



# **Schützen Sie sich vor Viren**

ONTAP 9

NetApp  
April 24, 2024

# Inhalt

- Schützen Sie sich vor Viren ..... 1
  - Übersicht über die Virenschutzkonfiguration ..... 1
  - Über den Virenschutz von NetApp ..... 1
  - Installation und Konfiguration des Vscan-Servers ..... 7
  - Konfigurieren von Scannerpools ..... 15
  - Konfigurieren Sie das Scannen beim Zugriff ..... 23
  - Konfigurieren Sie das Scannen nach Bedarf ..... 28
  - Best Practices zur Konfiguration der Off-Box-Antivirus-Funktion in ONTAP ..... 33
  - Aktivieren Sie das Virensuchen auf einer SVM ..... 35
  - Setzen Sie den Status der gescannten Dateien zurück ..... 35
  - Zeigen Sie Vscan-Ereignisprotokollinformationen an ..... 36
  - Überwachung und Fehlerbehebung von Konnektivitätsproblemen ..... 37

# Schützen Sie sich vor Viren

## Übersicht über die Virenschutzkonfiguration

Vscan ist eine von NetApp entwickelte Virenschutzlösung, mit der Kunden ihre Daten vor Angriffen durch Viren oder anderen Schadcode schützen können.

Vscan führt Virenprüfungen durch, wenn Clients über SMB auf Dateien zugreifen. Sie können Vscan so konfigurieren, dass er nach Bedarf oder nach einem Zeitplan scannt. Sie können mit Vscan über die ONTAP-Befehlszeilenschnittstelle (CLI) oder ONTAP-APIs (Application Programming Interfaces) interagieren.

### Verwandte Informationen

["Partnerlösungen von Vscan"](#)

## Über den Virenschutz von NetApp

### Informationen zur Virenprüfung von NetApp

Vscan ist eine von NetApp entwickelte Virenschutzlösung, mit der Kunden ihre Daten vor Angriffen durch Viren oder anderen Schadcode schützen können. Es kombiniert von Partnern bereitgestellte Antivirensoftware mit ONTAP-Funktionen, um Kunden die Flexibilität zu geben, die sie für die Verwaltung der Dateiprüfung benötigen.

### So funktioniert die Virenprüfung

Storage-Systeme verlagern Scanvorgänge auf externe Server, auf denen Virenschutz-Software von Drittanbietern gehostet wird.

Basierend auf dem aktiven Scanmodus sendet ONTAP Scananforderungen, wenn Clients über SMB (On-Access) auf Dateien zugreifen oder an bestimmten Orten auf Dateien zugreifen, nach Zeitplan oder sofort (On-Demand).

- Sie können *On-Access Scanning* verwenden, um nach Viren zu suchen, wenn Clients Dateien über SMB öffnen, lesen, umbenennen oder schließen. Dateivorgänge werden 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.

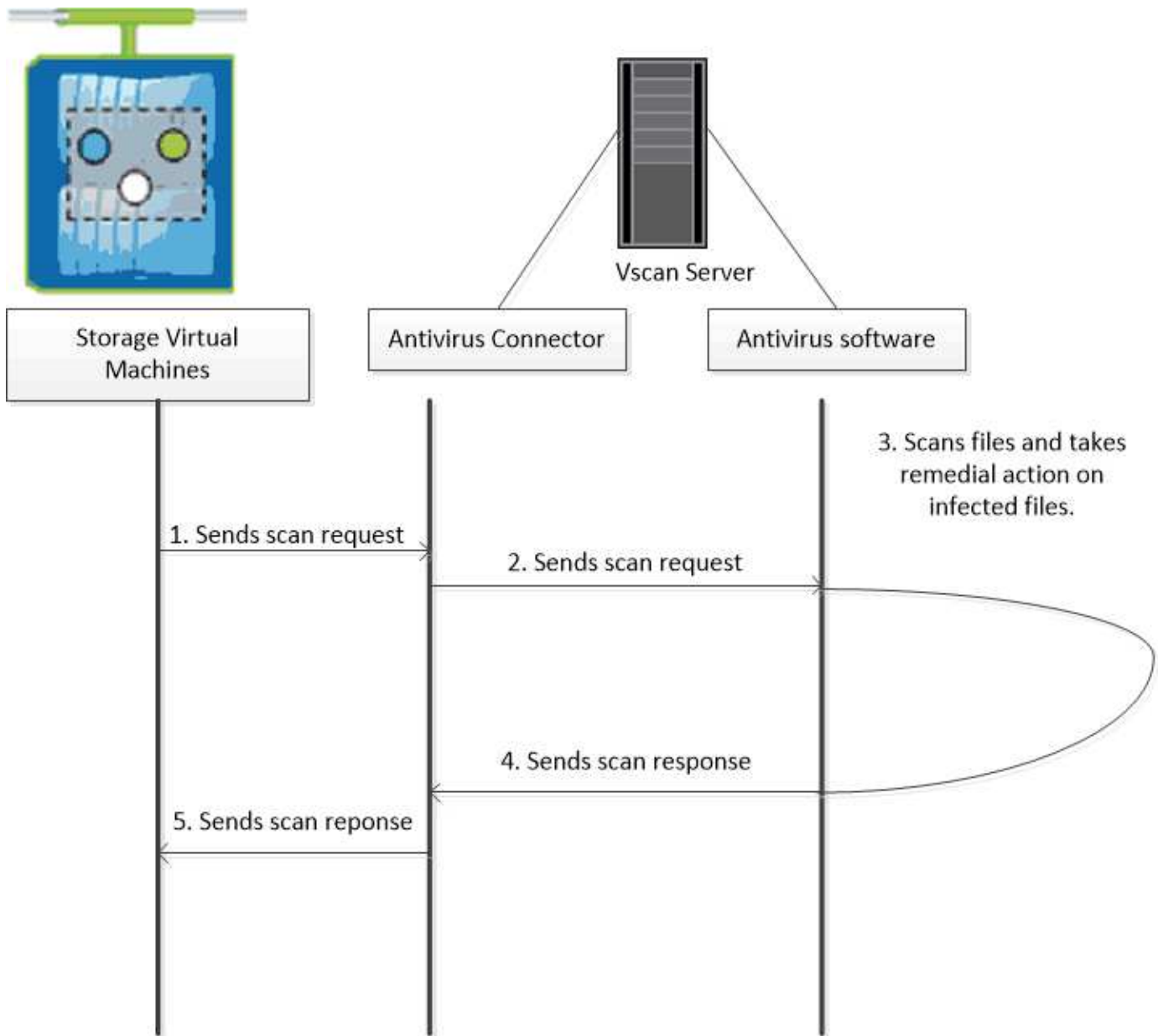
- Sie können *On-Demand Scan* verwenden, um Dateien sofort oder nach Zeitplan auf Viren zu überprüfen. Wir empfehlen die Ausführung von On-Demand-Scans nur in Zeiten geringerer Auslastung, um eine Überlastung der vorhandenen AV-Infrastruktur zu vermeiden, die normalerweise für Scans bei Zugriff verwendet wird. Der externe Server aktualisiert den Scanstatus der geprüften Dateien, sodass die Latenz beim Dateizugriff über SMB reduziert wird. Wenn Dateiänderungen oder Softwareupdates vorgenommen wurden, wird eine neue Dateiprüfung vom externen Server angefordert.

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

In der Regel können Sie auf einer SVM sowohl den Scan-Modus für den Zugriff als auch den On-Demand-

Modus aktivieren. In beiden Modi führt die Antivirensoftware anhand Ihrer Softwareeinstellungen Abhilfemaßnahmen für infizierte Dateien durch.

Der von NetApp bereitgestellte und auf dem externen Server installierte ONTAP Antivirus Connector übernimmt die Kommunikation zwischen dem Storage-System und der Antivirensoftware.



## Workflow für Virenprüfung

Sie müssen einen Scannerpool erstellen und eine Scannerrichtlinie anwenden, bevor Sie das Scannen aktivieren können. In der Regel können Sie auf einer SVM sowohl den Scan-Modus für den Zugriff als auch den On-Demand-Modus aktivieren.



Sie müssen die CIFS-Konfiguration abgeschlossen haben.



#### Nächste Schritte

- [Erstellen Sie einen Scanner-Pool auf einem einzelnen Cluster](#)
- [Wenden Sie eine Scannerrichtlinie auf einem einzelnen Cluster an](#)
- [Erstellen einer Zugriffsrichtlinie](#)

## Virenschutz-Architektur

Die NetApp Virenschutzarchitektur besteht aus der Vscan-Serversoftware und den zugehörigen Einstellungen.

