About NetApp antivirus protection

ONTAP 9

NetApp
August 02, 2023

Table of Contents

About NetApp antivirus protection

About NetApp virus scanning

Vscan is an antivirus scanning solution developed by NetApp that allows customers to protect their data from being compromised by viruses or other malicious code. It combines partner-provided antivirus software with ONTAP features to give customers the flexibility they need to manage file scanning.

How virus scanning works

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors.

Based on the active scanning mode, ONTAP sends scan requests when clients access files over SMB (on-access) or access files in specific locations, on a schedule or immediately (on-demand).

- You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files over SMB. File operations are suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a scan from the server.

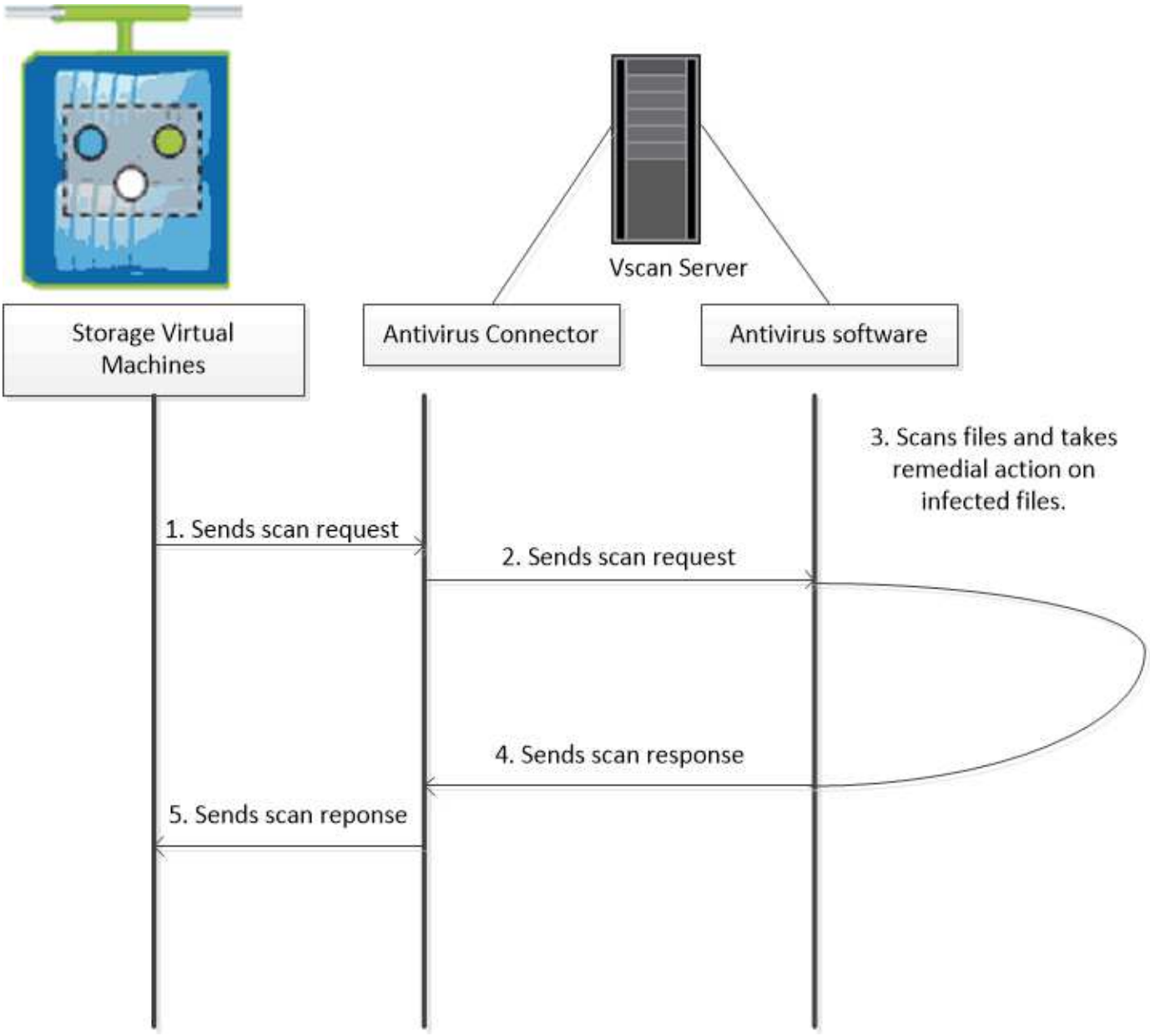
  On-access scanning is not supported for NFS.

- You can use *on-demand scanning* to check files for viruses immediately or on a schedule. We recommend that on-demand scans run only in off-peak hours to avoid overloading existing AV infrastructure, which is normally sized for on-access scanning. The external server updates the scan status of checked files, so that file-access latency is reduced over SMB. If there were file modifications or software version updates, it requests a new file scan from the external server.

