# Über den Virenschutz von NetApp

ONTAP 9

NetApp
February 12, 2026

# Inhalt


Über den Virenschutz von NetApp . . . 1
Erfahren Sie mehr über das Virenscannen von NetApp mit ONTAP Vscan . . . 1
So funktioniert die Virenprüfung . . . 1
Virenscan-Workflow mit ONTAP Vscan . . . 2
Antivirus-Architektur mit ONTAP Vscan . . . 3
Vscan Server-Software . . . 4
Vscan-Softwareeinstellungen . . . 4
Erfahren Sie mehr über die Partnerlösungen von ONTAP Vscan . . . 6

# Über den Virenschutz von NetApp

## Erfahren Sie mehr über das Virenscannen von NetApp mit ONTAP Vscan

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.

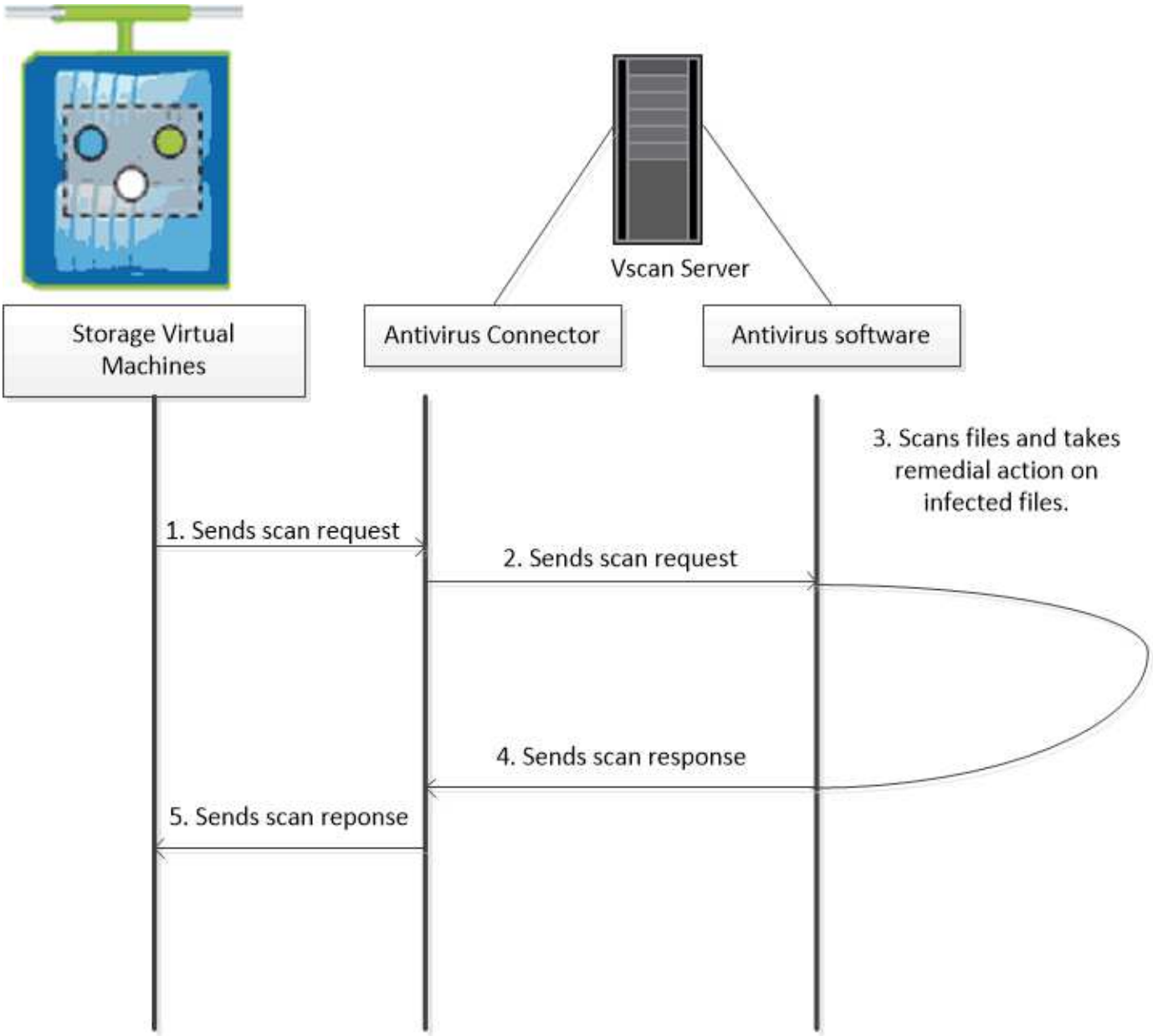
  Das Scannen beim Zugriff wird für NFS nicht unterstützt.

