vserver vscan commands

Command reference

NetApp
February 02, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-disable.html on February 02, 2026. Always check docs.netapp.com for the latest.

Table of Contents

vserver vscan commands . . . 1
- vserver vscan disable . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 1
- vserver vscan enable . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 1
- vserver vscan reset . . . 2
  - Description . . . 2
  - Parameters . . . 2
  - Examples . . . 2
- vserver vscan show-events . . . 2
  - Description . . . 2
  - Parameters . . . 3
  - Examples . . . 4
- vserver vscan show . . . 5
  - Description . . . 5
  - Parameters . . . 5
  - Examples . . . 5
- vserver vscan connection-status show-all . . . 6
  - Description . . . 6
  - Parameters . . . 6
  - Examples . . . 8
- vserver vscan connection-status show-connected . . . 8
  - Description . . . 8
  - Parameters . . . 9
  - Examples . . . 10
- vserver vscan connection-status show-not-connected . . . 10
  - Description . . . 11
  - Parameters . . . 11
  - Examples . . . 12
- vserver vscan connection-status show . . . 12
  - Description . . . 13
  - Parameters . . . 13
  - Examples . . . 13
- vserver vscan on-access-policy create . . . 14
  - Description . . . 14
  - Parameters . . . 14
  - Examples . . . 16
- vserver vscan on-access-policy delete . . . 16
  - Description . . . 16

Parameters . . . 17
Examples . . . 17
vserver vscan on-access-policy disable . . . 17
Description . . . 17
Parameters . . . 17
Examples . . . 17
vserver vscan on-access-policy enable . . . 18
Description . . . 18
Parameters . . . 18
Examples . . . 18
vserver vscan on-access-policy modify . . . 19
Description . . . 19
Parameters . . . 19
Examples . . . 21
vserver vscan on-access-policy show . . . 21
Description . . . 21
Parameters . . . 22
Examples . . . 23
vserver vscan on-access-policy file-ext-to-exclude add . . . 24
Description . . . 24
Parameters . . . 24
Examples . . . 24
vserver vscan on-access-policy file-ext-to-exclude remove . . . 25
Description . . . 25
Parameters . . . 25
Examples . . . 25
vserver vscan on-access-policy file-ext-to-exclude show . . . 26
Description . . . 26
Parameters . . . 26
Examples . . . 27
vserver vscan on-access-policy file-ext-to-include add . . . 27
Description . . . 27
Parameters . . . 27
Examples . . . 27
vserver vscan on-access-policy file-ext-to-include remove . . . 28
Description . . . 28
Parameters . . . 28
Examples . . . 28
vserver vscan on-access-policy file-ext-to-include show . . . 29
Description . . . 29
Parameters . . . 29
Examples . . . 30
vserver vscan on-access-policy paths-to-exclude add . . . 30
Description . . . 30
Parameters . . . 30

Examples . . . 30
vserver vscan on-access-policy paths-to-exclude remove . . . 31
Description . . . 31
Parameters . . . 31
Examples . . . 31
vserver vscan on-access-policy paths-to-exclude show . . . 32
Description . . . 32
Parameters . . . 32
Examples . . . 33
vserver vscan on-demand-task create . . . 33
Description . . . 33
Parameters . . . 33
Examples . . . 35
vserver vscan on-demand-task delete . . . 36
Description . . . 36
Parameters . . . 36
Examples . . . 37
vserver vscan on-demand-task modify . . . 37
Description . . . 37
Parameters . . . 37
Examples . . . 39
vserver vscan on-demand-task run . . . 40
Description . . . 40
Parameters . . . 40
Examples . . . 41
vserver vscan on-demand-task schedule . . . 41
Description . . . 41
Parameters . . . 41
Examples . . . 41
vserver vscan on-demand-task show . . . 42
Description . . . 42
Parameters . . . 43
Examples . . . 44
vserver vscan on-demand-task unschedule . . . 45
Description . . . 45
Parameters . . . 45
Examples . . . 46
vserver vscan on-demand-task report delete . . . 46
Description . . . 46
Parameters . . . 46
Examples . . . 47
vserver vscan on-demand-task report show . . . 47
Description . . . 47
Parameters . . . 48
Examples . . . 50

vserver vscan scanner-pool apply-policy . . . 50
Description . . . 51
Parameters . . . 51
Examples . . . 51
vserver vscan scanner-pool create . . . 52
Description . . . 52
Parameters . . . 52
Examples . . . 53
Related Links . . . 53
vserver vscan scanner-pool delete . . . 53
Description . . . 54
Parameters . . . 54
Examples . . . 54
vserver vscan scanner-pool modify . . . 54
Description . . . 54
Parameters . . . 54
Examples . . . 55
vserver vscan scanner-pool resolve-hostnames . . . 56
Description . . . 56
Parameters . . . 56
Examples . . . 56
vserver vscan scanner-pool show-active . . . 57
Description . . . 57
Parameters . . . 57
Examples . . . 58
vserver vscan scanner-pool show . . . 59
Description . . . 59
Parameters . . . 60
Examples . . . 61
vserver vscan scanner-pool privileged-users add . . . 62
Description . . . 62
Parameters . . . 62
Examples . . . 62
vserver vscan scanner-pool privileged-users remove . . . 63
Description . . . 63
Parameters . . . 63
Examples . . . 63
vserver vscan scanner-pool privileged-users show . . . 64
Description . . . 64
Parameters . . . 64
Examples . . . 65
vserver vscan scanner-pool servers add . . . 65
Description . . . 65
Parameters . . . 65
Examples . . . 65

vserver vscan scanner-pool servers remove . . . 66
Description . . . 66
Parameters . . . 66
Examples . . . 66
vserver vscan scanner-pool servers show . . . 67
Description . . . 67
Parameters . . . 67
Examples . . . 68

vserver vscan commands

vserver vscan disable

Disable Vscan on a Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan disable` command disables Vscan on a Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to disable Vscan.

Examples

The following example disables Vscan on Vserver vs1.

```
cluster1::> vserver vscan disable -vserver vs1

cluster1::> vserver vscan show -vserver vs1
Vserver: vs1
Vscan Status: off
```

vserver vscan enable

Enable Vscan on a Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan enable` command enables Vscan on a Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to enable Vscan. The Vscan configuration must already exist.

Examples

The following example enables Vscan on Vserver vs1.

```
cluster1::> vserver vscan enable -vserver vs1

cluster1::> vserver vscan show -vserver vs1
Vserver: vs1
Vscan Status: on
```

vserver vscan reset

Discard cached scan information

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan reset` command discards the cached information of the files that have been successfully scanned. After running this command, the files are scanned again when they are accessed.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver for which you want to discard the cached information.

Examples

The following example discards the cached information of the successfully scanned files.

```
cluster1::> vserver vscan reset -vserver vs1
Warning: Running this command can cause performance degradation because
files are scanned again when they are accessed.
Do you want to continue? {y|n}: y

cluster1::>
```

vserver vscan show-events

Display Vscan events

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

The `vserver vscan show-events` command displays contents of the event log, which is generated by the cluster to capture important events. If you do not specify any parameters, the command displays the following information for all Vscan servers:

- Vserver name

- Node name
- Vscan server
- Event type
- Event time

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields:

- File path
- Vscan server vendor
- Vscan server version
- Disconnect reason
- Scan engine status code
- Vserver LIF used for connection
- Consecutive occurrence count

Parameters

[-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] (privilege: advanced) }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have occurred on the specified node.

[-vserver <vserver name>] - Vserver (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have occurred for the specified Vserver.

[-event-time <MM/DD/YYYY HH:MM:SS>] - Event Log Time (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have occurred at the specified time.

[-server <IP Address>] - Server (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have occurred for the specified server.

[-event-type <event-type>] - Event Type (privilege: advanced)

If you specify this parameter, the command displays information only about the events that are of the specified event type.

[-file-path <text>] - File Path (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the

specified file path.

[-vendor <text>] - Vscanner Vendor (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the specified scan-engine vendor.

[-version <text>] - Vscanner Version (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the specified scan-engine version.

[-disconnect-reason <reason>] - Server Disconnect Reason (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the specified reason of the server disconnection.

[-lif <IP Address>] - Vserver LIF Used for Connection (privilege: advanced)

If you specify this parameter, the command displays information only about the events that have the specified IP address, which is used for connecting ONTAP with the Vscan server.

Examples

The following example displays all the events captured in the cluster:

```
cluster1::*> vserver vscan show-events

Vserver     Node            Server          Event Type        Event Time
----------- --------------- --------------- -----------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

The following example displays detailed event information about all the infected files:

```
cluster1::*> vserver vscan show-events -event-type file-infected -instance
Node: Cluster-01
                         Vserver: vs1
                 Event Log Time: 9/5/2014 11:37:38
                          Server: 192.168.1.1
                      Event Type: file-infected
                       File Path: \\1
                Vscanner Vendor: mighty master anti-evil scanner
               Vscanner Version: 1.0
       Server Disconnect Reason: -
Vserver LIF Used for Connection: 192.168.41.231
```

vserver vscan show

Display Vscan status

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan show ` command displays Vscan status information of the Vservers. If you do not specify any parameters, the command displays the following information about all Vservers:

- Vserver name
- Vscan status

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the specified Vserver.

[-vscan-status {on|off}] - Vscan Status

If you specify this parameter, the command displays information only about the Vservers that have the specified status.

Examples

The following example displays the Vscan status information.

