Configure on-access scanning

ONTAP 9

NetApp
July 17, 2023

Table of Contents

Configure on-access scanning

Create an on-access policy

An on-access policy defines the scope of an on-access scan. You can create an on-access policy for an individual SVM or for all the SVMs in a cluster. If you created an on-access policy for all the SVMs in a cluster, you must enable the policy on each SVM individually.

About this task

- 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.
- 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.
- By default, ONTAP creates an on-access policy named "default_CIFS" and enables it for all the SVMs in a cluster.
- Any file that qualifies for scan exclusion based on the `paths-to-exclude`, `file-ext-to-exclude`, or `max-file-size` parameters is not considered for scanning, even if the `scan-mandatory` option is set to on. (Check this troubleshooting section for connectivity issues related to the `scan-mandatory` option.)
- 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.
- Virus scanning is not performed on an SMB share for which the continuously-available parameter is set to Yes.
- See the Antivirus architecture section for details about the *Vscan file-operations profile*.
- You can create a maximum of ten (10) on-access policies per SVM. However, you can enable only one on-access policy at a time.
  - You can exclude a maximum of one hundred (100) paths and file extensions from virus scanning in an on-access policy.
- Some file exclusion recommendations:
  - Consider excluding large files (file size can be specified) from virus scanning because they can result in a slow response or scan request timeouts for CIFS users. The default file size for exclusion is 2GB.
  - Consider excluding file extensions such as `.vhd` and `.tmp` because files with these extensions might not be appropriate for scanning.
  - Consider excluding file paths such as the quarantine directory or paths in which only virtual hard drives or databases are stored.
  - Verify that all exclusions are specified in the same policy, because only one policy can be enabled at a time. NetApp highly recommends having the same set of exclusions specified in the antivirus engine.

Steps

1. Create an on-access policy:

```
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

- Specify a data SVM for a policy defined for an individual SVM, a cluster admin SVM for a policy defined for all the SVMs in a cluster.
- The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.
- Set `-scan-files-with-no-ext` to true to scan files without extensions. The following command creates an on-access policy named `Policy1` on the `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. Verify that the on-access policy has been created: `vserver vscan on-access-policy show -instance` *data_SVM*|*cluster_admin_SVM* `-policy-name policy_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `Policy1` policy:

```
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
```

Enable an on-access policy

An on-access policy defines the scope of an on-access scan. You must enable an on-access policy on an SVM before its files can be scanned.

If you created an on-access policy for all the SVMs in a cluster, you must enable the policy on each SVM individually. You can enable only one on-access policy on an SVM at a time.

Steps

1. Enable an on-access policy:

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   The following command enables an on-access policy named `Policy1` on the `vs1` SVM:

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. Verify that the on-access policy is enabled:

   `vserver vscan on-access-policy show -instance *data_SVM* -policy-name *policy_name*`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `Policy1` on-access policy:

   ```
   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
   ```

Modify the Vscan file-operations profile for an SMB share

The *Vscan file-operations profile* for an SMB share defines the operations on the share that can trigger scanning. By default, the parameter is set to `standard`. You can adjust the parameter as necessary when you create or modify an SMB share.

See the Antivirus architecture section for details about the *Vscan file-operations profile*.

Virus scanning is not performed on an SMB share that has the `continuously-available` parameter set to `Yes`.

Step

1. Modify the value of the Vscan file-operations profile for an SMB share:

   `vserver cifs share modify -vserver` *`data_SVM`* `-share-name` *`share`* `-path` *`share_path`* `-vscan-fileop-profile no-scan|standard|strict|writes-only`

   For a complete list of options, see the man page for the command.

   The following command changes the Vscan file operations profile for an SMB share to `strict`:

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

Commands for managing on-access policies

You can modify, disable, or delete an on-access policy. You can view a summary and details for the policy.

If you want to…	Enter the following command…
Create an on-access policy	`vserver vscan on-access-policy create`
Modify an on-access policy	`vserver vscan on-access-policy modify`
Enable an on-access policy	`vserver vscan on-access-policy enable`
Disable an on-access policy	`vserver vscan on-access-policy disable`
Delete an on-access policy	`vserver vscan on-access-policy delete`
View summary and details for an on-access policy	`vserver vscan on-access-policy show`
Add to the list of paths to exclude	`vserver vscan on-access-policy paths-to-exclude add`
Delete from the list of paths to exclude	`vserver vscan on-access-policy paths-to-exclude remove`
View the list of paths to exclude	`vserver vscan on-access-policy paths-to-exclude show`

Add to the list of file extensions to exclude	`vserver vscan on-access-policy file-ext-to-exclude add`
Delete from the list of file extensions to exclude	`vserver vscan on-access-policy file-ext-to-exclude remove`
View the list of file extensions to exclude	`vserver vscan on-access-policy file-ext-to-exclude show`
Add to the list of file extensions to include	`vserver vscan on-access-policy file-ext-to-include add`
Delete from the list of file extensions to include	`vserver vscan on-access-policy file-ext-to-include remove`
View the list of file extensions to include	`vserver vscan on-access-policy file-ext-to-include show`

For more information about these commands, see the man pages.

Copyright information

Trademark information