### Vscan Server-Software

Sie müssen diese Software auf dem Vscan-Server installieren.

- **ONTAP Antivirus Connector**

Hierbei handelt es sich um die von NetApp bereitgestellte Software, die die Kommunikation von Scananforderungen und -antworten zwischen SVMs und Virenschutz-Software übernimmt. Er kann auf einer virtuellen Maschine ausgeführt werden, um die bestmögliche Leistung zu erzielen, verwenden Sie jedoch eine physische Maschine. Sie können diese Software von der NetApp Support-Website herunterladen (Anmeldung erforderlich).

- **Antivirus-Software**

Dies ist eine vom Partner bereitgestellte Software, die Dateien auf Viren oder anderen schädlichen Code scannt. Sie geben die Abhilfemaßnahmen für infizierte Dateien an, wenn Sie die Software konfigurieren.

## **Vscan-Softwareeinstellungen**

Sie müssen diese Softwareeinstellungen auf dem Vscan-Server konfigurieren.

- **Scanner-Pool**

Diese Einstellung 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.



Sie sollten in der Antivirensoftware auf dem Vscan-Server die Zeitdauer für die Zeitüberschreitung bei Scan-Request-Anforderung des Scanners auf fünf Sekunden einstellen. Dadurch werden Situationen vermieden, in denen der Dateizugriff verzögert oder ganz verweigert wird, da die Zeitüberschreitung auf der Software größer ist als die Zeitdauer für die Scananforderung.

- **Privilegierter Benutzer**

Diese Einstellung ist ein Domänenbenutzerkonto, das ein Vscan-Server verwendet, um eine Verbindung mit der SVM herzustellen. Das Konto muss in der Liste der privilegierten Benutzer im Scanner-Pool vorhanden sein.

- **Scanner-Richtlinie**

Diese Einstellung bestimmt, ob ein Scannerpool aktiv ist. Scannerrichtlinien sind systemdefiniert, sodass Sie keine benutzerdefinierten Scannerrichtlinien erstellen können. Nur diese drei Richtlinien sind verfügbar:

- **Primary** Gibt an, dass der Scannerpool aktiv ist.
- **Secondary** Gibt an, dass der Scanner-Pool nur aktiv ist, wenn keiner der Vscan-Server im primären Scanner-Pool verbunden ist.
- **Idle** Gibt an, dass der Scannerpool inaktiv ist.

- **Zugangsrichtlinie**

Diese Einstellung definiert den Umfang eines Scans bei Zugriff. Sie können die maximale Dateigröße für den Scan, Dateierweiterungen und Pfade für den Scan sowie Dateierweiterungen und -Pfade für den Scan angeben.

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.



„Zugriff ausführen“ unterscheidet sich von „Berechtigung ausführen“. Ein bestimmter Client hat nur dann „Execute Access“ auf eine ausführbare Datei, 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. Im On-Access-Modus können Sie aus den folgenden beiden Optionen wählen, die sich gegenseitig ausschließen:

- **Obligatorisch:** Mit dieser Option versucht Vscan, die Scananforderung an den Server zu senden, bis die Timeout-Zeit abläuft. Wenn die Scananforderung vom Server nicht akzeptiert wird, wird die Clientzugriffsanforderung abgelehnt.
- **Nicht obligatorisch:** Mit dieser Option erlaubt Vscan immer den Client-Zugriff, unabhängig davon, ob ein Vscan-Server für den Virens Scanner verfügbar war oder nicht.

#### • On-Demand Task

Diese Einstellung definiert den Umfang eines On-Demand-Scans. Sie können die maximale Dateigröße für den Scan, Dateierweiterungen und Pfade für den Scan sowie Dateierweiterungen und -Pfade für den Scan angeben. 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` Befehl definiert, welche SMB-Dateioperationen einen Virus-Scan auslösen. Standardmäßig ist der Parameter auf `standard` festgelegt. Das ist NetApp Best Practice. Sie können diesen Parameter bei Bedarf anpassen, wenn Sie eine SMB-Freigabe erstellen oder ändern:

- `no-scan` Gibt an, dass Virens Scans nie für die Freigabe ausgelöst werden.
- `standard` Gibt an, dass Virens Scans durch Öffnen, Schließen und Umbenennen ausgelöst werden.
- `strict` Gibt an, dass Virens Scans durch Öffnen, Lesen, Schließen und Umbenennen ausgelöst werden.

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 dieses Profil mehr Scananforderungen generiert, kann dies die Performance beeinträchtigen.

- `writes-only` Gibt an, dass Virens Scans nur ausgelöst werden, wenn geänderte Dateien geschlossen werden.

Seit `writes-only` Weniger Scananforderungen werden generiert, in der Regel wird die Performance verbessert.

Wenn Sie dieses Profil verwenden, muss der Scanner so konfiguriert sein, dass nicht reparierbare infizierte Dateien gelöscht oder isoliert werden können, sodass kein Zugriff darauf möglich ist. Wenn beispielsweise ein Client eine Datei nach dem Schreiben eines Virus schließt und die Datei nicht repariert, gelöscht oder isoliert wird, kann jeder Client, der auf die Datei zugreift, eine Datei schließen `without` Das Schreiben wird infiziert sein.



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:

## Partnerlösungen von Vscan

NetApp arbeitet mit Trellix, Symantec, Trend Micro und Sentinel One zusammen, um branchenführende Anti-Malware- und Antiviren-Lösungen bereitzustellen, die auf der ONTAP Vscan-Technologie aufbauen. Diese Lösungen helfen Ihnen, Dateien auf Malware zu scannen und alle betroffenen Dateien zu beheben.

Wie in der folgenden Tabelle dargestellt, werden die Details zur Interoperabilität von Trellix, Symantec und Trend Micro in der Interoperabilitätsmatrix von NetApp beibehalten. Interoperabilitätsdetails für Trellix und Symantec finden Sie auch auf den Partner-Websites. Informationen zur Interoperabilität von Sentinel One und anderen neuen Partnern werden vom Partner auf seinen Websites gepflegt.

Partner	Lösungsdokumentation	Details zur Interoperabilität
Trellix (ehemals McAfee)	<a href="#">"Trellix Produktdokumentation"</a>	<ul style="list-style-type: none"><li>• <a href="#">"NetApp Interoperabilitäts-Matrix-Tool"</a></li><li>• <a href="#">"Unterstützte Plattformen für Endpoint Security Storage Protection (trellix.com)"</a></li></ul>
Symantec	<a href="#">"Symantec Protection Engine 9.0.0"</a>	<ul style="list-style-type: none"><li>• <a href="#">"NetApp Interoperabilitäts-Matrix-Tool"</a></li><li>• <a href="#">"Support Matrix für Partnergeräte, die mit Symantec Protection Engine (SPE) für Network Attached Storage (NAS) zertifiziert sind 9.x.x"</a></li><li>• <a href="#">"Support Matrix für Partnergeräte, die mit Symantec Protection Engine (SPE) für Network Attached Storage (NAS) zertifiziert sind 8.x (broadcom.com)"</a></li></ul>



Partner	Lösungsdokumentation	Details zur Interoperabilität
Trend Micro	<a href="#">"Trend Micro ServerProtect for Storage 6.0 – Leitfaden für die ersten Schritte"</a>	<a href="#">"NetApp Interoperabilitäts-Matrix-Tool"</a>
Sentinel One	<ul style="list-style-type: none"> <li>• <a href="#">"SentinelOne Singularity Cloud Data Security"</a></li> <li>• <a href="#">"SentinelOne-Unterstützung"</a></li> </ul> <p>Für diesen Link ist eine Benutzeranmeldung erforderlich. Sie können den Zugriff über Sentinel One anfordern.</p>	Tiefes Instinkt

## Installation und Konfiguration des Vscan-Servers

### Installation und Konfiguration des Vscan-Servers

Richten Sie einen oder mehrere Vscan-Server ein, um sicherzustellen, dass Dateien auf Ihrem System auf 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 von NetApp bereitgestellten README-Datei, um den ONTAP Antivirus Connector zu installieren und zu konfigurieren. Befolgen Sie alternativ die Anweisungen auf der ["Installieren Sie die Seite ONTAP Antivirus Connector"](#).



Für Disaster Recovery- und MetroCluster-Konfigurationen müssen Sie separate Vscan-Server für die primären/lokalen und sekundären/Partner-ONTAP-Cluster einrichten und konfigurieren.

### Anforderungen an die Virenschutz-Software

- Informationen zu den Anforderungen an Antivirensoftware finden Sie in der Dokumentation des Anbieters.
- Informationen zu den von Vscan unterstützten Herstellern, Software und Versionen finden Sie im ["Partnerlösungen von Vscan"](#) Seite.