```
cluster1::> vserver vscan show
Vserver          Vscan Status
--------------   ------------
vs1              on
vs2              off
2 entries were displayed.
```

vserver vscan connection-status show-all

Display Vscan servers connection status

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan connection-status show-all` command displays connection status information of the external virus-scanning servers, or "Vscan servers". If you do not specify any parameters, the command displays the following information for all Vscan servers:

- Vserver name
- Node name
- Vscan server
- Connection status
- Disconnect reason

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields:

- Server type
- Vscan server vendor
- Vscan server version
- Privileged user
- Vscan server connected since
- Vscan server disconnected since
- Vserver LIF used for connection

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

If you specify this parameter, the command displays information only about the Vscan servers attached to the specified node.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the Vscan servers for the specified Vserver.

[-server <IP Address>] - Server

If you specify this parameter, the command displays information only about the Vscan server that you specify.

[-server-status <Status>] - Server Status

If you specify this parameter, the command displays information only about the Vscan servers that have the specified status.

[-server-type <Server type>] - Server Type

If you specify this parameter, the command displays information only about the Vscan servers that have the specified server type.

[-vendor <text>] - Vscanner Vendor

If you specify this parameter, the command displays information only about the Vscan servers that are running scan-engine of the specified vendor.

[-version <text>] - Vscanner Version

If you specify this parameter, the command displays information only about the Vscan servers that are running scan-engine of the specified version.

[-disconnect-reason <reason>] - Server Disconnect Reason

If you specify this parameter, the command displays information only about the Vscan servers that are disconnected because of the specified reason.

[-disconnected-since <MM/DD/YYYY HH:MM:SS>] - Time When Vscanner Was Disconnected

If you specify this parameter, the command displays information only about the Vscan servers that have been disconnected since the specified time.

[-privileged-user <text>] - Privileged User Used for Connection

If you specify this parameter, the command displays information only about the Vscan servers that are connected to ONTAP using the specified privileged user.

[-connected-since <MM/DD/YYYY HH:MM:SS>] - Time When Vscanner Was Connected

If you specify this parameter, the command displays information only about the Vscan servers that have been connected since the specified time.

[-lif <IP Address>] - Vserver LIF Used for Connection

If you specify this parameter, the command displays information only about the Vscan servers that have used the specified IP address for connecting to ONTAP.

Examples

The following example displays connection-status information about all Vscan servers.

```
cluster1::> vserver vscan connection-status show-all
                                              Connection
Vserver     Node              Server          Status         Disconnect
Reason
----------- ----------------- --------------- --------------
-----------------
vs1         Cluster-01        1.1.1.1         disconnected   remote-closed
vs1         Cluster-01        2.2.2.2         connected      -
vs2         Cluster-01        3.3.3.3         disconnected   no-data-lif
vs2         Cluster-01        4.4.4.4         disconnected   no-data-lif
4 entries were displayed.
```

The following example displays detailed connection-status information about all Vscan servers which are connected.

```
cluster1::> vserver vscan connection-status show-all -instance
            -server-status connected
Node: Cluster-01
                            Vserver: vs1
                             Server: 2.2.2.2
                      Server Status: connected
                        Server Type: primary
                   Vscanner Vendor: XYZ
                  Vscanner Version: 1.12.2
           Server Disconnect Reason: -
  Time When Server Was Disconnected: -
Privileged User Used for Connection: cifs\u2
     Time When Server Was Connected: 6/3/2013 08:44:21
    Vserver LIF Used for Connection: 10.238.41.223
```

vserver vscan connection-status show-connected

Display connection status of connected Vscan servers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan connection-status show-connected` command displays connection status information of the connected external virus-scanning servers, or "Vscan servers". If you do not specify any parameters, the command displays the following information for all Vscan servers:

- Vserver name
- Node name
- Vscan server
- Vscan server vendor
- Privileged user

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields:

- Server type
- Vscan server version
- Vscan server connected since
- Vserver LIF used for connection

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

If you specify this parameter, the command displays information only about the Vscan servers attached to the specified node.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the Vscan servers for the specified Vserver.

[-server <IP Address>] - Server

If you specify this parameter, the command displays information only about the Vscan server that you specify.

[-vendor <text>] - Vscan Server Vendor

If you specify this parameter, the command displays information only about the Vscan servers that are running scan-engine of the specified vendor.

[-version <text>] - Vscan Server Version

If you specify this parameter, the command displays information only about the Vscan servers that are running scan-engine of the specified version.

[-privileged-user <text>] - Privileged User Used for Connection

If you specify this parameter, the command displays information only about the Vscan servers that are connected to ONTAP using the specified privileged user.

[-connected-since <MM/DD/YYYY HH:MM:SS>] - Time When Vscan Server Was Connected

If you specify this parameter, the command displays information only about the Vscan servers that have been connected since the specified time.

[-server-type <Server type>] - Server Type

If you specify this parameter, the command displays information only about the Vscan servers that have the specified server type.

[-lif <IP Address>] - Vserver LIF Used for Connection

If you specify this parameter, the command displays information only about the Vscan servers that have used the specified IP address for connecting to ONTAP.

Examples

The following example displays connection-status information about all connected Vscan servers.

```
cluster1::> vserver vscan connection-status show-connected
                                                                  Privileged
Vserver       Node              Server           Vendor         User
------------- ----------------- ---------------- -------------
---------------
vs1           Cluster-01        1.1.1.1          ABC            cifs\u2
vs1           Cluster-01        2.2.2.2          XYZ            cifs\u2
2 entries were displayed.
```

The following example displays detailed connection-status information about connected Vscan servers which are running XYZ scan-engine.

```
cluster1::> vserver vscan connection-status show-connected -instance
-vendor XYZ
Node: Cluster-01
                            Vserver: vs1
                             Server: 2.2.2.2
                    Vscanner Vendor: XYZ
                   Vscanner Version: 1.12
Privileged User Used for Connection: cifs\u2
   Time When Vscanner Was Connected: 6/3/2013 08:44:21
                        Server Type: primary
    Vserver LIF Used for Connection: 10.238.41.223
```

vserver vscan connection-status show-not-connected

Display connection status of Vscan servers which are allowed to connect but not yet connected

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan connection-status show-not-connected` command displays connection status information of the external virus-scanning servers, or "Vscan servers" that are ready to accept connection but are not yet connected. This command could be useful for troubleshooting. If you do not specify any parameters, the command displays the following information for all Vscan servers:

- Vserver name
- Node name
- Vscan server
- Connection status
- Disconnect reason

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields:

- Server type
- Vscan server disconnected since

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

If you specify this parameter, the command displays information only about the Vscan servers attached to the specified node.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the Vscan servers for the specified Vserver.

[-server <IP Address>] - Server

If you specify this parameter, the command displays information only about the Vscan server that you specify.

[-server-status <Status>] - Server Status

If you specify this parameter, the command displays information only about the Vscan servers that have the specified status.

[-disconnect-reason <reason>] - Server Disconnect Reason

If you specify this parameter, the command displays information only about the Vscan servers that are disconnected because of the specified reason.

[-disconnected-since <MM/DD/YYYY HH:MM:SS>] - Time When Vscan Server Was Disconnected

If you specify this parameter, the command displays information only about the Vscan servers that have been disconnected since the specified time.

[-server-type <Server type>] - Server Type

If you specify this parameter, the command displays information only about the Vscan servers that have the specified server type.

Examples

The following example displays connection-status information about all Vscan servers which are ready to accept connection but not yet connected.

```
cluster1::> vserver vscan connection-status show-not-connected
                                                  Connection    Disconnect
Vserver       Node               Server           Status        Reason
------------- ------------------ ---------------- -------------
---------------
vs2           Cluster-01         3.3.3.3          disconnected  invalid-
                                                                session-id
vs2           Cluster-01         4.4.4.4          disconnected  remote-
closed
2 entries were displayed.
```

The following example displays detailed connection-status information about Vscan servers which are disconnected because the connection is remotely closed.

```
cluster1::> vserver vscan connection-status show-not-connected -instance
            -disconnect-reason remote-closed
Node: Cluster-01
                            Vserver: vs2
                             Server: 4.4.4.4
                      Server Status: disconnected
           Server Disconnect Reason: remote-closed
Time When Vscanner Was Disconnected: 6/4/2013 06:51:32
                        Server Type: primary
```

vserver vscan connection-status show

Display Vscan servers connection status summary

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan connection-status show` command displays connection status summary of the external virus-scanning servers, or "Vscan servers" for a Vserver. If you do not specify any parameters, the command displays the following information for all Vservers:

- Vserver name
- Node name
- List of connected Vscan servers
- Connected count

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

If you specify this parameter, the command displays information only about the Vscan servers attached to the specified node.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the Vscan servers for the specified Vserver.

[-servers <IP Address>,…] - List of Connected Vscan Servers

If you specify this parameter, the command displays information only about the Vservers that have the specified server or servers.

[-connection-count <integer>] - Number of Connected Vscan Servers Serving the Vserver

If you specify this parameter, the command displays information only about the Vservers that have the specified connection count.

Examples

The following example displays connection-status summary for all Vservers.