- 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.

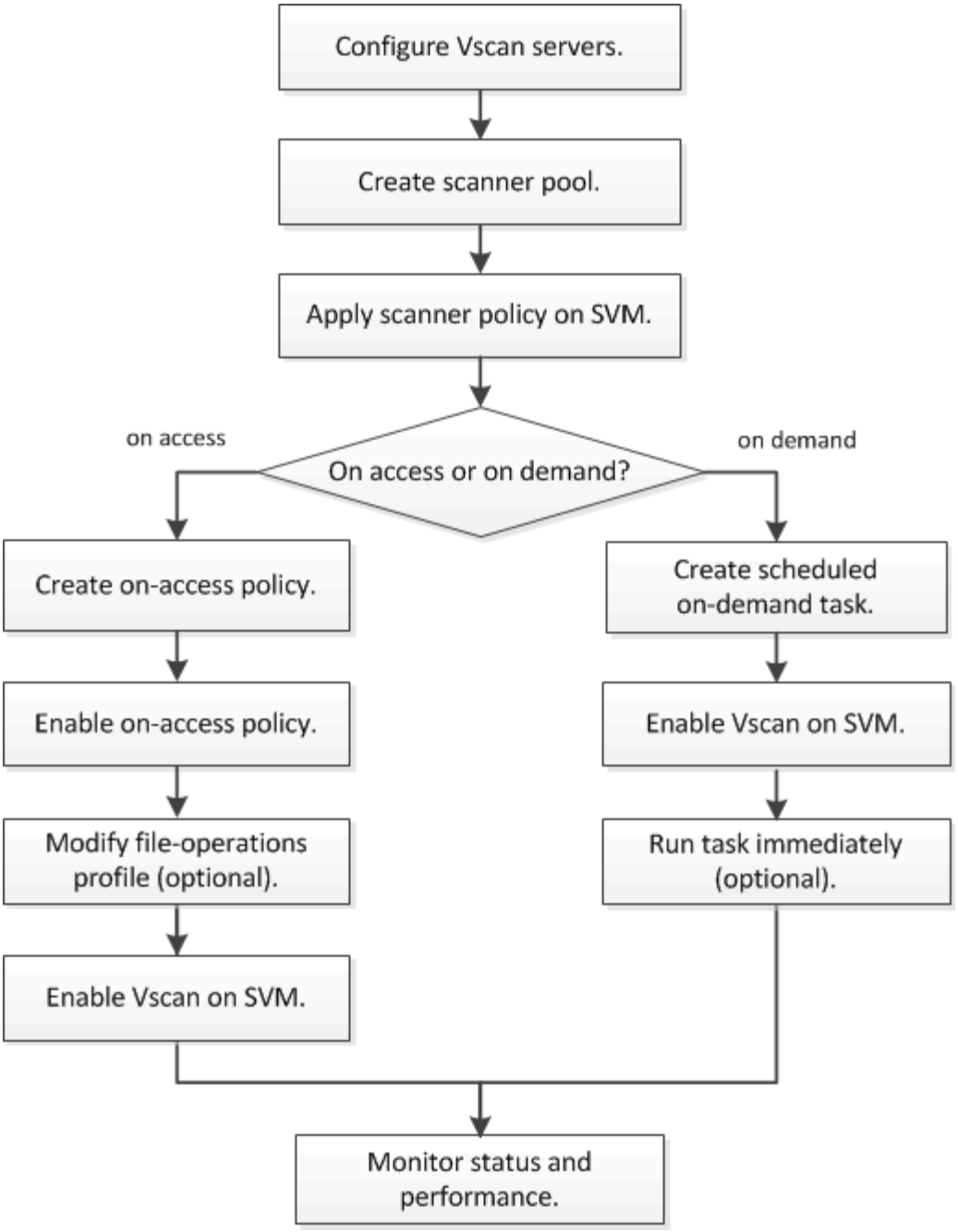
Der von NetApp bereitgestellte und auf dem externen Server installierte ONTAP Antivirus Connector übernimmt die Kommunikation zwischen dem Storage-System und der Antivirensoftware.




# Virenscan-Workflow mit ONTAP Vscan

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.




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.

