mandatory` Option auf der SVM, um sicherzustellen, dass der Dateizugriff nicht verweigert wird, da keine Vscan-Serververbindung

verfügbar ist. Sie können die Option wieder einschalten, nachdem der Server verbunden ist.

- Wenn ein Ziel-LIF alle Vscan-Serververbindungen für eine SVM hostet, geht die Verbindung zwischen dem Server und der SVM verloren, wenn die LIF migriert wird. Um sicherzustellen, dass der Dateizugriff nicht verweigert wird, weil keine Vscan-Serververbindung verfügbar ist, müssen Sie das deaktivieren `scan-mandatory` Vor der Migration des LIF Option. Sie können die Option wieder einschalten, nachdem das LIF migriert wurde.

Jeder SVM sollten mindestens zwei Vscan-Server zugewiesen sein. Als Best Practice wird empfohlen, Vscan-Server über ein anderes Netzwerk als den für Client-Zugriffe verwendeten Vscan-Servern mit dem Speichersystem zu verbinden.

Befehle zum Anzeigen des Verbindungsstatus des Vscan-Servers

Sie können das verwenden `vserver vscan connection-status show` Befehle zum Anzeigen der Zusammenfassung und detaillierter Informationen zum Verbindungsstatus des Vscan-Servers.

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Zeigen Sie eine Zusammenfassung der Vscan-Serververbindungen an	`vserver vscan connection-status show`
Details zu Vscan-Serververbindungen anzeigen	`vserver vscan connection-status show-all`
Details für verbundene Vscan-Server anzeigen	`vserver vscan connection-status show-connected`
Details zu verfügbaren Vscan-Servern anzeigen, die nicht verbunden sind	`vserver vscan connection-status show-not-connected`

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