```
cluster1::> vserver vscan connection-status show
                                        Connected Connected
Vserver         Node                 Server-Count Servers
--------------- -------------------- ------------
-----------------------------
vs1             Cluster-01                      2 1.1.1.1, 2.2.2.2
vs2             Cluster-01                      0 -
2 entries were displayed.
```

vserver vscan on-access-policy create

Create an On-Access policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy create` command creates an On-Access policy.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create an On-Access policy.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the On-Access policy that you want to create. An On-Access policy name can be up to 256 characters long and is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "_", "-" and ".".

`-protocol <CIFS>` - File-Access Protocol

This parameter specifies the protocol name for which the On-Access policy will be created. Currently only CIFS is supported.

`[-filters {scan-ro-volume|scan-execute-access}]` - Filters

This parameter specifies a list of filters which can be used to define the scope of the On-Access policy more precisely. The list can include one or more of the following:

- *`scan-ro-volume`* - Enable scans for read-only volume.
- *`scan-execute-access`* - Scan only files opened with execute-access (CIFS only).

`[-scan-mandatory {on|off}]` - Mandatory Scan

This parameter specifies if access to a file is allowed or denied when there are no external virus-scanning servers available for virus scanning. The default value for this parameter is "on", this denies file access if an external virus-scanning server is not available. This parameter has no impact when an external virus-scanning server is available for file scanning because access to the file is allowed or denied based on the response from the virus-scanning server.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

This parameter specifies the maximum size of the file which will be considered for virus scanning. By default, it is *2GB* .

[-paths-to-exclude <File path>,…] - File Paths Not to Scan

This parameter specifies a list of paths, separated by commas, to exclude from virus scanning. This path is given from the root of the Vserver and can be up to 255 characters long. By default, no paths are excluded. CIFS protocol based On-Access policies must use "\" as the path separator. The path can be in one of the following forms:

- *\dir1\dir2\name* - This would match "\dir1\dir2\name" as well as "\dir1\dir2\name...".
- *\dir1\dir2\name* - This would only match "\dir1\dir2\name...".

If you are using the CLI, you must delimit all paths with double quotation marks ("). For instance, to add the paths "\vol\a b\" and "\vol\a,b\" to the `-paths-to-exclude` in the CLI, type *"\vol\a b\","\vol\a,b\"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

This parameter specifies a list of file extensions, separated by commas, to exclude from virus scanning. By default, no file extensions are excluded. Each file extension can be up to 16 characters long. The `-file-ext-to-exclude` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** would match mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* would match mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

This parameter specifies a list of file extensions, separated by commas, to include for virus scanning. By default it is *** , which means all the file extensions are considered for virus scanning except those which match one of the patterns provided in `-file-ext-to-exclude` list. Each file extension can be up to 16 characters long. The `-file-ext-to-include` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** would match mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* would match mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

If you specify both `-file-ext-to-include` and `-file-ext-to-exclude` lists, then only those file extensions are considered for virus scanning which match one of the patterns provided in `-file-ext-to-include` list but do not match any of the patterns provided in `-file-ext-to-exclude` list.

`[-scan-files-with-no-ext {true|false}]` - Scan Files with No Extension

This parameter specifies if the files without any extension are considered for virus scanning or not. By default, it is true.

Examples

The following example creates an On-Access policy.

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name test
                -protocol CIFS -scan-mandatory on -filters scan-ro-volume
-max-file-size 3GB
                -file-ext-to-exclude "mp3","txt" -file-ext-to-include
"mp*","tx*"
                -paths-to-exclude "\vol\a b\","\vol\a,b\"

cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name test
Vserver: vs1
                            Policy: test
                     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: true
```

vserver vscan on-access-policy delete

Delete an On-Access policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy delete` command deletes an On-Access policy.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver from which you want to delete an On-Access policy.

-policy-name <Policy name> - Policy

This parameter specifies the name of the On-Access policy that you want to delete.

Examples

The following example deletes an On-Access policy.

```
cluster1::> vserver vscan on-access-policy delete -vserver vs1 -policy
-name test

cluster1::> vserver vscan on-access-policy show -vserver vs1 -policy-name
test
There are no entries matching your query.
```

vserver vscan on-access-policy disable

Disable an On-Access policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy disable` command disable an On-Access policy for the specified Vserver.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to disable an On-Access policy. The Vserver administrator can disable On-Access policies created within the scope of the Vserver and can also disable an On-Access policy created by the cluster administrator. The cluster administrator can disable On-Access policies for any Vserver.

-policy-name <Policy name> - Policy

This parameter specifies the name of the On-Access policy you want to disable.

Examples

The following command disable an On-Access policy on specified Vserver.

```
cluster1::> vserver vscan on-access-policy disable -vserver vs1 -policy
-name new

cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name new
Vserver: vs1
                            Policy: new
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 4GB
             File-Paths Not to Scan: \vol\temp
       File-Extensions Not to Scan: txt
```

vserver vscan on-access-policy enable

Enable an On-Access policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy enable` command enables an On-Access policy for the specified Vserver. Only one On-Access policy of a specific protocol can be enabled at one time.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to enable an On-Access policy. The Vserver administrator can enable On-Access policy created within the scope of the Vserver or the cluster. The cluster administrator can enable On-Access policy for any Vserver but cannot enable them with a scope of cluster. The scope is determined at a Vserver level.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the On-Access policy you want to enable.

Examples

The following command enables an On-Access policy on specified Vserver.

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

cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name new
Vserver: vs1
                            Policy: new
                     Policy Status: on
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 4GB
            File-Paths Not to Scan: \vol\temp
       File-Extensions Not to Scan: txt
```

vserver vscan on-access-policy modify

Modify an On-Access policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy modify` command modifies an On-Access policy.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to modify an On-Access policy.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the On-Access policy that you want to modify.

`[-filters {scan-ro-volume|scan-execute-access}]` - Filters

This parameter specifies a list of filters which can be used to define the scope of the On-Access policy more precisely. The list can include one or more of the following:

- *`scan-ro-volume`* - Enable scans for read-only volume.
- *`scan-execute-access`* - Scan only files opened with execute-access (CIFS only).

`[-scan-mandatory {on|off}]` - Mandatory Scan

This parameter specifies whether access to a file is allowed if there are no external virus-scanning servers available for virus scanning.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

This parameter specifies the maximum size of the file which will be considered for virus scanning.

[-paths-to-exclude <File path>,…] - File Paths Not to Scan

This parameter specifies a list of paths, separated by commas, to exclude from virus scanning. This path is given from the root of the Vserver and can be up to 255 characters long. CIFS protocol based On-Access policies must use "\" as the path separator. The path can be in one of the following forms:

- *\dir1\dir2\name* - This would match "\dir1\dir2\name" as well as "\dir1\dir2\name...".
- *\dir1\dir2\name* - This would only match "\dir1\dir2\name...".

If you are using the CLI, you must delimit all paths with double quotation marks ("). For instance, to add the paths "\vol\a b\" and "\vol\a,b\" to the `-paths-to-exclude` in the CLI, type *"\vol\a b\","\vol\a,b\"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

This parameter specifies a list of file extensions, separated by commas, to exclude from virus scanning. Each file extension can be up to 16 characters long. The `-file-ext-to-exclude` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** would match mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* would match mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

This parameter specifies a list of file extensions, separated by commas, to include for virus scanning. Each file extension can be up to 16 characters long. The `-file-ext-to-include` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** would match mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* would match mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

If you specify both `-file-ext-to-include` and `-file-ext-to-exclude` lists, then only those file extensions are considered for virus scanning which match one of the patterns provided in `-file-ext-to-include` list but do not match any of the patterns provided in `-file-ext-to-exclude` list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

This parameter specifies if the files without any extension are considered for virus scanning or not.

Examples

The following example modifies an On-Access policy.

```
cluster1::> vserver vscan on-access-policy modify -vserver vs1 -policy
-name test
                -protocol CIFS -scan-mandatory on -filters scan-ro-volume
-max-file-size 10GB
                -file-ext-to-exclude "mp3" -file-ext-to-include "mp*"
-scan-files-with-no-ext false
                -paths-to-exclude "\vol1\temp","\vol2\a"

cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name test
Vserver: vs1
                            Policy: test
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: off
Max File Size Allowed for Scanning: 10GB
             File Paths Not to Scan: \vol1\temp, \vol2\a
       File Extensions Not to Scan: mp3
           File Extensions to Scan: mp*
      Scan Files with No Extension: false
```

vserver vscan on-access-policy show

Display On-Access policies

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy show` command displays information about the On-Access policies belonging to the Vserver. It also displays the current status in Vserver scope. If you do not specify any parameters, the command displays the following information about all On-Access policies:

- Vserver name
- Policy name
- Policy status
- Policy owner

- Protocol
- File paths to exclude
- File extensions to exclude

You can specify the `-fields` parameter to specify which fields of information to display about On-Access policies. In addition to the fields above, you can display the following fields:

- List of filters
- Mandatory scan
- Max file size
- File extensions to include
- Scan files without extension

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the On-Access policies for the specified Vserver.

[-policy-name <Policy name>] - Policy

If you specify this parameter, the command displays information only about the specified On-Access policy.

[-policy-status {on|off}] - Policy Status

If you specify this parameter, the command displays information only about the On-Access policies that have the specified status.

[-owner <Configuration owner>] - Policy Config Owner

If you specify this parameter, the command displays information only about the On-Access policies that have the specified owner.

[-protocol <CIFS>] - File-Access Protocol

If you specify this parameter, the command displays information only about the On-Access policies that have the specified protocol.

[-filters {scan-ro-volume|scan-execute-access}] - Filters

If you specify this parameter, the command displays information only about the On-Access policies that have the specified filter or filters in the filter list.

[-scan-mandatory {on|off}] - Mandatory Scan

If you specify this parameter, the command displays information only about the On-Access policies that have mandatory scanning enabled.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

If you specify this parameter, the command displays information only about the On-Access policies that have the specified max-file-size.

[-paths-to-exclude <File path>,…] - File Paths Not to Scan

If you specify this parameter, the command displays information only about the On-Access policies that have the specified path or paths in the exclude list.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

If you specify this parameter, the command displays information only about the On-Access policies that have the specified file extension or extensions in the exclude list.

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

If you specify this parameter, the command displays information only about the On-Access policies that have the specified file extension or extensions in the include list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

If you specify this parameter, the command displays information only about the On-Access policies that have the specified value.

Examples

The following example displays information about all On-Access policies.