### Anforderungen für den Antivirus Connector von ONTAP

- Sie können den ONTAP Antivirus Connector von der Seite **Software-Download** auf der NetApp Support-Website herunterladen. ["NetApp Downloads: Software"](#)
- Informationen zu den Windows-Versionen, die vom ONTAP-VirenschutzConnector unterstützt werden, und zu den Interoperabilitätsanforderungen finden Sie unter ["Partnerlösungen von Vscan"](#).



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.

## Installieren Sie den ONTAP Antivirus Connector

Installieren Sie den ONTAP-Virenschutzanschluss auf dem Vscan-Server, um die Kommunikation zwischen dem System, auf dem ONTAP ausgeführt wird, und dem Vscan-Server zu ermöglichen. Bei der Installation des ONTAP Antivirus Connectors kann die Virenschutzsoftware mit einer oder mehreren Storage Virtual Machines (SVMs) kommunizieren.

### Über diese Aufgabe

- Siehe "[Partnerlösungen von Vscan](#)" Auf dieser Seite finden Sie Informationen zu unterstützten Protokollen, Softwareversionen von Antivirenanbietern, ONTAP-Versionen, Interoperabilitätsanforderungen und Windows-Servern.
- .NET 4.5.1 oder höher muss installiert sein.
- Der ONTAP Antivirus Connector kann auf einer virtuellen Maschine ausgeführt werden. Um die beste Performance zu erzielen, empfiehlt NetApp jedoch die Verwendung einer dedizierten Virtual Machine für Virenschutzprüfungen.
- SMB 2.0 muss auf dem Windows-Server aktiviert sein, auf dem Sie den ONTAP-Antivirus-Connector installieren und ausführen.

### Bevor Sie beginnen

- Laden Sie die Installationsdatei für den ONTAP Antivirus Connector von der Support-Website herunter und speichern Sie sie in einem Verzeichnis auf Ihrer Festplatte.
- Stellen Sie sicher, dass Sie die Anforderungen für die Installation des ONTAP-Virenschutzanschlusses erfüllen.
- Überprüfen Sie, ob Sie über Administratorrechte für die Installation des Antivirus Connectors verfügen.

### Schritte

1. Starten Sie den Antivirus Connector-Installationsassistenten, indem Sie die entsprechende Setup-Datei ausführen.
2. Wählen Sie **Next**. Das Dialogfeld Zielordner wird geöffnet.
3. Wählen Sie **Next**, um den Antivirus Connector in dem Ordner zu installieren, der aufgelistet ist, oder wählen Sie **Change**, um ihn in einem anderen Ordner zu installieren.
4. Das Dialogfeld ONTAP AV-Connector Windows-Dienstanmeldeinformationen wird geöffnet.
5. Geben Sie Ihre Windows-Dienstanmeldeinformationen ein, oder wählen Sie **Hinzufügen**, um einen Benutzer auszuwählen. Bei einem ONTAP-System muss dieser Benutzer ein gültiger Domänenbenutzer sein und in der Scannerpoolkonfiguration für die SVM vorhanden sein.
6. Wählen Sie **Weiter**. Das Dialogfeld bereit zur Installation des Programms wird geöffnet.
7. Wählen Sie **Installieren**, um mit der Installation zu beginnen, oder wählen Sie **Zurück**, wenn Sie Änderungen an den Einstellungen vornehmen möchten. Ein Statusfeld wird geöffnet und zeigt den Fortschritt der Installation an, gefolgt vom Dialogfeld InstallShield Wizard abgeschlossen.
8. Aktivieren Sie das Kontrollkästchen ONTAP LIFs konfigurieren, wenn Sie mit der Konfiguration von ONTAP Management oder Daten-LIFs fortfahren möchten. Sie müssen mindestens eine ONTAP Management- oder Daten-LIF konfigurieren, bevor dieser Vscan-Server verwendet werden kann.
9. Aktivieren Sie das Kontrollkästchen Windows Installer-Protokoll anzeigen\*, wenn Sie die Installationsprotokolle anzeigen möchten.
10. Wählen Sie **Fertig stellen**, um die Installation zu beenden und den InstallShield-Assistenten zu schließen.

Das Symbol **Configure ONTAP LIFs** wird auf dem Desktop gespeichert, um die ONTAP LIFs zu konfigurieren.

11. Fügen Sie dem Antivirus Connector eine SVM hinzu. Sie können dem VirenschutzConnector eine SVM hinzufügen, indem Sie entweder eine ONTAP-Management-LIF hinzufügen, die zum Abrufen der Liste der Daten-LIFs abgefragt wird, oder die Daten-LIF oder LIFs direkt konfigurieren. Wenn die ONTAP Management LIF konfiguriert ist, müssen Sie außerdem die Abfrageinformationen und die Anmeldeinformationen des ONTAP Administratorkontos angeben.

- Vergewissern Sie sich, dass die Management-LIF oder die IP-Adresse der SVM für aktiviert ist `management-https`. Dies ist nicht erforderlich, wenn Sie nur die Daten-LIFs konfigurieren.
- Vergewissern Sie sich, dass Sie ein Benutzerkonto für die HTTP-Anwendung erstellt und eine Rolle zugewiesen haben, die (mindestens schreibgeschützt) Zugriff auf das hat `/api/network/ip/interfaces` REST-API: Weitere Informationen zum Erstellen eines Benutzers finden Sie im ["Rolle für Sicherheits-Login erstellen"](#) Und ["Sicherheits-Login erstellen"](#) ONTAP-man-Pages.



Sie können den Domänenbenutzer auch als Konto verwenden, indem Sie eine SVM für einen Authentifizierungstunnel für eine administrative SVM hinzufügen. Weitere Informationen finden Sie im ["Sicherheit Login Domain-Tunnel erstellen"](#) ONTAP-man-Page verwenden oder `/api/security/accouts` Und `/api/security/roles` REST-APIs zum Konfigurieren des Administratorkontos und der Rolle.

## Schritte

1. Klicken Sie mit der rechten Maustaste auf das Symbol **ONTAP-LIFs konfigurieren**, das nach Abschluss der Installation des Virenschutzanschlusses auf Ihrem Desktop gespeichert wurde, und wählen Sie dann **als Administrator ausführen** aus.
2. Wählen Sie im Dialogfeld ONTAP LIFs konfigurieren den bevorzugten Konfigurationstyp aus und führen Sie dann die folgenden Aktionen durch:

Um diesen Typ von LIF zu erstellen...	Führen Sie diese Schritte aus...
Daten-LIF	<ol style="list-style-type: none"><li>a. „Rolle“ auf „Daten“ setzen</li><li>b. Stellen Sie das „Datenprotokoll“ auf „cifs“ ein.</li><li>c. Firewall-Richtlinie auf „Daten“ setzen</li><li>d. Setzen Sie „Service Policy“ auf „default-Data-files“</li></ol>
Management-LIF	<ol style="list-style-type: none"><li>a. „Rolle*“ auf „Daten“ setzen</li><li>b. Stellen Sie „Datenprotokoll“ auf „keine“ ein.</li><li>c. Firewall-Richtlinie auf „Management“ setzen</li><li>d. Service-Richtlinie auf Standardmanagement setzen</li></ol>

Weitere Informationen ["Erstellen einer LIF"](#).

Nachdem Sie eine LIF erstellt haben, geben Sie die Daten- oder Management-LIF- oder IP-Adresse der hinzuzufügenden SVM ein. Sie können auch die Cluster-Management-LIF eingeben. Wenn Sie die Cluster-Management-LIF angeben, können alle SVMs innerhalb des Clusters, die SMB verwenden, den Vscan-Server verwenden.



Wenn Kerberos-Authentifizierung für Vscan-Server erforderlich ist, muss jede SVM-Daten-LIF über einen eindeutigen DNS-Namen verfügen. Sie müssen diesen Namen als Server-Principal-Name (SPN) im Windows Active Directory registrieren. Wenn für jede Daten-LIF kein eindeutiger DNS-Name verfügbar oder als SPN registriert ist, verwendet der Vscan-Server den NT LAN Manager-Mechanismus zur Authentifizierung. Wenn Sie die DNS-Namen und SPNs nach der Verbindung mit dem Vscan-Server hinzufügen oder ändern, müssen Sie den Antivirus Connector-Dienst auf dem Vscan-Server neu starten, um die Änderungen anzuwenden.

