About NetApp antivirus protection

ONTAP 9

NetApp
March 21, 2022

Table of Contents

About NetApp antivirus protection

About NetApp virus scanning

You can use integrated antivirus functionality on NetApp storage systems to protect data from being compromised by viruses or other malicious code. NetApp virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

How virus scanning works

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors. The ONTAP Antivirus Connector, provided by NetApp and installed on the external server, handles communication between the storage system and the antivirus software.

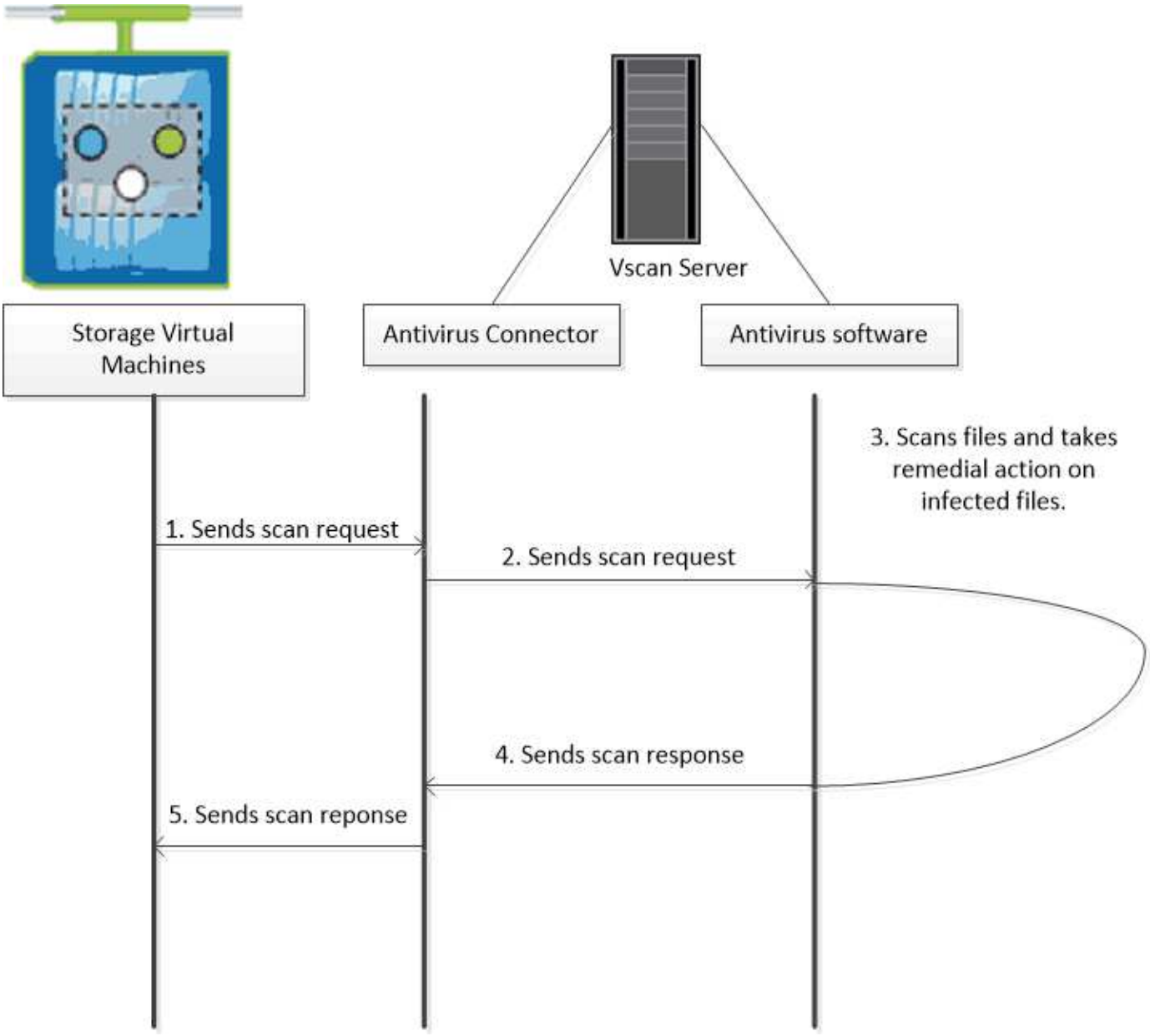
- You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files over SMB. File operation is suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a 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. You might want to run scans only in off-peak hours, for example. The external server updates the scan status of the checked files, so that file-access latency for those files (assuming they have not been modified) is typically reduced when they are next accessed over SMB.