  You can use on-demand scanning for any path in the SVM namespace, even for volumes that are exported only through NFS.

You typically enable both on-access and on-demand scanning modes on an SVM. In either mode, the antivirus software takes remedial action on infected files based on your software settings.

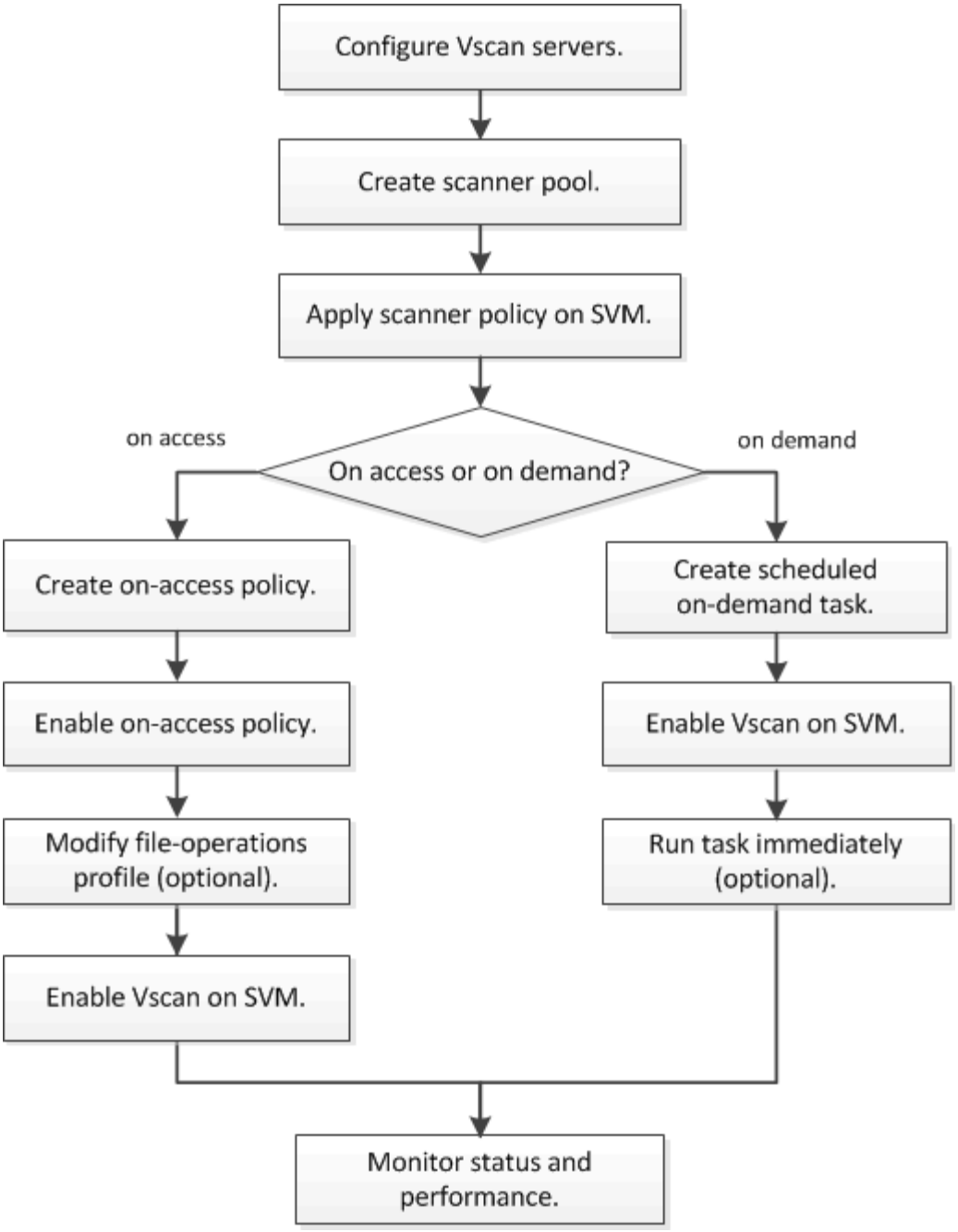
The ONTAP Antivirus Connector, provided by NetApp and installed on the external server, handles communication between the storage system and the antivirus software.



Virus scanning workflow

You must create a scanner pool and apply a scanner policy before you can enable scanning. You typically enable both on-access and on-demand scanning modes on an SVM.

You must have completed the CIFS configuration.



To create an on-demand task, there must be at least one on-access policy enabled. It can be the default policy or a user created on-access policy.

Antivirus architecture

The NetApp antivirus architecture consists of Vscan server software and associated settings.

Vscan server software

You must install this software on the Vscan server.

- **ONTAP Antivirus Connector**

This is NetApp-provided software that handles scan request and response communication between the SVMs and antivirus software. It can run on a virtual machine, but for best performance use a physical machine. You can download this software from the NetApp Support Site (requires login).

- **Antivirus software**

  This is partner-provided software that scans files for viruses or other malicious code. You specify the remedial actions to be taken on infected files when you configure the software.