3. Geben Sie zum Konfigurieren einer Management-LIF die Abfragedauer in Sekunden ein. Die Abfragedauer ist die Häufigkeit, mit der der Antivirus Connector auf Änderungen an den SVMs oder der LIF-Konfiguration des Clusters prüft. Das standardmäßige Abfrageintervall beträgt 60 Sekunden.
4. Geben Sie den Namen und das Passwort des ONTAP Administratorkontos ein, um eine Management-LIF zu konfigurieren.
5. Klicken Sie auf **Test**, um die Verbindung zu überprüfen und die Authentifizierung zu überprüfen. Die Authentifizierung wird nur für eine Management-LIF-Konfiguration verifiziert.
6. Klicken Sie auf **Update**, um die LIF zur Liste der LIFs hinzuzufügen, zu denen Sie die Abfrage durchführen oder eine Verbindung herstellen möchten.
7. Klicken Sie auf **Speichern**, um die Verbindung zur Registrierung zu speichern.
8. Klicken Sie auf **Export**, wenn Sie die Liste der Verbindungen in eine Registry-Import- oder Registry-Export-Datei exportieren möchten. Dies ist nützlich, wenn mehrere Vscan-Server denselben Satz an Management- oder Daten-LIFs verwenden.

Siehe ["Konfigurieren Sie die Seite ONTAP Antivirus Connector"](#) Für Konfigurationsoptionen.

## Konfigurieren Sie den ONTAP-Virenschutzanschluss

Konfigurieren Sie den ONTAP Antivirus Connector so, dass eine oder mehrere Storage Virtual Machines (SVMs) angegeben werden, zu denen Sie eine Verbindung herstellen möchten, indem Sie entweder die ONTAP Management-LIF eingeben, Abfrageinformationen und die Anmeldedaten des ONTAP Administratorkontos oder nur die Daten-LIF eingeben. Sie können auch die Details einer SVM-Verbindung ändern oder eine SVM-Verbindung entfernen. Standardmäßig verwendet der ONTAP Antivirus Connector REST-APIs, um die Liste der Daten-LIFs abzurufen, wenn die ONTAP Management-LIF konfiguriert ist.

### Ändern Sie die Details einer SVM-Verbindung

Sie können die Details einer SVM-Verbindung (Storage Virtual Machine) aktualisieren, die dem VirenschutzConnector hinzugefügt wurde, indem Sie die ONTAP-Verwaltungs-LIF und die Abfrageinformationen ändern. Sie können die Daten-LIFs nicht aktualisieren, nachdem sie hinzugefügt wurden. Zum Aktualisieren der Daten-LIFs müssen Sie sie zunächst entfernen und sie dann erneut mit der neuen LIF oder IP-Adresse hinzufügen.

### Bevor Sie beginnen

Vergewissern Sie sich, dass Sie ein Benutzerkonto für die HTTP-Anwendung erstellt und eine Rolle zugewiesen haben, die (mindestens schreibgeschützt) Zugriff auf das `/api/network/ip/interfaces` REST-API: Weitere Informationen zum Erstellen eines Benutzers finden Sie im ["Rolle für Sicherheits-Login erstellen"](#) Und das ["Sicherheits-Login erstellen"](#) Befehle. Sie können den Domänenbenutzer auch als Konto

verwenden, indem Sie eine SVM für einen Authentifizierungstunnel für eine administrative SVM hinzufügen. Weitere Informationen finden Sie im ["Sicherheit Login Domain-Tunnel erstellen"](#) ONTAP-Hauptseite.

### Schritte

1. Klicken Sie mit der rechten Maustaste auf das Symbol **ONTAP-LIFs konfigurieren**, das nach Abschluss der Installation des Virenschutzanschlusses auf Ihrem Desktop gespeichert wurde, und wählen Sie dann **als Administrator ausführen** aus. Das Dialogfeld ONTAP LIFs konfigurieren wird geöffnet.
2. Wählen Sie die SVM-IP-Adresse aus, und klicken Sie dann auf **Update**.
3. Aktualisieren Sie die Informationen nach Bedarf.
4. Klicken Sie auf **Speichern**, um die Verbindungsdetails in der Registrierung zu aktualisieren.
5. Klicken Sie auf **Export**, wenn Sie die Liste der Verbindungen in einen Registry-Import oder eine Registry-Exportdatei exportieren möchten. Dies ist nützlich, wenn mehrere Vscan-Server denselben Satz an Management- oder Daten-LIFs verwenden.

### Entfernen Sie eine SVM-Verbindung aus dem Antivirus Connector

Wenn Sie keine SVM-Verbindung mehr benötigen, können Sie sie entfernen.

### Schritte

1. Klicken Sie mit der rechten Maustaste auf das Symbol **ONTAP-LIFs konfigurieren**, das nach Abschluss der Installation des Virenschutzanschlusses auf Ihrem Desktop gespeichert wurde, und wählen Sie dann **als Administrator ausführen** aus. Das Dialogfeld ONTAP LIFs konfigurieren wird geöffnet.
2. Wählen Sie eine oder mehrere SVM-IP-Adressen aus, und klicken Sie dann auf **Entfernen**.
3. Klicken Sie auf **Speichern**, um die Verbindungsdetails in der Registrierung zu aktualisieren.
4. Klicken Sie auf **Export**, wenn Sie die Liste der Verbindungen in eine Registry-Import- oder Registry-Export-Datei exportieren möchten. Dies ist nützlich, wenn mehrere Vscan-Server denselben Satz an Management- oder Daten-LIFs verwenden.

### Fehlerbehebung

#### Bevor Sie beginnen

Wenn Sie in diesem Verfahren Registrierungswerte erstellen, verwenden Sie den rechten Fensterbereich.

Sie können Antivirus Connector-Protokolle für Diagnosezwecke aktivieren oder deaktivieren. Diese Protokolle sind standardmäßig deaktiviert. Um die Leistung zu verbessern, sollten Sie die Antivirus Connector-Protokolle deaktiviert halten und nur für kritische Ereignisse aktivieren.

### Schritte

1. Wählen Sie **Start**, geben Sie "regedit" in das Suchfeld ein, und wählen Sie dann `regedit.exe` in der Liste Programme.
2. Suchen Sie in **Registrierungs-Editor** den folgenden Unterschlüssel für den ONTAP Antivirus Connector:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Erstellen Sie Registrierungswerte, indem Sie den Typ, den Namen und die Werte angeben, die in der folgenden Tabelle aufgeführt sind:

Typ	Name	Werte
-----	------	-------

Zeichenfolge	Tracepath	c:\avshim.log
--------------	-----------	---------------

Dieser Registrierungswert kann jeder andere gültige Pfad sein.

- Erstellen Sie einen weiteren Registrierungswert, indem Sie den Typ, den Namen, die Werte und die Protokollinformationen in der folgenden Tabelle angeben:

Typ	Name	Kritische Protokollierung	Zwischenprotokollierung	Ausführliche Protokollierung
DWORD	Tracelevel	1	2 oder 3	4

Dadurch werden die Protokolle des Antivirus Connector aktiviert, die unter dem im TracePath in Schritt 3 angegebenen Pfadwert gespeichert werden.

- Deaktivieren Sie Antivirus Connector-Protokolle, indem Sie die in Schritt 3 und 4 erstellten Registrierungswerte löschen.
- Erstellen Sie einen weiteren Registrierungswert vom Typ "MULTI\_SZ" mit dem Namen "LogRotation" (ohne Anführungszeichen). In „LogRotation“ Geben Sie „logFileSize:1“ als Eintrag für die Rotationsgröße an (wobei 1 für 1MB steht) und geben Sie in der nächsten Zeile „logFileCount:5“ als an an an Eingabe für Rotationsgrenze (5 ist die Grenze).



Diese Werte sind optional. Wenn sie nicht angegeben werden, werden für die Rotationsgröße bzw. die Rotationsgrenze Standardwerte von 20MB und 10 Dateien verwendet. Die angegebenen Ganzzahlwerte enthalten keine Dezimalwerte oder Bruchwerte. Wenn Sie Werte angeben, die höher als die Standardwerte sind, werden stattdessen die Standardwerte verwendet.

- Um die benutzerdefinierte Protokollrotation zu deaktivieren, löschen Sie die Registrierungswerte, die Sie in Schritt 6 erstellt haben.

## Anpassbares Banner

Ein benutzerdefiniertes Banner ermöglicht es Ihnen, eine rechtsverbindliche Aussage und einen Haftungsausschluss für den Systemzugriff im Fenster *Configure ONTAP LIF API* zu platzieren.

### Schritt

- Ändern Sie das Standard-Banner, indem Sie den Inhalt im aktualisieren `banner.txt` Datei im Installationsverzeichnis speichern und dann die Änderungen speichern. Sie müssen das Fenster ONTAP LIF-API konfigurieren erneut öffnen, um die Änderungen im Banner anzuzeigen.