**Nächste Schritte**

- Erstellen Sie einen Scanner-Pool auf einem einzelnen Cluster
- Wenden Sie eine Scannerrichtlinie auf einem einzelnen Cluster an
- Erstellen einer Zugriffsrichtlinie

# Antivirus-Architektur mit ONTAP Vscan

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 Scanner-Pool 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 Scanner-Pool 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` Beschränkt das Scannen auf Dateien, die mit Ausführungszugriff 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 `scan-mandatory` Option auf aus setzen, um anzugeben, 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 Virenscanner 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 den `vserver vscan on-demand-task run` Befehl verwenden, um die Aufgabe sofort auszuführen. Erfahren Sie mehr über `vserver vscan on-demand-task run` in der "ONTAP-Befehlsreferenz".

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

Der `vscan-fileop-profile` Parameter für den `vserver cifs share create` Befehl definiert, welche SMB-Dateioperationen einen Virus-Scan auslösen. Standardmäßig wird der Parameter auf `standard`, gesetzt, was NetApp Best Practice ist. Sie können diesen Parameter bei Bedarf anpassen, wenn Sie eine SMB-Freigabe erstellen oder ändern:

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

  Das `strict` Profil bietet erhöhte Sicherheit für Situationen, in denen mehrere Clients gleichzeitig auf eine Datei zugreifen. Wenn ein Client eine Datei nach dem Schreiben eines Virus schließt und dieselbe Datei 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, um das `strict` Profil auf Freigaben zu beschränken, die Dateien enthalten, von denen Sie erwarten, dass gleichzeitig auf sie zugegriffen wird. Da dieses Profil mehr Scananforderungen generiert, kann dies die Performance beeinträchtigen.

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

  Da `writes-only` weniger Scananforderungen generiert werden, wird in der Regel 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 schließt, nachdem er einen Virus darauf geschrieben `without` hat, und die Datei nicht repariert, gelöscht oder gesperrt wird, wird jeder Client, der auf die Datei zugreift, auf die er schreibt, infiziert.

Wenn eine Client-Anwendung einen Umbenennung durchführt, wird die Datei mit dem neuen Namen geschlossen und nicht gescannt. Wenn solche Vorgänge in Ihrer Umgebung ein Sicherheitsbedenken darstellen, sollten Sie das `standard` oder- `strict`Profil verwenden.

Erfahren Sie mehr über `vserver cifs share create` in der "ONTAP-Befehlsreferenz".

# Erfahren Sie mehr über die Partnerlösungen von ONTAP Vscan

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

Wie in der folgenden Tabelle zu sehen ist, werden die Details zur Interoperabilität von Trellix, Symantec und Trend Micro in der Interoperabilitätsmatrix von NetApp beibehalten. Interoperabilitätsdetails für Trellix, Symantec, Deep Instinct und OPSWAT finden Sie auch auf den Partner-Websites. Interoperabilitätsdetails für Sentinel One, Deep Instinct, OPSWAT und andere neue Partner werden vom Partner auf ihren Websites gepflegt.

| Partner | Lösungsdokumentation | Details zur Interoperabilität |
|---|---|---|
| Trellix (ehemals McAfee) | "Trellix Produktdokumentation" | • "NetApp Interoperabilitäts-Matrix-Tool"<br>• "Unterstützte Plattformen für Endpoint Security Storage Protection (trellix.com)" |

| Partner | Lösungsdokumentation | Details zur Interoperabilität |
| --- | --- | --- |
| Symantec | "Symantec Protection Engine 9.0.0" | • "NetApp Interoperabilitäts-Matrix-Tool"<br>• "Support Matrix für Partnergeräte, die mit Symantec Protection Engine (SPE) für Network Attached Storage (NAS) zertifiziert sind 9.x.x" |
| Trend Micro | "Trend Micro ServerProtect for Storage 6.0 – Leitfaden für die ersten Schritte" | "NetApp Interoperabilitäts-Matrix-Tool" |
| Sentinel One | • "SentinelOne Singularity Cloud Data Security"<br>• "SentinelOne-Unterstützung"<br>Dieser Link erfordert eine Benutzeranmeldung. Sie können den Zugriff von Sentinel One anfordern. | K. A. |
| Tiefes Instinkt | Deep Instinct DSX für NAS<br>• "Dokumentation und Interop"<br>Für diesen Link ist eine Benutzeranmeldung erforderlich. Sie können den Zugriff über Deep Instinct anfordern.<br>• "Datenblatt" | K. A. |
| OPSWAT | OPSWAT MetaDefender Storage Security<br>• "MetaDefender Speichersicherheitsintegration mit NetApp"<br>• "OPSWAT Partnerseite"<br>• "Integrationslösung Im Überblick" | K. A. |