```
cluster1::> vserver vscan on-access-policy show
            Policy     Policy                              File-Ext
Policy
Vserver     Name       Owner    Protocol Paths Excluded    Excluded
Status
----------- ---------  -------- -------- ----------------- -----------
------
Cluster     default_   cluster  CIFS     -                 -           off
            CIFS
vs1         default_   cluster  CIFS     -                 -           on
            CIFS
vs1         new        vserver  CIFS     \vol\temp         txt         off
vs2         default_   cluster  CIFS     -                 -           on
            CIFS
4 entries were displayed.
```

The following example displays detailed information about an On-Access policy.

```
cluster1::> vserver vscan on-access-policy show -instance -vserver vs1
-policy-name new
Vserver: vs1
                             Policy: new
                      Policy Status: off
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 4GB
             File Paths Not to Scan: \vol\temp
       File Extensions Not to Scan: txt
           File Extensions to Scan: *
      Scan Files with No Extension: true
```

vserver vscan on-access-policy file-ext-to-exclude add

Add to the list of file extensions to exclude

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy file-ext-to-exclude add` command adds a file extension or a list of file extensions that must be excluded from scanning to the specified policy name.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy to which you want to add a file extension or a list of file extensions that must be excluded from scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy to which you want to add a file extension or a list of file extensions that must be excluded from scanning.

`-file-ext-to-exclude <File extension>,…` - File Extensions Not to Scan

This parameter specifies the file extension or a list of file extensions that must be excluded from scanning.

Examples

The following example adds a list of file extensions that must be excluded from scanning to the specified on-access policy:

```
cluster1::> vserver vscan on-access-policy file-ext-to-exclude add
-vserver vs1
            -policy-name policy1 -file-ext-to-exclude txt,mp4

cluster1::> vserver vscan on-access-policy file-ext-to-exclude show
-vserver vs1
            -policy-name policy1
Vserver: vs1
                      Policy: policy1
File-Extensions Not to Scan: mp3, mp4, txt, wav
```

vserver vscan on-access-policy file-ext-to-exclude remove

Remove from the list of file extensions to exclude

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy file-ext-to-exclude remove` command removes a file extension or a list of file extensions that are excluded from scanning from the specified policy name.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy from which you want to remove a file extension or a list of file extensions that are excluded from scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy from which you want to remove a file extension or a list of file extensions that are excluded from scanning.

`-file-ext-to-exclude <File extension>,…` - File Extensions Not to Scan

This parameter specifies the file extension or a list of file extensions that must be removed from the on-access policy.

Examples

The following example removes a list of file extensions that are to be excluded from scanning from the specified on-access policy:

```
cluster1::> vserver vscan on-access-policy file-ext-to-exclude remove
-vserver vs1
            -policy-name policy1 -file-ext-to-exclude mp3,txt

cluster1::> vserver vscan on-access-policy file-ext-to-exclude show
-vserver vs1
            -policy-name policy1
Vserver: vs1
                      Policy: policy1
File-Extensions Not to Scan: mp4, wav
```

vserver vscan on-access-policy file-ext-to-exclude show

Display list of file extensions to exclude

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy file-ext-to-exclude show` command displays the list of file extensions that are excluded from scanning belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all on-access policies:

- Vserver name
- Policy name
- List of File-Extensions to exclude

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the policy names for the specified Vserver.

[-policy-name <Policy name>] - Policy

If you specify this parameter, the command displays information only about the specified policy name.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

If you specify this parameter, the command displays information only about the policies that have the specified file extensions that are excluded from scanning.

Examples

The following example displays the list of file extensions that are excluded from scanning for all the policies:

```
cluster1::> vserver vscan on-access-policy file-ext-to-exclude show
Vserver         Policy Name       File-Ext Excluded
--------------- -----------------
-----------------------------------------
cluster1        default_CIFS      txt
vs1             default_CIFS      txt
vs1             policy1           mp4, wav
vs1             policy3           wmv
vs2             default_CIFS      txt
vs2             policy2           mp3
6 entries were displayed.
```

vserver vscan on-access-policy file-ext-to-include add

Add to the list of file extensions to include

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy file-ext-to-include add` command adds a file extension or list of file extensions to include for virus scanning to the specified policy.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy to which you want to add a file extension or a list of file extensions to include for virus scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy to which you want to add a file extension or a list of file extensions to include for virus scanning.

`-file-ext-to-include <File extension>,…` - File Extensions to Scan

This parameter specifies the file extension or a list of file extensions to include for virus scanning.

Examples

The following example adds a list of file extensions to include for virus scanning to the specified on-access policy.

```
cluster1::> vserver vscan on-access-policy file-ext-to-include add
-vserver vs1
            -policy-name policy1 -file-ext-to-include "mp*","tx*"

cluster1::> vserver vscan on-access-policy file-ext-to-include show
-vserver vs1
            -policy-name policy1
Vserver: vs1
                      Policy: policy1
    File Extensions to Scan: mp*, tx*, wav
```

vserver vscan on-access-policy file-ext-to-include remove

Remove from the list of file extensions to include

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy file-ext-to-include remove` command removes a file extension or list of file extension that are included for virus scanning from the specified policy.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy from which you want to remove a file extension or list of file extensions that are included for virus scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy from which you want to remove a file extension or a list of file extensions that are included for virus scanning.

`-file-ext-to-include <File extension>,…` - File Extensions to Scan

This parameter specifies the file extension or a list of file extensions that you want to remove from the specified on-access policy.

Examples

The following example removes a list of file extensions from the specified on-access policy.

```
cluster1::> vserver vscan on-access-policy file-ext-to-include remove
-vserver vs1
            -policy-name policy1 -file-ext-to-include "txt*,"wav"

cluster1::> vserver vscan on-access-policy file-ext-to-include show
-vserver vs1
            -policy-name policy1
Vserver: vs1
                      Policy: policy1
    File Extensions to Scan: mp*
```

vserver vscan on-access-policy file-ext-to-include show

Display list of file extensions to include

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy file-ext-to-include show` command displays the list of file extensions to include for virus scanning belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all on access policies:

- Vserver name
- Policy name
- List of File-Extensions to Scan

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the policies for the specified Vserver.

[-policy-name <Policy name>] - Policy

If you specify this parameter, the command displays information only about the specified policy.

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

If you specify this parameter, the command displays information only about the policies that have the specified file extensions that are included for virus scanning.

Examples

The following example displays the list of file extensions that are included for virus scanning for all policies.

```
cluster1::> vserver vscan on-access-policy file-ext-to-include show
Vserver         Policy Name       File-Ext Included
--------------- -----------------
-----------------------------------------
cluster1        default_CIFS      *
vs1             default_CIFS      *
vs1             policy1           mp*
vs1             policy3           doc*, xl*
vs2             default_CIFS      *
vs2             policy2           d*, m*, t*
6 entries were displayed.
```

vserver vscan on-access-policy paths-to-exclude add

Add to the list of paths to exclude

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy paths-to-exclude add` command adds a path or a list of paths that must be excluded from scanning to the specified policy name.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy to which you want to add a path or a list of paths that must be excluded from scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy to which you want to add a path or a list of paths that must be excluded from scanning.

`-paths-to-exclude <File path>,…` - Paths Not to Scan

This parameter specifies the path or list of paths that must be excluded from scanning.

Examples

The following example adds a list of paths that must be excluded from scanning to the specified on-access policy:

```
cluster1::> vserver vscan on-access-policy paths-to-exclude add -vserver
vs1
            -policy-name policy1 -paths-to-exclude \test\test2,\test\test3

cluster1::> vserver vscan on-access-policy paths-to-exclude show -vserver
vs1
            -policy-name policy1
Vserver: vs1
                Policy: policy1
File-Paths Not to Scan: \test\test1, \test\test2, \test\test3
```

vserver vscan on-access-policy paths-to-exclude remove

Remove from the list of paths to exclude

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy paths-to-exclude remove` command removes a path or a list of paths that are excluded from scanning from the specified policy name.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified on-access policy from which you want to remove a path or list of paths that are excluded from scanning.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the on-access policy from which you want to remove a path or a list of paths that are excluded from scanning.

`-paths-to-exclude <File path>,…` - Paths Not to Scan

This parameter specifies the path or a list of paths that must be removed from the on-access policy.

Examples

The following example removes a list of paths that are excluded from scanning from the specified policy name:

```
cluster:> vserver vscan on-access-policy paths-to-exclude remove -vserver
vs1
          -policy-name policy1 -paths-to-exclude \test\test2,\test\test3

cluster1:> vserver vscan on-access-policy paths-to-exclude show -vserver
vs1
          -policy-name policy1
Vserver: vs1
                 Policy: policy1
File-Paths Not to Scan: \test\test1
```

vserver vscan on-access-policy paths-to-exclude show

Display list of paths to exclude

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-access-policy paths-to-exclude show` command displays the list of paths that are excluded from scanning belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all on-access policies:

- Vserver name
- Policy name
- List of Paths to exclude

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the policy names for the specified Vserver.

[-policy-name <Policy name>] - Policy

If you specify this parameter, the command displays information only about the specified policy name.

[-paths-to-exclude <File path>,…] - File Paths Not to Scan

If you specify this parameter, the command displays information only about the policies that have the specified paths that are excluded from scanning.

Examples

The following example displays the list of paths that are excluded from scanning for all the policies:

```
cluster1::> vserver vscan on-access-policy paths-to-exclude  show
Vserver         Policy Name       Paths Excluded
--------------- -----------------
-----------------------------------------
cluster1        default_CIFS      \test\test1
vs1             default_CIFS      \test\test1
vs1             policy1           \test\test2,\test\test3
vs1             policy3           \test\test4
vs2             default_CIFS      \test\test1
vs2             policy2           \test\test5
6 entries were displayed.
```

vserver vscan on-demand-task create

Create an On-Demand task

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-demand-task create` command creates an On-Demand task. The On-Demand task consists of a set of attributes that are used for configuring the scope of scanning. It also specifies the cron schedule at which the task should run.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create an On-Demand task.

`-task-name <text>` - Task Name

This parameter specifies the name of the On-Demand task that you want to create. An On-Demand task name can be up to 256 characters long.

`-scan-paths <text>,…` - List of Scan Paths

This parameter specifies a list of paths, separated by commas, for virus scanning. This path is given from the root of the Vserver using UNIX path delimiter "/".

`-report-directory <text>` - Report Directory Path

This parameter specifies a directory path where the On-Demand report file is created. Each run for a task creates a new file. The report directory path is given from the root of the Vserver using UNIX path delimiter "/".

[-schedule <text>] - Job Schedule

This parameter specifies the already existing cron schedule. The On-Demand task triggers virus scanning for the specified scan-paths at the time configured in the schedule.

> A Vserver can have only one scheduled task at a time.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

This parameter specifies the maximum size of the file that will be considered for virus scanning. By default, it is *10GB* .

[-paths-to-exclude <text>,…] - File Paths Not to Scan

This parameter specifies a list of paths, separated by commas, to exclude from virus scanning. This path is given from the root of the Vserver using UNIX path delimiter "/". By default, no paths are excluded. The path can be in one of the following forms:

- */dir1/dir2/name* - This would match "/dir1/dir2/name" as well as "/dir1/dir2/name/…".
- */dir1/dir2/name/* - This would only match "/dir1/dir2/name/…".

> If you are using the CLI, you must delimit all paths with double quotation marks ("). For instance, to add the paths "/vol/a b/" and "/vol/a,b/" to the `-paths-to-exclude` in the CLI, type *"/vol/a b/","/vol/a,b/"* at the command prompt.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

This parameter specifies a list of file extensions, separated by commas, to exclude from virus scanning. By default, no file extensions are excluded. Each file extension can be up to 16 characters long. The `-file-ext-to-exclude` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** matches mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* matches mp3, mp4 but not mp and mpeg.

> If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

This parameter specifies a list of file extensions, separated by commas, to include for virus scanning. By default it is *** , which means all the file extensions are considered for virus scanning except those that match one of the patterns provided in `-file-ext-to-exclude` list. Each file extension can be up to 16 characters long. The `-file-ext-to-include` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** matches mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* matches mp3, mp4 but not mp and mpeg.

> If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

If you specify both `-file-ext-to-include` and `-file-ext-to-exclude` lists, then only those file extensions are considered for virus scanning which match one of the patterns provided in `-file-ext-to-include` list but do not match any of the patterns provided in `-file-ext-to-exclude` list.

`[-scan-files-with-no-ext {true|false}]` - Scan Files with No Extension

This parameter specifies if the files without any extension are considered for virus scanning or not. By default, it is true.

`[-request-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Request Service Timeout

This parameter specifies the timeout value for a scan request. It is used to specify the time interval in which the node waits for a response from the Vscan server. Beyond this timeout period, the scan request is considered as failed. The value for this field must be between 10s and 1h. By default, it is 5m.

`[-cross-junction {true|false}]` - Cross Junction

This parameter specifies if the On-Demand task is allowed to cross volume junctions. If the parameter is set to false, crossing junctions is not allowed. By default, it is true.

`[-directory-recursion {true|false}]` - Directory Recursion

This parameter specifies if the On-Demand task is allowed to recursively scan through sub-directories. If the parameter is set to false, recursive scanning is not allowed. By default, it is true.

`[-scan-priority {low|normal}]` - Scan Priority

This parameter specifies the priority of the On-Demand scan requests generated by this task compared to On-Access scan requests. By default, it is low.

`[-report-log-level {verbose|info|error}]` - Report Log Level

This parameter specifies the log level of the On-Demand report. By default, it is info.

`[-report-expiry-time <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Expiration Time for Report

This parameter specifies the expiration time for the reports generated by On-Demand scans. Once this time elapses, the reports are auto-deleted. The default value is 0, which means reports are retained until they are manually deleted.

Examples

The following example creates an On-Demand task:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name t1
            -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
            -schedule daily -max-file-size 5GB -paths-to-exclude
"/vol1/cold-files/"
            -file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude
"mp3","mp4"
            -scan-files-with-no-ext false -request-timeout 2m -cross
-junction false
            -directory-recursion true -scan-priority low -report-log-level
verbose
            -report-expiry-time 12h
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.

cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                         Task Name: t1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 2m
                    Cross Junction: false
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: verbose
```

vserver vscan on-demand-task delete

Delete an On-Demand task

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-demand-task delete` command deletes an On-Demand task.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver from which you want to delete an On-Demand task.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task that you want to delete.

Examples

The following example deletes an On-Demand task:

```
cluster1::> vserver vscan on-demand-task delete -vserver vs1 -task-name t1

cluster1::> vserver vscan on-demand-task show -vserver vs1 -task-name t1
There are no entries matching your query.
```

vserver vscan on-demand-task modify

Modify an On-Demand task

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-demand-task modify` command modifies an On-Demand task. The On-Demand task consists of a set of attributes that are used for configuring the scope of scanning. It also specifies the cron schedule at which the task should run.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to modify an On-Demand task.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task that you want to modify.

[-scan-paths <text>,…] - List of Scan Paths

This parameter specifies a list of paths, separated by commas, for virus scanning. This path is given from the root of the Vserver using UNIX path delimiter "/".

[-report-directory <text>] - Report Directory Path

This parameter specifies a directory path where the On-Demand report file is created. Each run for a task creates a new file. The report directory path is given from the root of the Vserver using UNIX path delimiter "/".

[-schedule <text>] - Job Schedule

This parameter specifies the already existing cron schedule. The On-Demand task triggers virus scanning for the specified scan-paths at the time configured in the schedule. Providing empty schedule ("") unschedules the task.

A Vserver can have only one scheduled task at a time.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

This parameter specifies the maximum size of the file which will be considered for virus scanning.

[-paths-to-exclude <text>,…] - File Paths Not to Scan

This parameter specifies a list of paths, separated by commas, to exclude from virus scanning. This path is given from the root of the Vserver using UNIX path delimiter "/". The path can be in one of the following forms:

- */dir1/dir2/name* - This would match "/dir1/dir2/name" as well as "/dir1/dir2/name/…".
- */dir1/dir2/name/* - This would only match "/dir1/dir2/name/…".

If you are using the CLI, you must delimit all paths with double quotation marks ("). For instance, to add the paths "/vol/a b/" and "/vol/a,b/" to the `-paths-to-exclude` in the CLI, type *"/vol/a b/","/vol/a,b/"* at the command prompt.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

This parameter specifies a list of file extensions, separated by commas, to exclude from virus scanning. Each file extension can be up to 16 characters long. The `-file-ext-to-exclude` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** matches mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* matches mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

This parameter specifies a list of file extensions, separated by commas, to include for virus scanning. Each file extension can be up to 16 characters long. The `-file-ext-to-include` supports wildcard patterns containing "*" and "?". Pattern matching is defined as:

- *** - Matches any string, including the empty string. For example, *mp** matches mp, mp3, mp4, mpeg etc.
- *?* - Matches any single character. For example, *mp?* matches mp3, mp4 but not mp and mpeg.

If you are using the CLI, you must delimit all patterns with double quotation marks ("). For instance, to enter the pattern *mp** in the CLI, type *"mp*"* at the command prompt. To add a "?" to the expression, press ESC followed by the "?".

If you specify both `-file-ext-to-include` and `-file-ext-to-exclude` lists, then only those file extensions are considered for virus scanning which match one of the patterns provided in `-file-ext-to-include` list but do not match any of the patterns provided in `-file-ext-to-exclude` list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

This parameter specifies if the files without any extension are considered for virus scanning or not.

[-request-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Request Service Timeout

This parameter specifies the timeout value for a scan request. It is used to specify the time interval in which the node waits for a response from the Vscan server. Beyond this timeout period, the scan request is considered as failed. The value for this field must be between 10s and 1h.

[-cross-junction {true|false}] - Cross Junction

This parameter specifies if the On-Demand task is allowed to cross volume junctions. If the parameter is set to false, crossing junctions is not allowed.

[-directory-recursion {true|false}] - Directory Recursion

This parameter specifies if the On-Demand task is allowed to recursively scan through sub-directories. If the parameter is set to false, recursive scanning is not allowed.

[-scan-priority {low|normal}] - Scan Priority

This parameter specifies the priority of the On-Demand scan requests generated by this task compared to On-Access scan requests.

[-report-log-level {verbose|info|error}] - Report Log Level

This parameter specifies the log level of the On-Demand report.

[-report-expiry-time <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Expiration Time for Report

This parameter specifies the expiration time for the reports generated by On-Demand scans. Once this time elapses, the reports are auto-deleted. The default value is 0, which means reports are retained until they are manually deleted.

Examples

The following example modifies an On-Demand task:

```
cluster1::> vserver vscan on-demand-task modify -vserver vs1 -task-name t1
            -scan-paths "/vol3/","/vol4/cifs/" -report-directory "/report-
dir"
            -schedule custom -max-file-size 2GB -paths-to-exclude
"/vol1/cold-files/"
            -file-ext-to-include "*" -file-ext-to-exclude "mp3","mp4"
            -scan-files-with-no-ext true -request-timeout 1m -cross
-junction true
[Job 136]: Vscan On-Demand job is queued. Use the "job show -id 136"
command to view the status.

cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                         Task Name: t1
                List of Scan Paths: /vol3/, /vol4/cifs/
             Report Directory Path: /report-dir
                      Job Schedule: custom
Max File Size Allowed for Scanning: 2GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: *
      Scan Files with No Extension: true
           Request Service Timeout: 1m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: verbose
```

vserver vscan on-demand-task run

Run an On-Demand task

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-demand-task run` command start virus scanning immediately for an On-Demand task.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to start start virus scanning.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task that you want to start virus scanning.