## Aktivieren Sie den Modus Erweiterte Verordnung (EO)

Sie können den EO-Modus (Extended Ordinance) für einen sicheren Betrieb aktivieren und deaktivieren.

### Schritte

- Wählen Sie **Start**, geben Sie "regedit" in das Suchfeld ein, und wählen Sie dann aus `regedit.exe` In der Liste Programme.
- Suchen Sie in **Registrierungs-Editor** den folgenden Unterschlüssel für den ONTAP Antivirus Connector:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP

- Erstellen Sie im rechten Fensterbereich einen neuen Registrierungswert vom Typ "DWORD" mit dem Namen "EO\_Mode" (ohne Anführungszeichen) und dem Wert "1" (ohne Anführungszeichen), um den EO-Modus zu aktivieren oder den Wert "0" (ohne Anführungszeichen), um den EO-Modus zu deaktivieren.



Standardmäßig, wenn die EO\_Mode Registrierungseintrag fehlt, EO-Modus ist deaktiviert. Wenn Sie den EO-Modus aktivieren, müssen Sie sowohl den externen Syslog-Server als auch die gegenseitige Zertifikatauthentifizierung konfigurieren.

## Konfigurieren Sie den externen Syslog-Server

### Bevor Sie beginnen

Beachten Sie, dass Sie beim Erstellen von Registrierungswerten in diesem Verfahren den rechten Fensterbereich verwenden.

### Schritte

- Wählen Sie **Start**, geben Sie "regedit" in das Suchfeld ein, und wählen Sie dann aus `regedit.exe` In der Liste Programme.
- Erstellen Sie in **Registrierungs-Editor** den folgenden Unterschlüssel für den ONTAP Antivirus Connector für die Syslog-Konfiguration: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
- Erstellen Sie einen Registrierungswert, indem Sie den Typ, den Namen und den Wert wie in der folgenden Tabelle dargestellt angeben:

Typ	Name	Wert
DWORD	Syslog_aktiviert	1 oder 0

Bitte beachten Sie, dass ein Wert „1“ das Syslog aktiviert und mit einem Wert „0“ deaktiviert.

- Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name
REG_SZ	Syslog_Host

Geben Sie die IP-Adresse oder den Domännennamen des Syslog-Hosts für das Wertfeld an.

- Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name
REG_SZ	Syslog_Port

Geben Sie im Feld Wert die Portnummer an, auf der der Syslog-Server ausgeführt wird.

- Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten

Informationen bereitstellen:

Typ	Name
REG_SZ	Syslog_Protocol

Geben Sie das Protokoll, das auf dem Syslog-Server verwendet wird, entweder „tcp“ oder „udp“ in das Wertfeld ein.

7. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_Level	2	5	6	7

8. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name	Wert
DWORD	Syslog_tls	1 oder 0

Bitte beachten Sie, dass ein Wert von „1“ Syslog mit Transport Layer Security (TLS) aktiviert und ein Wert von „0“ das Syslog mit TLS deaktiviert.

**Stellen Sie sicher, dass ein konfigurierter externer Syslog-Server reibungslos ausgeführt wird**

- Wenn der Schlüssel fehlt oder einen Nullwert hat:
  - Das Protokoll ist standardmäßig auf „tcp“ eingestellt.
  - Der Port ist standardmäßig auf "514" für einfaches "tcp/udp" und standardmäßig auf "6514" für TLS.
  - Die Syslog-Ebene ist standardmäßig auf 5 (LOG\_NOTICE) eingestellt.
- Sie können bestätigen, dass Syslog aktiviert ist, indem Sie überprüfen, ob das `syslog_enabled` Wert ist „1“. Wenn der `syslog_enabled` Der Wert ist „1“, Sie sollten sich beim konfigurierten Remote-Server anmelden können, unabhängig davon, ob der EO-Modus aktiviert ist.
- Wenn der EO-Modus auf „1“ eingestellt ist und Sie den ändern `syslog_enabled` Wert von „1“ bis „0“, gilt:
  - Sie können den Service nicht starten, wenn syslog im EO-Modus nicht aktiviert ist.
  - Wenn das System in einem stabilen Zustand ausgeführt wird, erscheint eine Warnung, die besagt, dass Syslog im EO-Modus nicht deaktiviert werden kann und syslog zwangsweise auf „1“ gesetzt ist, was Sie in der Registrierung sehen können. In diesem Fall sollten Sie zuerst den EO-Modus deaktivieren und dann syslog deaktivieren.
- Wenn der Syslog-Server bei Aktivierung von EO-Modus und Syslog nicht erfolgreich ausgeführt werden kann, wird der Dienst nicht mehr ausgeführt. Dies kann aus einem der folgenden Gründe auftreten:
  - Ein ungültiger oder kein `syslog_Host` ist konfiguriert.
  - Ein ungültiges Protokoll außer UDP oder TCP ist konfiguriert.
  - Eine Portnummer ist ungültig.



- Bei einer TCP- oder TLS-über-TCP-Konfiguration schlägt die Verbindung fehl, wenn der Server den IP-Port nicht abhört, und der Dienst wird heruntergefahren.

## Konfigurieren Sie die Authentifizierung des gegenseitigen X.509-Zertifikats

X.509-zertifikatbasierte gegenseitige Authentifizierung ist für die SSL-Kommunikation (Secure Sockets Layer) zwischen dem Antivirus Connector und ONTAP im Verwaltungspfad möglich. Wenn der EO-Modus aktiviert ist und das Zertifikat nicht gefunden wird, wird der AV-Connector beendet. Führen Sie die folgenden Schritte auf dem Antivirus Connector durch:

### Schritte

1. Der Antivirus Connector sucht nach dem Clientzertifikat des Virenschutzanschlusses und dem Zertifikat der Zertifizierungsstelle (CA) für den NetApp-Server im Verzeichnispfad, von dem aus der Virenschutzanschluss das Installationsverzeichnis ausführt. Kopieren Sie die Zertifikate in diesen festen Verzeichnispfad.
2. Betten Sie das Clientzertifikat und seinen privaten Schlüssel in das PKCS12-Format ein und benennen Sie es mit „AV\_Client.P12“.
3. Stellen Sie sicher, dass das zum Signieren des Zertifikats für den NetApp-Server verwendete Zertifizierungsstellenzertifikat (zusammen mit jeder Zwischenzertifizierungsstelle bis zur Stammzertifizierungsstelle) im PEM-Format (Privacy Enhanced Mail) mit dem Namen „ONTAP\_CA.pem“ vorliegt. Platzen Sie es im Installationsverzeichnis des Antivirus Connectors. Installieren Sie auf dem NetApp ONTAP-System das CA-Zertifikat (zusammen mit einer Zwischenzertifizierungsberechtigung bis zur Stammzertifizierungsstelle), mit dem das Clientzertifikat für den Antivirus-Connector unter „ONTAP“ als Zertifikat vom Typ „Client-CA“ signiert wird.

## 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 eines Clusters erstellen.

#### Was Sie benötigen

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

- Die Liste der privilegierten Benutzer muss das Domain-Benutzerkonto enthalten, das der Vscan-Server zur Verbindung mit der SVM verwendet.
- Sobald der Scanner-Pool konfiguriert ist, überprüfen Sie den Verbindungsstatus zu den Servern.

## 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 Scanner-Pools, die für eine einzelne SVM definiert sind, müssen Sie den ONTAP Antivirus Connector mit der logischen Schnittstelle für das SVM-Management oder SVM-Daten konfiguriert haben.
- Für Scanner-Pools, die für alle SVMs in einem Cluster definiert sind, müssen Sie den ONTAP Antivirus Connector mit der Cluster-Management-LIF konfiguriert haben.
- Die Liste der privilegierten Benutzer muss das Domain-Benutzerkonto enthalten, das der Vscan-Server zur Verbindung mit der SVM verwendet.
- Sobald der Scanner-Pool konfiguriert ist, überprüfen Sie den Verbindungsstatus zu den Servern.

### 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 heißt, Sie müssen auf jedem Cluster in einer MetroCluster-Konfiguration primäre und sekundäre Scanner-Pools erstellen. Der sekundäre Pool wird dann aktiv, wenn das Cluster damit beginnt, Daten von der sekundären SVM bereitzustellen. Für Disaster Recovery (DR) ist die Konfiguration ähnlich wie MetroCluster.