Vscan software settings

You must configure these software settings on the Vscan server.

- **Scanner pool**

  This setting defines the Vscan servers and privileged users that can connect to SVMs. It also defines a scan request timeout period, after which the scan request is sent to an alternative Vscan server if one is available.

  > You should set the timeout period in the antivirus software on the Vscan server to five seconds less than the scanner-pool scan-request timeout period. This will avoid situations in which file access is delayed or denied altogether because the timeout period on the software is greater than the timeout period for the scan request.

- **Privileged user**

  This setting is a domain user account that a Vscan server uses to connect to the SVM. The account must exist in the list of privileged users in the scanner pool.

- **Scanner policy**

  This setting determines whether a scanner pool is active. Scanner policies are system-defined, so you cannot create custom scanner policies. Only these three policies are available:

  - `Primary` specifies that the scanner pool is active.
  - `Secondary` specifies that the scanner pool is active, only when none of the Vscan servers in the primary scanner pool are connected.
  - `Idle` specifies that the scanner pool is inactive.

- **On-access policy**

  This setting defines the scope of an on-access scan. You can specify the maximum file size to scan, file extensions and paths to include in the scan, and file extensions and paths to exclude from the scan.

  By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access:

  - `scan-ro-volume` enables scanning of read-only volumes.
  - `scan-execute-access` restricts scanning to files opened with execute access.

    > “Execute access” is different from “execute permission.” A given client will have “execute access” on an executable file only if the file was opened with “execute intent.”

You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan servers are available for virus scanning. Within on-access mode you can choose from these two mutually-exclusive options:

- Mandatory: With this option, Vscan tries to deliver the scan request to the server until the timeout period expires. If the scan request is not accepted by the server, then the client access request is denied.
- Non-Mandatory: With this option, Vscan always allows client access, whether or not a Vscan server was available for virus scanning.

- **On-demand task**

  This setting defines the scope of an on-demand scan. You can specify the maximum file size to scan, file extensions and paths to include in the scan, and file extensions and paths to exclude from the scan. Files in subdirectories are scanned by default.

  You use a cron schedule to specify when the task runs. You can use the `vserver vscan on-demand-task run` command to run the task immediately.

- **Vscan file-operations profile (on-access scanning only)**

  The `vscan-fileop-profile` parameter for the `vserver cifs share create` command defines which SMB file operations trigger virus scanning. By default, the parameter is set to `standard`, which is NetApp best practice. You can adjust this parameter as necessary when you create or modify an SMB share:

  - `no-scan` specifies that virus scans are never triggered for the share.
  - `standard` specifies that virus scans are triggered by open, close, and rename operations.
  - `strict` specifies that virus scans are triggered by open, read, close, and rename operations.

    The `strict` profile provides enhanced security for situations in which multiple clients access a file simultaneously. If one client closes a file after writing a virus to it, and the same file remains open on a second client, `strict` ensures that a read operation on the second client triggers a scan before the file is closed.

    You should be careful to restrict the `strict` profile to shares containing files that you anticipate will be accessed simultaneously. Since this profile generates more scan requests, it may impact performance.

  - `writes-only` specifies that virus scans are triggered only when modified files are closed.

    Since `writes-only` generates fewer scan requests, it typically improves performance.

    If you use this profile, the scanner must be configured to delete or quarantine unrepairable infected files, so they cannot be accessed. If, for example, a client closes a file after writing a virus to it, and the file is not repaired, deleted, or quarantined, any client that accesses the file `without` writing to it will be infected.

> If a client application performs a rename operation, the file is closed with the new name and is not scanned. If such operations pose a security concern in your environment, you should use the `standard` or `strict` profile.

Vscan partner solutions

NetApp collaborates with Trellix, Symantec, Trend Micro, and Sentinel One to deliver industry-leading anti-malware and anti-virus solutions that build upon ONTAP Vscan technology. These solutions help you scan files for malware and remediate any affected files.

As shown in the table below, interoperability details for Trellix, Symantec and Trend Micro are maintained on the NetApp Interoperability Matrix. Interoperability details for Trellix and Symantec can also be found on the partner websites. Interoperability details for Sentinel One and other new partners will be maintained by the partner on their websites.

Partner	Solution documentation	Interoperability details
Trellix (Formerly McAfee)	Trellix Product Documentation	• NetApp Interoperability Matrix Tool • Supported platforms for Endpoint Security Storage Protection (trellix.com)
Symantec	Symantec Protection Engine 9.0.0	• NetApp Interoperability Matrix Tool • Support Matrix for Partner Devices Certified with Symantec Protection Engine (SPE) for Network Attached Storage (NAS) 8.x (broadcom.com)
Trend Micro	Trend Micro ServerProtect for Storage 6.0 Getting Started Guide	NetApp Interoperability Matrix Tool
Sentinel One	Sentinel One support This link requires a user log-in. You can request access from Sentinel One.	

Copyright information

Trademark information