Examples

The following example starts virus scanning an On-Demand task:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name t1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

vserver vscan on-demand-task schedule

Schedule an On-Demand task

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-demand-task schedule` command schedules an On-Demand task.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to schedule an On-Demand task.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task that you want to schedule.

-schedule <text> - Schedule Name

This parameter specifies the already existing cron schedule. The On-Demand task triggers virus scanning for the specified scan-paths at the time configured in the schedule.

A Vserver can have only one scheduled task at a time.

Examples

The following example schedules an On-Demand task:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs1 -task-name
t1 -schedule daily
[Job 150]: Vscan On-Demand job is queued. Use the "job show -id 150"
command to view the status.

cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                         Task Name: t1
                List of Scan Paths: /test
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 2GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: *
      Scan Files with No Extension: true
           Request Service Timeout: 1m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: verbose
```

vserver vscan on-demand-task show

Display On-Demand tasks

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-demand-task show` command displays information about the On-Demand tasks belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all On-Demand tasks:

- Vserver name
- Task name
- Scan paths
- Report directory path
- Schedule

You can specify the `-fields` parameter to specify which fields of information to display about On-Demand tasks. In addition to the fields above, you can display the following fields:

- Max file size

- File paths to exclude
- File extensions to exclude
- File extensions to include
- Scan files without extension
- Scan timeout
- Cross junction
- Directory recursion
- Scan priority
- Report log level

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the On-Demand tasks for the specified Vserver.

[-task-name <text>] - Task Name

If you specify this parameter, the command displays information only about the specified On-Demand task.

[-scan-paths <text>,…] - List of Scan Paths

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified path or paths in the scan-paths list.

[-report-directory <text>] - Report Directory Path

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified report-directory.

[-schedule <text>] - Job Schedule

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified schedule.

[-max-file-size {<integer>[KB|MB|GB|TB|PB]}] - Max File Size Allowed for Scanning

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified max-file-size.

[-paths-to-exclude <text>,…] - File Paths Not to Scan

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified path or paths in the exclude list.

[-file-ext-to-exclude <File extension>,…] - File Extensions Not to Scan

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified file extension or extensions in the exclude list.

[-file-ext-to-include <File extension>,…] - File Extensions to Scan

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified file extension or extensions in the include list.

[-scan-files-with-no-ext {true|false}] - Scan Files with No Extension

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified value.

[-request-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Request Service Timeout

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified request-timeout.

[-cross-junction {true|false}] - Cross Junction

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified value.

[-directory-recursion {true|false}] - Directory Recursion

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified value.

[-scan-priority {low|normal}] - Scan Priority

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified scan-priority.

[-report-log-level {verbose|info|error}] - Report Log Level

If you specify this parameter, the command displays information only about the On-Demand tasks that have the specified report-log-level.

[-report-expiry-time <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Expiration Time for Report

This parameter specifies the expiration time for the reports generated by On-Demand scans. Once this time elapses, the reports are auto-deleted. The default value is 0, which means reports are retained until they are manually deleted.

Examples

The following example displays information about all On-Demand tasks:

```
cluster1::> vserver vscan on-demand-task show
                                            Report
Vserver     Task Name   Scan Paths          Directory Path    Schedule
----------- ----------  ------------------- -----------------
--------------
vs1         t1          /test               /report           -
vs2         t2          /, /test/           /report           daily
2 entries were displayed.
```

The following example displays detailed information about an On-Demand task:

```
cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                         Task Name: t1
                List of Scan Paths: /test
             Report Directory Path: /report
                       Job Schedule: -
Max File Size Allowed for Scanning: 2GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: *
      Scan Files with No Extension: true
           Request Service Timeout: 1m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: verbose
```

vserver vscan on-demand-task unschedule

Unschedule an On-Demand task

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-demand-task unschedule` command unschedules an On-Demand task.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to unschedule an On-Demand task.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task that you want to unschedule.

Examples

The following example unschedules an On-Demand task:

```
cluster1::> vserver vscan on-demand-task unschedule -vserver vs1 -task
-name t1

cluster1::> vserver vscan on-demand-task show -instance -vserver vs1 -task
-name t1
Vserver: vs1
                         Task Name: t1
                List of Scan Paths: /test
             Report Directory Path: /report
                      Job Schedule: -
Max File Size Allowed for Scanning: 2GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: *
      Scan Files with No Extension: true
           Request Service Timeout: 1m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: verbose
```

vserver vscan on-demand-task report delete

Delete an On-Demand report

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-demand-task report delete` command deletes an On-Demand report.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver from which you want to delete an On-Demand report.

-task-name <text> - Task Name

This parameter specifies the name of the On-Demand task whose report you want to delete.

-report-file <text> - Report File Path

This parameter specifies the path of the report-file whose report record you want to delete.

[-delete-report-file {true|false}] - Delete Report File Also

This parameter specifies if the corresponding report file is also to be deleted. By default, it is false.

Examples

The following example deletes only On-Demand report record:

```
cluster1::> vserver vscan on-demand-task report delete -vserver vs1 -task
-name t1
            -report-file /rep/avod_146_20150902_161439.log

cluster1::> vserver vscan on-demand-task report delete -vserver vs1 -task
-name t1
            -report-file /rep/avod_146_20150902_161439.log
There are no entries matching your query.
```

The following example deletes an On-Demand report file along with the report record:

```
cluster1::> vserver vscan on-demand-task report delete -vserver vs1 -task
-name t1
            -report-file /rep/avod_146_20150902_161439.log -delete-report
-file true

cluster1::> vserver vscan on-demand-task report delete -vserver vs1 -task
-name t1
            -report-file /rep/avod_146_20150902_161439.log -delete-report
-file true
There are no entries matching your query.
```

vserver vscan on-demand-task report show

Display On-Demand reports

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan on-demand-task report show` command displays information about the On-Demand reports belonging to the Vserver. A new report record is generated at the end of an On-Demand task run. If you do not specify any parameters, the command displays the following information about all On-Demand tasks:

- Vserver name

- Task name
- Report file path
- Number of clean files
- Number of infected files

You can specify the `-fields` parameter to specify which fields of information to display about On-Demand report. In addition to the fields above, you can display the following fields:

- Job ID
- Job duration
- Number of attempted scans
- Number of files skipped from scanning
- Number of already scanned files
- Number of successful scans
- Number of failed scans
- Number of timed-out scans
- Job start time
- Job end time

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the On-Demand reports for the specified Vserver.

[-task-name <text>] - Task Name

If you specify this parameter, the command displays information only about the On-Demand reports for the specified task.

[-report-file <text>] - Report File Path

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified report file-path.

[-job-id <integer>] - Job ID

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified job ID.

[-job-duration <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Job Duration

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-attempted-scans <integer>] - Number of Attempted Scans

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-skipped-scans <integer>] - Number of Files Skipped from Scanning

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-already-scanned-files <integer>] - Number of Already Scanned Files

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-successful-scans <integer>] - Number of Successful Scans

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-failed-scans <integer>] - Number of Failed Scans

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-timedout-scans <integer>] - Number of Timedout Scans

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-files-cleaned <integer>] - Number of Clean Files

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-files-infected <integer>] - Number of Infected Files

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-internal-error <integer>] - Number of Internal Error (privilege: advanced)

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-scan-retries <integer>] - Number of Scan Retries (privilege: advanced)

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-job-start-time <MM/DD/YYYY HH:MM:SS>] - Job Start Time

If you specify this parameter, the command displays information only about the On-Demand reports that have the specified value.

[-job-end-time <MM/DD/YYYY HH:MM:SS>] - Job End Time

If you specify this parameter, the command displays information only about the On-Demand reports that

have the specified value.

Examples

The following example displays information about all On-Demand reports:

```
cluster1::> vscan on-demand-task report show
                                                                  Files
Files
Vserver     Task Name   Report File Path                    Cleaned
Infected
----------- ----------  ---------------------------------- ---------
---------
vs1         t1          /rep/avod_146_20150902_161439.log       6240
5
vs1         t1          /rep/avod_149_20150903_160313.log        115
0
2 entries were displayed.
```

The following example displays detailed information about an On-Demand task:

```
cluster1::> vscan on-demand-task report show -vserver vs1 -task-name t1
            -report-file /rep/avod_146_20150902_161439.log
Vserver: vs1
                            Task Name: t1
                     Report File Path: /rep/avod_146_20150902_161439.log
                               Job ID: 146
                         Job Duration: 76s
             Number of Attempted Scans: 6245
Number of Files Skipped from Scanning: 1286
      Number of Already Scanned Files: 987
           Number of Successful Scans: 6245
               Number of Failed Scans: 0
             Number of Timedout Scans: 0
                Number of Clean Files: 6240
             Number of Infected Files: 5
                       Job Start Time: 9/2/2015 16:14:39
                         Job End Time: 9/2/2015 16:15:55
```

vserver vscan scanner-pool apply-policy

Apply scanner-policy to a scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool apply-policy` command applies a scanner policy to the specified scanner pool on a specified Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to apply the scanner policy. The Vserver administrator can apply the scanner policy to a scanner pool created within the scope of the Vserver or the cluster. The cluster administrator can apply the scanner policy to a scanner pool for any Vserver but cannot apply it within the scope of cluster. The scope is determined at a Vserver level.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool.

`-scanner-policy <Scanner policy>` - Scanner Policy

This parameter specifies the scanner policy that you want to apply to the specified scanner pool on a Vserver. Currently only system policies are available. Available system policies are:

- *`primary`* - Makes it active always.
- *`secondary`* - Makes it active only when none of the primary external virus-scanning servers are connected.
- *`idle`* - Makes it inactive always.

`[-cluster <Cluster name>]` - Cluster on Which Policy Is Applied

This parameter specifies the name of the cluster on which you want to apply the scanner policy of a scanner pool. By default, it is applied on the local cluster. This parameter does not have any significance if the cluster is not in a DR relationship.

Examples

The following command applies a scanner policy to the specified scanner pool on a specified Vserver.

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
            -scanner-pool p1 -scanner-policy primary -cluster cluster2

cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool p1
Vserver: vs1
                        Scanner Pool: p1
                      Applied Policy: primary
                      Current Status: on
  Cluster on Which Policy Is Applied: cluster2
           Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2
            List of Privileged Users: cifs\u1, cifs\u2
```

vserver vscan scanner-pool create

Create a scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool create` command creates a Vscan scanner pool. Scanner pool is a set of attributes which are used to validate and manage connection between ONTAP and external virus-scanning server, or "Vscan server". It also specifies other parameters which are used for connection management. After creating a scanner pool, a scanner-policy must be applied to it using the command vserver vscan scanner-pool apply-policy . The default applied policy is *`idle`* , which means the scanner pool is inactive.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create a scanner pool.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool. Scanner pool name can be up to 256 characters long and is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "_", "-" and ".".

`-hostnames <text>,…` - List of Host Names of Allowed Vscan Servers

This parameter specifies a list of host names or IP addresses of the Vscan servers which are allowed to connect to ONTAP.

`-privileged-users <Privileged user>,…` - List of Privileged Users

This parameter specifies a list of privileged users. A valid form of privileged user-name is "domain-name\user-name" and can be up to 256 characters long. Privileged user-names are stored and treated as case-insensitive strings. Virus scanners must use one of the registered privileged users for connecting to ONTAP for exchanging virus-scanning protocol messages and to access file for scanning, remedying and quarantining operations.

`[-request-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Request Service Timeout (privilege: advanced)

This parameter specifies the timeout value for a scan request. It specifies the time interval in which the node waits for a response from the Vscan server. If the timeout is reached, the node allows the file-operation if the applicable On-Access policy has scan-mandatory set to 'off'. If the policy has scan-mandatory set to 'on', then the node will retry the scan or disallow the file-operation depending on the remaining lifetime of the CIFS request. Valid values for this field are from 10s to 40s. However, if scan-mandatory is set to 'off', the effective value is limited to a maximum of 35s. The default value is 30s.

`[-scan-queue-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Scan Queue Timeout (privilege: advanced)

This parameter specifies the timeout value for a scan request in scan-engine’s queue. The value for this field must be between 10s and 30s. By default, it is 20s.

[-session-setup-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Session Setup Timeout (privilege: advanced)

This parameter specifies the timeout value for a response for session-setup-message. The value for this field must be between 5s and 10s. By default, it is 10s.

[-session-teardown-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Session Teardown Timeout (privilege: advanced)

This parameter specifies the timeout value for a response for session-teardown-message, or for any message to be received for a session-id, after the underlying connection has been disconnected. The value for this field must be between 5s and 10s. By default, it is 10s.

[-max-session-setup-retries <integer>] - Max Number of Consecutive Session Setup Attempts (privilege: advanced)

This parameter specifies the maximum number of consecutive session-setup attempts. The value for this field must be between 1 and 10. By default, it is 5.

Examples

The following example creates a scanner pool.

```
Cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP
            -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2

Cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool SP
Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

Related Links

- vserver vscan scanner-pool apply-policy

vserver vscan scanner-pool delete

Delete a scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool delete` command deletes a scanner pool.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver from which you want to delete a scanner pool.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner-pool that you want to delete.

Examples

The following example deletes a scanner pool.

```
cluster1::> vserver vscan scanner-pool delete -vserver vs1 -scanner-pool
test

cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
test
There are no entries matching your query.
```

vserver vscan scanner-pool modify

Modify a scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool modify` command modifies a Vscan scanner pool. Scanner pool is a set of attributes which are used to validate and manage connection between ONTAP and external virus-scanning server, or "Vscan server". It also specifies other parameters which are used for connection management.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver on which you want to modify a scanner pool.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool. Scanner pool name can be up to 256 characters long and is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "_", "-" and ".".

[-hostnames <text>,…] - List of Host Names of Allowed Vscan Servers

This parameter specifies a list of host names or IP addresses of the Vscan servers which are allowed to connect to ONTAP.

[-privileged-users <Privileged user>,…] - List of Privileged Users

This parameter specifies a list of privileged users. A valid form of privileged user-name is "domain-name\user-name" and can be up to 256 characters long. Privileged user-names are stored and treated as case-insensitive strings. Virus scanners must use one of the registered privileged users for connecting to ONTAP for exchanging virus-scanning protocol messages and to access file for scanning, remedying and quarantining operations.

[-request-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Request Service Timeout (privilege: advanced)

This parameter specifies the timeout value for a scan request. It specifies the time interval in which the node waits for a response from the Vscan server. If the timeout is reached, the node allows the file-operation if the applicable On-Access policy has scan-mandatory set to 'off'. If the policy has scan-mandatory set to 'on', then the node will retry the scan or disallow the file-operation depending on the remaining lifetime of the CIFS request. Valid values for this field are from 10s to 40s. However, if scan-mandatory is set to 'off', the effective value is limited to a maximum of 35s.

[-scan-queue-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Scan Queue Timeout (privilege: advanced)

This parameter specifies the timeout value for a scan request in scan-engine’s queue. The value for this field must be between 10s and 30s.

[-session-setup-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Session Setup Timeout (privilege: advanced)

This parameter specifies the timeout value for a response for session-setup-message. The value for this field must be between 5s and 10s.

[-session-teardown-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Session Teardown Timeout (privilege: advanced)

This parameter specifies the timeout value for a response for session-teardown-message, or for any message to be received for a session-id, after the underlying connection has been disconnected. The value for this field must be between 5s and 10s.

[-max-session-setup-retries <integer>] - Max Number of Consecutive Session Setup Attempts (privilege: advanced)

This parameter specifies the maximum number of consecutive session-setup attempts. The value for this field must be between 1 and 10.

Examples

The following example modifies a scanner pool.

```
Cluster1::> vserver vscan scanner-pool modify -vserver vs1 -scanner-pool
SP
            -hostnames 2.2.2.2,vmwin204-29.fsct.nb -privileged-users
cifs\u3

Cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool SP
Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 2.2.2.2, 10.72.204.29
List of Host Names of Allowed Vscan Servers: 2.2.2.2, vmwin204-29.fsct.nb
                   List of Privileged Users: cifs\u3
```

vserver vscan scanner-pool resolve-hostnames

Resolve the hostnames configured in the scanner pool

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool resolve-hostnames` command resolves the host names configured in the scanner pool and update it with the IP addresses. This command also updates the active scanner pool configuration of the Vserver if the scanner pool is part of that. You must run this command for the scanner pool whose host name entry is modified in the DNS server.

Parameters

`-vserver <vserver>` - Vserver

This parameter specifies the name of the Vserver for which you want to resolve host names.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool for which you want to resolve host names.

Examples

The following example resolves the host names of a scanner pool:

```
cluster1::> vserver vscan scanner-pool resolve-hostnames -vserver vs1
-scanner-pool SP

Cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool SP
Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: Cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 10.72.204.27, 10.72.204.29
List of Host Names of Allowed Vscan Servers: vmwin204-27.fsct.nb,
vmwin204-29.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

vserver vscan scanner-pool show-active

Display active scanner pools

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool show-active` command displays active scanner pool information available to the Vserver. The active scanner pool configuration is derived by merging the information of the scanner pools which are currently active on a Vserver. If you do not specify any parameters, the command displays the following information about all Vservers:

- Vserver name
- List of scanner pools
- List of servers
- List of privileged user

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the specified Vserver.

[-scanner-pools <Scanner pool>,…] - List of Enabled Scanner Pools

If you specify this parameter, the command displays information only about the Vservers that have the specified scanner pool or pools. A scanner pool becomes part of this list if it is active at this time.

[-servers <IP Address>,…] - Merged List of IPs of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the Vservers that have the specified server or servers. Servers of all active scanner pools on a Vserver are merged to derive this effective server list.

[-privileged-users <Privileged user>,…] - Merged List of Privileged Users

If you specify this parameter, the command displays information only about the Vservers that have the specified privileged user or users. Privileged users of all active scanner pools on a Vserver are merged to derive this effective privileged user list.

[-request-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Request Service Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified request-timeout. This is set to the maximum value of the request-timeout of all active scanner pools on a Vserver.

[-scan-queue-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Scan Queue Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified scan-queue-timeout. This is set to the maximum value of the scan-queue-timeout of all active scanner pools on a Vserver.

[-session-setup-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Session Setup Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified session-setup-timeout. This is set to the maximum value of the session-setup-timeout of all active scanner pools on a Vserver.

[-session-teardown-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Session Teardown Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified session-teardown-timeout. This is set to the maximum value of the session-teardown-timeout of all active scanner pools on a Vserver.