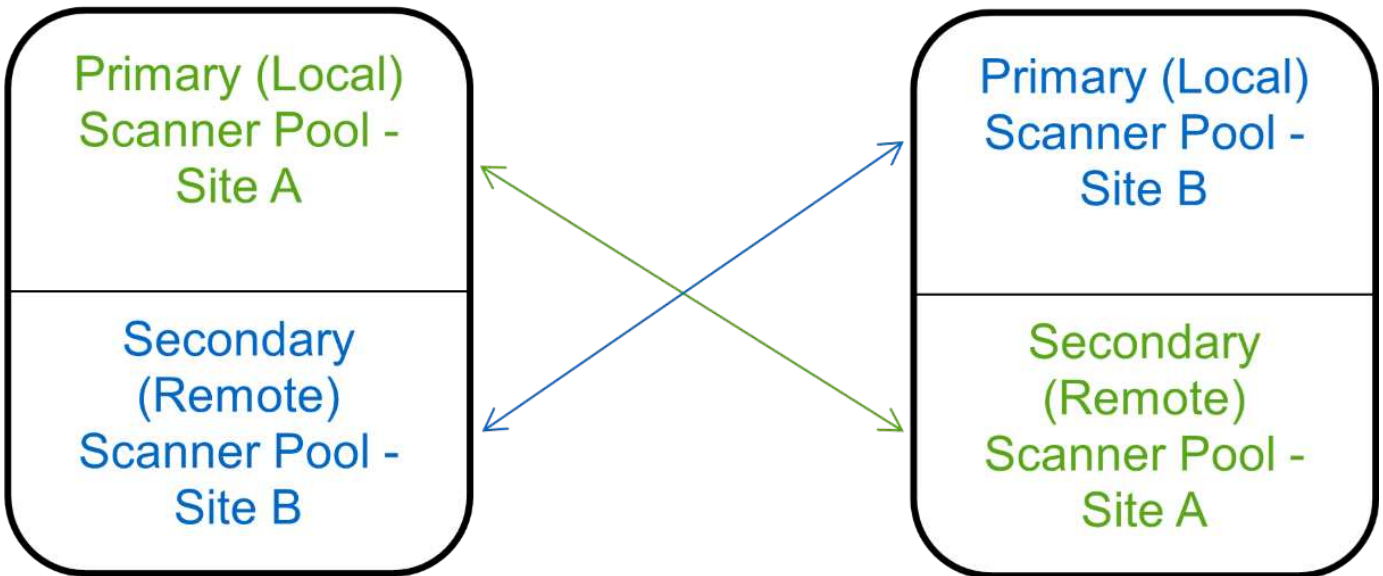
Diese Abbildung zeigt eine typische MetroCluster/DR-Konfiguration.



Site A



Site B



### 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 Scanner-Pool aktivieren, bevor die von ihm definierten Vscan-Server eine Verbindung zu einer

SVM herstellen können.

### Über diese Aufgabe

- Sie können nur eine Scannerrichtlinie auf einen Scannerpool anwenden.
- Wenn Sie einen Scanner-Pool für alle SVMs eines Clusters erstellt haben, müssen Sie für jede SVM einzeln eine Scannerrichtlinie 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.

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.
- Wenn Sie einen Scanner-Pool für alle SVMs eines Clusters erstellt haben, müssen Sie für jede SVM einzeln eine Scannerrichtlinie anwenden.
- Für Disaster Recovery- und MetroCluster-Konfigurationen müssen Sie eine Scannerrichtlinie auf jeden Scanner-Pool im lokalen Cluster und Remote-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 den Remote-Cluster erstellen, müssen Sie den Remote-Cluster in angeben `cluster` Parameter. Der Remote-Cluster kann dann im Katastrophenfall Virenskans übernehmen.

### 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 auch zusammenfassende Informationen zum Scanner-Pool anzeigen.

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

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 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	<code>vserver vscan on-access-policy create</code>
Ändern Sie eine Zugriffsrichtlinie	<code>vserver vscan on-access-policy modify</code>
Aktivieren einer Zugriffsrichtlinie	<code>vserver vscan on-access-policy enable</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>vserver vscan on-access-policy paths-to-exclude add</code>
Löschen Sie die Liste der auszuschließenden Pfade	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
Zeigen Sie die Liste der auszuschließenden Pfade an	<code>vserver vscan on-access-policy paths-to-exclude show</code>
Fügen Sie zur Liste der auszuschließenden Dateierweiterungen hinzu	<code>vserver vscan on-access-policy file-ext-to-exclude add</code>

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

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 anzugeben, wann die Aufgabe ausgeführt wird.

#### Zu diesem Thema behandelt wird

- Sie können beim Erstellen einer Aufgabe einen Zeitplan zuweisen.
- 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.



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



Um eine On-Demand-Aufgabe zu erstellen, muss mindestens eine On-Access-Richtlinie aktiviert sein. Dabei kann es sich um eine Standardrichtlinie oder eine beim Zugriff erstellte Richtlinie handeln.

### Erstellen Sie eine On-Demand-Aufgabe

Eine On-Demand-Aufgabe definiert den Umfang des On-Demand-Virus-Scans. 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.

### Über diese Aufgabe

- Für jede SVM können maximal zehn (10) On-Demand-Aufgaben vorhanden sein, aber nur eine kann aktiv sein.
- Eine On-Demand-Aufgabe erstellt einen Bericht, der Informationen zu den Statistiken zu den Scans enthält. Auf diesen Bericht kann mit einem Befehl oder durch Herunterladen der Berichtsdatei zugegriffen werden, die von der Aufgabe an dem definierten Speicherort erstellt wurde.

### Bevor Sie beginnen

- Dieser muss unbedingt vorhanden sein [Richtlinie beim Zugriff erstellt](#). Dabei kann es sich um eine Standard- oder eine vom Benutzer erstellte Richtlinie handeln. Ohne die Richtlinie für den Zugriff können Sie den Scan nicht aktivieren.

### 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 -file-ext-to  
-exclude file_extensions -file-ext-to-include file_extensions -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 im ["Befehlsreferenz"](#).

Mit dem folgenden Befehl wird eine On-Demand-Aufgabe mit dem Namen erstellt Task1 Auf der `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

