



Configure on-access scanning

ONTAP 9

NetApp
July 17, 2023

Table of Contents

- Configure on-access scanning 1
 - Create an on-access policy 1
 - Enable an on-access policy 2
 - Modify the Vscan file-operations profile for an SMB share 3
 - Commands for managing on-access policies 4

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	<code>vserver vscan on-access-policy create</code>
Modify an on-access policy	<code>vserver vscan on-access-policy modify</code>
Enable an on-access policy	<code>vserver vscan on-access-policy enable</code>
Disable an on-access policy	<code>vserver vscan on-access-policy disable</code>
Delete an on-access policy	<code>vserver vscan on-access-policy delete</code>
View summary and details for an on-access policy	<code>vserver vscan on-access-policy show</code>
Add to the list of paths to exclude	<code>vserver vscan on-access-policy paths-to-exclude add</code>
Delete from the list of paths to exclude	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
View the list of paths to exclude	<code>vserver vscan on-access-policy paths-to-exclude show</code>

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

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

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.