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

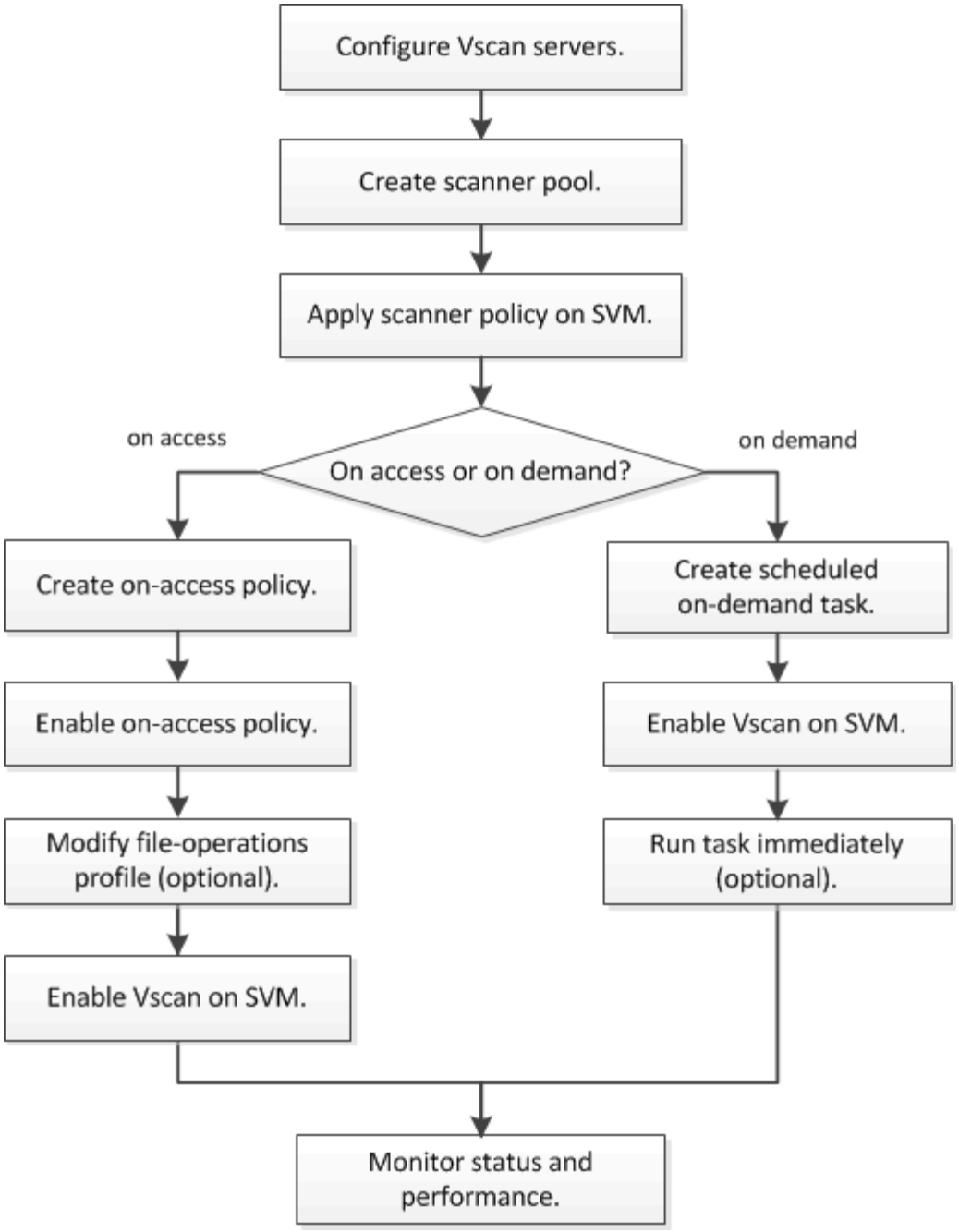
You typically enable both scanning modes on an SVM. In either mode, the antivirus software takes remedial action on infected files based on your settings in the software.



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 on an SVM.

You must have completed the CIFS configuration.



Antivirus architecture

The NetApp antivirus architecture consists of a Vscan server and a set of ONTAP configurables.

Vscan server components

You must install the following components on the Vscan server.

- **ONTAP Antivirus Connector**

  The ONTAP Antivirus Connector provided by NetApp handles communication between ONTAP and the Vscan server.

- **Antivirus software**

  ONTAP-compliant third-party antivirus software scans files for viruses or other malicious code. You specify the remedial actions to be taken on infected files when you configure the software.

ONTAP configurables

You must configure the following items on the NetApp storage system.

- **Scanner pool**

  A scanner pool 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.

  > It is a best practice to set the timeout period in the antivirus software on the Vscan server to five seconds less than the scanner-pool request timeout period, to 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**

  A privileged user is a domain user account that a Vscan server uses to connect to the SVM. The account must be included in the list of privileged users defined in the scanner pool.

- **Scanner policy**

  A scanner policy determines whether a scanner pool is active. A scanner policy can have one of the following values:

  - `Primary` specifies that the scanner pool is active.
  - `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool is connected.
  - `Idle` specifies that the scanner pool is inactive. Scanner policies are system-defined. You cannot create a custom scanner policy.

- **On-access policy**

  An on-access policy defines the scope of an on-access scan. You can specify the maximum size of the files to be scanned, the extensions of the files to be included in the scan, and the extensions and paths of the files to be excluded 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 not identical with “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.

- **On-demand task**

  An on-demand task defines the scope of an on-demand scan. You can specify the maximum size of the files to be scanned, the extensions and paths of the files to be included in the scan, and the extensions and paths of the files to be excluded 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 operations on a SMB share can trigger virus scanning. By default, the parameter is set to `standard`, which is the NetApp best practice.

  You can adjust this parameter as necessary when you create or modify a SMB share:

  - `no-scan` specifies that virus scans are never triggered for the share.
  - `standard` specifies that virus scans can be triggered by open, close, and rename operations.
  - `strict` specifies that virus scans can be 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. Because the profile generates more scan requests than the others, it may affect performance adversely.

  - `writes-only` specifies that virus scans can be triggered only when a file that has been modified is closed.

    > 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.

    Because `writes-only` generates fewer scan requests than the other profiles (except `no-scan`), it typically improves performance.

    Keep in mind, though, that if you use this profile for a share, the scanner must be configured to delete or quarantine an unrepairable infected file, so that it cannot be accessed by clients later. 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.