Sie können eine Aufgabe erstellen, ohne einen Zeitplan zuzuweisen, und die verwenden `vserver vscan on-demand-task schedule` Befehl zum Zuweisen eines Zeitplans oder Hinzufügen eines Zeitplans beim Erstellen 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.
```

Um den Status des Jobs anzuzeigen, verwenden Sie die `job show` Befehl. Der `job pause` Und `job resume` Befehle bzw. den Job anhalten und neu starten; der `job stop` Befehl beendet den Job.

## 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.

### Bevor Sie beginnen

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...
Erstellen Sie eine On-Demand-Aufgabe	<code>vserver vscan on-demand-task create</code>
Ändern Sie eine Aufgabe nach Bedarf	<code>vserver vscan on-demand-task modify</code>
Löschen Sie eine On-Demand-Aufgabe	<code>vserver vscan on-demand-task delete</code>
Führen Sie eine On-Demand-Aufgabe aus	<code>vserver vscan on-demand-task run</code>
On-Demand-Aufgabe planen	<code>vserver vscan on-demand-task schedule</code>
Aufheben der Planung einer On-Demand-Aufgabe	<code>vserver vscan on-demand-task unschedule</code>
Zusammenfassung und Details für eine On-Demand-Aufgabe anzeigen	<code>vserver vscan on-demand-task show</code>
On-Demand-Berichte anzeigen	<code>vserver vscan on-demand-task report show</code>

On-Demand-Berichte löschen	<code>vserver vscan on-demand-task report delete</code>
----------------------------	---

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

## Best Practices zur Konfiguration der Off-Box-Antivirus-Funktion in ONTAP

Beachten Sie die folgenden Empfehlungen zur Konfiguration der Off-Box-Funktion in ONTAP.

- Beschränken Sie privilegierte Benutzer auf Virenprüfungen. Normale Benutzer sollten von der Verwendung privilegierter Benutzeranmeldeinformationen abschrecken. Diese Einschränkung kann erreicht werden, indem die Anmelderechte für privilegierte Benutzer in Active Directory deaktiviert werden.
- Privilegierte Benutzer müssen nicht Teil einer Benutzergruppe sein, die über eine große Anzahl von Rechten in der Domäne verfügt, z. B. der Administratorengruppe oder der Gruppe der Backup-Operatoren. Privilegierte Benutzer dürfen nur durch das Storage-System validiert werden, damit sie Vscan-Serververbindungen herstellen und auf Dateien für Virenprüfungen zugreifen können.
- Verwenden Sie die Computer, auf denen Vscan-Server ausgeführt werden, nur für Virenschans. Um die allgemeine Nutzung zu verhindern, deaktivieren Sie die Windows-Terminaldienste und andere Remote-Zugriffsbestimmungen auf diesen Computern und gewähren das Recht, neue Software nur Administratoren auf diesen Computern zu installieren.
- Widmen Sie die Vscan-Server Virenprüfungen und verwenden Sie sie nicht für andere Vorgänge, z. B. Backups. Sie können den Vscan-Server als virtuelle Maschine (VM) ausführen. Wenn Sie den Vscan-Server als VM ausführen, stellen Sie sicher, dass die der VM zugewiesenen Ressourcen nicht gemeinsam genutzt werden und zum Durchführen eines Virus-Scans ausreichen.
- Bereitstellen einer ausreichenden CPU-, Arbeitsspeicher- und Festplattenkapazität für den Vscan-Server, um eine übermäßige Zuweisung von Ressourcen zu vermeiden. Die meisten Vscan-Server sind für die Verwendung mehrerer CPU-Core-Server und die Verteilung der Last über die CPUs konzipiert.
- NetApp empfiehlt für die Verbindung von SVM zu dem Vscan-Server die Verwendung eines dedizierten Netzwerks mit einem privaten VLAN, damit der Scan-Verkehr nicht durch anderen Client-Netzwerk-Traffic beeinträchtigt wird. Erstellen Sie eine separate Netzwerkkarte (NIC), die speziell für das Virenschutz-VLAN auf dem Vscan-Server und die logische Datenschnittstelle auf der SVM eingerichtet ist. Dieser Schritt vereinfacht die Administration und die Fehlerbehebung bei Netzwerkproblemen. Der Antivirus-Verkehr sollte über ein privates Netzwerk getrennt werden. Der Virenschutz-Server sollte so konfiguriert werden, dass er mit dem Domänencontroller (DC) und ONTAP auf eine der folgenden Arten kommuniziert:
  - Das DC sollte über das private Netzwerk, das zur Trennung des Datenverkehrs verwendet wird, mit den Antivirenservers kommunizieren.
  - Der DC- und Antivirus-Server sollten über ein anderes Netzwerk (nicht das zuvor erwähnte private Netzwerk) kommunizieren, das nicht mit dem CIFS-Client-Netzwerk identisch ist.
  - Um die Kerberos-Authentifizierung für die Virenkommunikation zu aktivieren, erstellen Sie einen DNS-Eintrag für die privaten LIFs und einen Dienstprinzipalnamen auf dem DC, der dem für die private LIF erstellten DNS-Eintrag entspricht. Verwenden Sie diesen Namen, wenn Sie eine LIF zum Antivirus Connector hinzufügen. Der DNS sollte in der Lage sein, einen eindeutigen Namen für jede private LIF zurückzugeben, die mit dem Antivirus Connector verbunden ist.



Wenn die LIF für Vscan-Datenverkehr für Client-Datenverkehr auf einem anderen Port als der LIF konfiguriert ist, kann die Vscan LIF ein Failover auf einen anderen Node durchführen, wenn ein Port-Ausfall auftritt. Die Änderung bewirkt, dass der Vscan-Server vom neuen Knoten nicht erreichbar ist und die Scanbenachrichtigungen für Dateivorgänge auf dem Knoten fehlschlagen. Vergewissern Sie sich, dass der Vscan-Server über mindestens eine LIF auf einem Node erreichbar ist, damit er Scananforderungen für Dateivorgänge verarbeiten kann, die auf diesem Node ausgeführt werden.

- Verbinden Sie das NetApp Storage-System und den Vscan-Server über mindestens ein 1-GbE-Netzwerk.
- Verbinden Sie in einer Umgebung mit mehreren Vscan-Servern alle Server mit ähnlichen leistungsstarken Netzwerkverbindungen. Die Verbindung der Vscan-Server verbessert die Leistung durch die Möglichkeit der Lastverteilung.
- Für Remote-Standorte und Zweigstellen empfiehlt NetApp die Verwendung eines lokalen Vscan-Servers statt eines externen Vscan-Servers, da ersterer sich ideal für eine hohe Latenz eignet. Wenn die Kosten ein Faktor sind, verwenden Sie einen Laptop oder PC für einen moderaten Virenschutz. Sie können regelmäßige vollständige Filesystem-Scans planen, indem Sie die Volumes oder qtrees gemeinsam nutzen und von jedem System am Remote-Standort aus scannen.
- Verwenden Sie mehrere Vscan-Server, um die Daten auf der SVM für Lastverteilung und Redundanz zu scannen. Die Menge der CIFS-Workloads und der daraus resultierende Virenschutzdatenverkehr variieren je SVM. Überwachen Sie CIFS und die Latenz beim Virenschannen auf dem Storage Controller. Überwachen Sie den Trend der Ergebnisse im Laufe der Zeit. Wenn die CIFS-Latenz und die Latenz von Virenschans aufgrund von CPU- oder Anwendungswarteschlangen auf den Vscan-Servern über die Trendschwellenwerte hinaus zunimmt, kann es bei CIFS-Clients zu langen Wartezeiten kommen. Fügen Sie zusätzliche Vscan-Server hinzu Um die Last zu verteilen.
- Installieren Sie die neueste Version des ONTAP-Virenschutzanschlusses.
- Halten Sie Virenschutz-Engines und Definitionen auf dem neuesten Stand. Wenden Sie sich an Partner, um Empfehlungen zu erhalten, wie oft Sie Updates durchführen sollten.
- In einer mandantenfähigen Umgebung kann ein Scanner-Pool (Pool von Vscan Servern) mit mehreren SVMs genutzt werden, vorausgesetzt die Vscan Server und SVMs sind Teil derselben Domäne oder derselben vertrauenswürdigen Domäne.
- Die Virenschutzrichtlinie für infizierte Dateien sollte auf „löschen“ oder „Quarantäne“ gesetzt werden, was der von den meisten Antivirenanbietern festgelegte Standardwert ist. Wenn das "vscan-fileop-Profil" auf "write\_only" gesetzt ist und eine infizierte Datei gefunden wird, bleibt die Datei in der Freigabe und kann geöffnet werden, da das Öffnen einer Datei keinen Scan auslöst. Die Virenprüfung wird erst ausgelöst, nachdem die Datei geschlossen wurde.
- Der `scan-engine timeout` Der Wert muss kleiner sein als der `scanner-pool request-timeout` Wert: Wenn sie auf einen höheren Wert eingestellt ist, kann der Zugriff auf Dateien verzögert werden und möglicherweise eine Zeitverzögerung erreichen. Um dies zu vermeiden, konfigurieren Sie das `scan-engine timeout` Bis 5 Sekunden weniger als der `scanner-pool request-timeout` Wert:  
Anweisungen zum Ändern des finden Sie in der Dokumentation des Scannerherstellers `scan-engine timeout` Einstellungen. Der `scanner-pool timeout` Kann mit dem folgenden Befehl im erweiterten Modus und durch Angabe des entsprechenden Werts für geändert werden `request-timeout` Parameter:  
`vserver vscan scanner-pool modify.`
- Bei einer Umgebung, die auf Scan-Workloads beim Zugriff ausgelegt ist und On-Demand-Scans erfordert, empfiehlt NetApp, den On-Demand-Scan-Job außerhalb der Spitzenzeiten zu planen, um zusätzliche Belastungen der vorhandenen Virenschutz-Infrastruktur zu vermeiden.

Weitere Informationen zu Best Practices für Partner finden Sie unter ["Partnerlösungen von Vscan"](#).

# Aktivieren Sie das Virensuchen auf einer SVM

Sie müssen den Virenskan auf einer SVM aktivieren, bevor ein Zugriff oder On-Demand-Scan ausgeführt werden kann.

## Schritte

1. Virenprüfung auf einer SVM aktivieren:

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



Sie können das verwenden `vserver vscan disable` Befehl zum Deaktivieren des Virenskans, 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.

### Was Sie benötigen

Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

### Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. 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.

### Bevor Sie beginnen

Zum Anzeigen des Vscan-Ereignisprotokolls 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.

## Überwachung und Fehlerbehebung 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	<code>vserver vscan connection-status show</code>
Details zu Vscan-Serververbindungen anzeigen	<code>vserver vscan connection-status show-all</code>
Details für verbundene Vscan-Server anzeigen	<code>vserver vscan connection-status show-connected</code>
Details zu verfügbaren Vscan-Servern anzeigen, die nicht verbunden sind	<code>vserver vscan connection-status show-not-connected</code>

Weitere Informationen zu diesen Befehlen finden Sie im ["ONTAP-man-Pages"](#).

## Fehlerbehebung beim Virensan

Bei häufigen Problemen mit der Virenprüfung gibt es mögliche Ursachen und Möglichkeiten, diese zu lösen. Virus-Scan wird auch als Vscan bezeichnet.

Problem	Wie man es löst
Die Vscan-Server können keine Verbindung herstellen Dem Storage-System Clustered ONTAP	Prüfen Sie, ob die Scannerpoolkonfiguration die IP-Adresse des Vscan-Servers angibt. Überprüfen Sie auch, ob die zulässigen privilegierten Benutzer in der Scannerpoolliste aktiv sind. Führen Sie zum Überprüfen des Scannerpools den aus <code>vserver vscan scanner-pool show</code> In der Eingabeaufforderung des Storage-Systems. Wenn die Vscan-Server immer noch keine Verbindung herstellen können, liegt möglicherweise ein Problem mit dem Netzwerk vor.
Bei Clients beobachten wir eine hohe Latenz.	Es ist wahrscheinlich an der Zeit, dem Scanner-Pool weitere Vscan-Server hinzuzufügen.
Es werden zu viele Scans ausgelöst.	Ändern Sie den Wert des <code>vscan-fileop-profile</code> Parameter, um die Anzahl der für Virenprüfungen überwachten Dateioperationen zu beschränken.
Einige Dateien werden nicht gescannt.	Überprüfen Sie die Zugangsrichtlinie. Es ist möglich, dass der Pfad für diese Dateien zur Pfadausschlussliste hinzugefügt wurde oder dass ihre Größe den konfigurierten Wert für Ausschlüsse überschreitet. Führen Sie zum Überprüfen der Zugriffsrichtlinie den aus <code>vserver vscan on-access-policy show</code> In der Eingabeaufforderung des Storage-Systems.



Dateizugriff wurde verweigert.	Prüfen Sie, ob die Einstellung „ <i>Scan-mandatory</i> “ in der Richtlinienkonfiguration angegeben ist. Diese Einstellung verweigert den Datenzugriff, wenn keine Vscan-Server verbunden sind. Ändern Sie die Einstellung nach Bedarf.
--------------------------------	--

## Überwachen Sie den Status und die Performance-Aktivitäten

Sie können die kritischen Aspekte des Vscan-Moduls überwachen, z. B. den Verbindungsstatus des Vscan-Servers, Der Zustand der Vscan-Server und die Anzahl der gescannten Dateien. Diese Informationen helfen Sie diagnostizieren Probleme im Zusammenhang mit dem Vscan-Server.

### Anzeigen von Vscan-Serververbindungsinformationen

Sie können den Verbindungsstatus von Vscan-Servern anzeigen, um die bereits verwendeten Verbindungen zu verwalten Und die verfügbaren Verbindungen. Verschiedene Befehle zeigen Informationen an Informationen zum Verbindungsstatus von Vscan-Servern.

Befehl...	Angezeigte Informationen...
<code>vserver vscan connection-status show</code>	Zusammenfassung des Verbindungsstatus
<code>vserver vscan connection-status show-all</code>	Detaillierte Informationen zum Verbindungsstatus
<code>vserver vscan connection-status show-not-connected</code>	Status der verfügbaren, aber nicht verbundenen Verbindungen
<code>vserver vscan connection-status show-connected</code>	Informationen zum angeschlossenen Vscan-Server

Weitere Informationen zu diesen Befehlen finden Sie im ["Man-Pages"](#).

### Vscan-Server-Statistiken anzeigen

Sie können Vscan-Server-spezifische Statistiken anzeigen, um die Leistung zu überwachen und Probleme im Zusammenhang mit zu diagnostizieren Virus-Scan. Sie müssen eine Datenprobe erfassen, bevor Sie den verwenden können `statistics show` Befehl an Zeigt die Vscan-Server-Statistiken an. Um eine Datenprobe auszufüllen, gehen Sie wie folgt vor:

#### Schritt

1. Führen Sie die aus `statistics start` Befehl und das optional `statistics` Befehl stoppen.

### Anzeigen von Statistiken für Vscan-Serveranfragen und -Latenzen

Sie können ONTAP verwenden `offbox_vscan` Zähler pro SVM zur Überwachung der Vscan-Rate Serveranfragen, die pro Sekunde versendet und empfangen werden, und die Server-Latenzen über alle Vscan hinweg Server: Führen Sie zum Anzeigen dieser Statistiken den folgenden Schritt aus:

## Schritt

1. Führen Sie die Statistikshow aus `object offbox_vscan -instance SVM` Befehl mit dem folgende Zähler:

Zähler...	Angezeigte Informationen...
<code>scan_request_dispatched_rate</code>	Anzahl der von ONTAP an die Vscan-Server gesendeten Virens Scanner pro Sekunde
<code>scan_noti_received_rate</code>	Anzahl der von ONTAP von den Vscan-Servern zurückempfungenen Virens Scans pro Sekunde
<code>dispatch_latency</code>	Latenz innerhalb von ONTAP, um einen verfügbaren Vscan-Server zu identifizieren und die Anforderung an diesen Vscan-Server zu senden
<code>scan_latency</code>	Round-Trip-Latenz von ONTAP auf den Vscan-Server, einschließlich der Zeit für die Ausführung des Scans

## Beispiel für Statistiken, die von einem ONTAP Offbox vscan-Zähler generiert wurden

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-----
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-----
```

## Anzeigen von Statistiken zu einzelnen Vscan-Serveranfragen und -Latenzen

Sie können ONTAP verwenden `offbox_vscan_server` Zähler auf einem pro SVM, pro Box-Vscan-Server, Und auf Node-Basis, um die Rate der versendeten Vscan-Serveranfragen und die Serverlatenz zu überwachen Jeder Vscan-Server einzeln. Um diese Informationen zu erfassen, führen Sie den folgenden Schritt aus:

## Schritt

1. Führen Sie die aus `statistics show -object offbox_vscan -instance SVM:servername:nodename` Befehl mit den folgenden Zählern:

Zähler...	Angezeigte Informationen...
scan_request_dispatched_rate	Anzahl der von ONTAP gesendeten Virens Scanner
scan_latency	Round-Trip-Latenz von ONTAP auf den Vscan-Server, einschließlich der Zeit für die Ausführung des Scans Zu den Vscan-Servern pro Sekunde

### Beispiel für Statistiken, die von einem ONTAP offbox\_vscan\_Server-Zähler generiert wurden

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-----
scan_request_dispatched_rate 291
scan_latency 3433830us
-----
```

### Anzeigen von Statistiken für die Vscan-Serverauslastung

Sie können auch ONTAP verwenden `offbox_vscan_server` Zähler zur Erfassung der serverseitigen Vscan-Nutzung Statistiken. Diese Statistiken werden auf SVM-, Off-Box- und Vscan-Server- und Node-Basis verfolgt. Sie Einbeziehen der CPU-Auslastung auf dem Vscan-Server, Warteschlangentiefe für Scanvorgänge auf dem Vscan-Server (Aktuell und maximal), verwendeter Speicher und verwendetes Netzwerk. Diese Statistiken werden vom Antivirus Connector an die Statistikzähler in ONTAP weitergeleitet. Sie Auf Daten basieren, die alle 20 Sekunden abgefragt werden und zur Genauigkeit mehrfach erfasst werden müssen; Andernfalls spiegeln die Werte in den Statistiken nur die letzte Abfrage wider. CPU-Auslastung und Warteschlangen Dies ist besonders wichtig für die Überwachung und Analyse. Ein hoher Wert für eine durchschnittliche Warteschlange kann darauf hinweisen, dass der Vscan Server hat einen Engpass. Erfassen von Auslastungsstatistiken für den Vscan-Server auf einem pro SVM, pro-Off-Box-Vscan-Server und pro Node Gehen Sie wie folgt vor:

#### Schritt

1. Sammeln von Auslastungsstatistiken für den Vscan-Server

Führen Sie die `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` Mit dem folgenden Befehl `offbox_vscan_server` Zähler:

Zähler...	Angezeigte Informationen...
scanner_stats_pct_cpu_used	CPU-Auslastung auf dem Vscan-Server

scanner_stats_pct_input_queue_avg	Durchschnittliche Warteschlange von Scananforderungen auf dem Vscan-Server
scanner_stats_pct_input_queue_hiwatermark	Spitzenwarteschlange von Scananforderungen auf dem Vscan-Server
scanner_stats_pct_mem_used	Auf dem Vscan-Server verwendeter Speicher
scanner_stats_pct_network_used	Auf dem Vscan-Server verwendetes Netzwerk

### Beispiel für Auslastungsstatistiken für den Vscan-Server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
```

```
-----
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
-----
```

## Copyright-Informationen

Copyright © 2024 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 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.