[-max-session-setup-retries <integer>] - Max Number of Consecutive Session Setup Attempts (privilege: advanced)

If you specify this parameter, the command displays information only about the Vservers that have the specified max-session-setup-retries. This is set to the maximum number of the max-session-setup-retry of all active scanner pools on a Vserver.

Examples

The following example displays information about active scanner pool on all Vservers.

```
cluster1::> vserver vscan scanner-pool show
            Scanner    Pool                          Privileged
Scanner
Vserver     Pool       Owner   Servers               Users           Policy
----------- ---------- ------- -------------------- ---------------
----------
Cluster     clus       cluster 5.5.5.5              cifs\u5         idle
vs1         new        vserver 1.1.1.1, 2.2.2.2     cifs\u1
primary
vs1         clus       cluster 5.5.5.5              cifs\u5         idle
vs1         p1         vserver 3.3.3.3              cifs\u4
primary
vs2         clus       cluster 5.5.5.5              cifs\u5
primary
vs2         p2         vserver 3.3.3.3, 4.4.4.4     cifs\u2
primary
6 entries were displayed.

cluster1::> vserver vscan scanner-pool show-active
                                                      Privileged
Vserver     Scanner Pools      Servers                     Users
----------- ------------ --------------------------
------------------------
vs1         new, p1       1.1.1.1, 2.2.2.2, 3.3.3.3   cifs\u1, cifs\u4
vs2         clus, p2      3.3.3.3, 4.4.4.4, 5.5.5.5   cifs\u2, cifs\u5
2 entries were displayed.
```

vserver vscan scanner-pool show

Display scanner pools

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool show` command displays information about the Vscan scanner pools belonging to the Vserver. It also displays the scanner policy applied to the scanner pool and its current status in Vserver scope. If you do not specify any parameters, the command displays the following information about all scanner pools:

- Vserver name
- Scanner pool
- Scanner pool owner
- Scanner policy
- Current status

- Cluster on which policy is applied
- List of servers
- List of host names
- List of privileged user

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the scanner pools for the specified Vserver.

[-scanner-pool <Scanner pool>] - Scanner Pool

If you specify this parameter, the command displays information only about the specified scanner pool.

[-scanner-policy <Scanner policy>] - Applied Policy

If you specify this parameter, the command displays information only about the scanner pools for the specified scanner policy.

[-current-status {on|off}] - Current Status

If you specify this parameter, the command displays information only about the scanner pools that have the specified status.

[-cluster <Cluster name>] - Cluster on Which Policy Is Applied

If you specify this parameter, the command displays information only about the scanner pools that are applied to the specified cluster.

[-owner <Configuration owner>] - Scanner Pool Config Owner

If you specify this parameter, the command displays information only about the scanner pools that have the specified owner.

[-servers <IP Address>,…] - List of IPs of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the scanner pools that have the specified IP address or IP addresses.

[-hostnames <text>,…] - List of Host Names of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the scanner pools that have the specified host name or host names.

[-privileged-users <Privileged user>,…] - List of Privileged Users

If you specify this parameter, the command displays information only about the scanner pools that have the specified privileged user or users.

[-request-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Request Service Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified request-timeout.

[-scan-queue-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Scan Queue Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified scan-queue-timeout.

[-session-setup-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Session Setup Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified session-setup-timeout.

[-session-teardown-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Session Teardown Timeout (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified session-teardown-timeout.

[-max-session-setup-retries <integer>] - Max Number of Consecutive Session Setup Attempts (privilege: advanced)

If you specify this parameter, the command displays information only about the scanner pools that have the specified max-session-setup-retries.

Examples

The following example displays information about all scanner pools.

```
Cluster1::> vserver vscan scanner-pool show
            Scanner    Pool                          Privileged
Scanner
Vserver     Pool       Owner   Servers               Users           Policy
----------- ---------- ------- -------------------- ---------------
----------
vs1         SP         vserver 1.1.1.1,             cifs\u1,
primary
                               10.72.204.27         cifs\u2
vs1         p1         vserver 3.3.3.3              cifs\u1,
secondary
                                                    cifs\u2
2 entries were displayed.
```

The following example displays detailed information about one scanner pool.

```
Cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool SP
Vserver: vs1
                                Scanner Pool: SP
                              Applied Policy: primary
                              Current Status: on
         Cluster on Which Policy Is Applied: Cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

vserver vscan scanner-pool privileged-users add

Add to the list of privileged users

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool privileged-users add` command adds one privileged users or list of privileged users to the specified scanner pool.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified scanner pool on which you want to add a privileged user or users.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool to which you want to add a privileged user or users.

`-privileged-users <Privileged user>,…` - List of Privileged Users

This parameter specifies a list of privileged users. A valid form of privileged user-name is "domain-name\user-name" and can be up to 256 characters long. Privileged user-names are stored and treated as case-insensitive strings. Virus scanners must use one of the registered privileged users for connecting to ONTAP for exchanging virus-scanning protocol messages and to access file for scanning, remedying and quarantining operations.

Examples

The following example adds a list of privileged users to the specified scanner pool.

```
cluster1::> vserver vscan scanner-pool privileged-users add -vserver vs1
            -scanner-pool p1 -privileged-users cifs\u2,cifs\u3

cluster1::> vserver vscan scanner-pool privileged-users show -vserver vs1
            -scanner-pool p1
Vserver: vs1
            Scanner Pool: p1
List of Privileged Users: cifs\u1, cifs\u2, cifs\u3
```

vserver vscan scanner-pool privileged-users remove

Remove from the list of privileged users

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool privileged-users remove` command removes one privileged users or list of privileged users from the specified scanner pool. All the existing privileged users of a scanner pool cannot be removed.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified scanner pool on which you want to remove a privileged user or users.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool from which you want to remove a privileged user or users.

`-privileged-users <Privileged user>,…` - List of Privileged Users

This parameter specifies the privileged user or users that you want to remove from the specified scanner pool.

Examples

The following example removes a list of privileged users from the specified scanner pool.

```
cluster1::> vserver vscan scanner-pool privileged-users remove -vserver
vs1
            -scanner-pool p1 -privileged-users cifs\u2,cifs\u3

cluster1::> vserver vscan scanner-pool privileged-users show -vserver vs1
            -scanner-pool p1
Vserver: vs1
            Scanner Pool: p1
List of Privileged Users: cifs\u1
```

vserver vscan scanner-pool privileged-users show

Display list of privileged users

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool privileged-users show` command displays the list of privileged users of the Vscan scanner pools belonging to the Vserver. If you do not specify any parameters, the command displays the following information about the scanner pools:

- Vserver name
- Scanner pool
- List of privileged users

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the scanner pools for the specified Vserver.

[-scanner-pool <Scanner pool>] - Scanner Pool

If you specify this parameter, the command displays information only for the specified scanner pool.

[-privileged-users <Privileged user>,…] - List of Privileged Users

If you specify this parameter, the command displays information only about the scanner pools that have the specified privileged user or users.

Examples

The following example displays the list of privileged users of all scanner pools.

```
cluster1::> vserver vscan scanner-pool privileged-users show
Vserver         Scanner Pool      Privileged Users
--------------- -----------------
-------------------------------------------
Cluster         clus              cifs\u5
vs1             new               cifs\u7
vs1             clus              cifs\u5
vs1             p1                cifs\u1, cifs\u2
vs2             clus              cifs\u5
vs2             p2                cifs\u2
6 entries were displayed.
```

vserver vscan scanner-pool servers add

Add to the list of hostnames

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool servers add` command adds one server or list of servers to the specified scanner pool.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified scanner pool on which you want to add a server or servers.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool to which you want to add a server or servers.

`-hostnames <text>,…` - List of Host Names for Vscan Servers

This parameter specifies the host name or host names that you want to add to the specified scanner pool.

Examples

The following example adds a list of servers to the specified scanner pool.

```
Cluster1::> vserver vscan scanner-pool servers add -vserver vs1
            -scanner-pool SP -hostnames 2.2.2.2, vmwin204-27.fsct.nb

Cluster1::> vserver vscan scanner-pool servers show -vserver vs1 -scanner
-pool SP
Vserver: vs1
                               Scanner Pool: SP
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2,
10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2,
                                            vmwin204-27.fsct.nb
```

vserver vscan scanner-pool servers remove

Remove from the list of hostnames

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool servers remove` command removes one server or list of servers from the specified scanner pool. All the existing servers of a scanner pool cannot be removed.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver containing the specified scanner pool on which you want to remove a server or servers.

`-scanner-pool <Scanner pool>` - Scanner Pool

This parameter specifies the name of the scanner pool from which you want to remove a server or servers.

`-hostnames <text>,…` - List of hostnames for Vscan Servers

This parameter specifies the host name or host names that you want to remove from the specified scanner pool.

Examples

The following example removes a list of servers from the specified scanner pool.

```
Cluster1::> vserver vscan scanner-pool servers remove -vserver vs1
-scanner-pool SP -hostnames vmwin204-27.fsct.nb

Cluster1::> vserver vscan scanner-pool servers show -vserver vs1 -scanner
-pool SP
Vserver: vs1
                                Scanner Pool: SP
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2
 List of Host Names of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2
```

vserver vscan scanner-pool servers show

Display list of servers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver vscan scanner-pool servers show` command displays the list of servers of the Vscan scanner pools belonging to the Vserver. If you do not specify any parameters, the command displays the following information about all scanner pools:

- Vserver name
- Scanner pool
- List of servers

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the scanner pools for the specified Vserver.

[-scanner-pool <Scanner pool>] - Scanner Pool

If you specify this parameter, the command displays information only for the specified scanner pool.

[-servers <IP Address>,…] - List of IPs of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the scanner pools that have the specified IP address or IP addresses.

[-hostnames <text>,…] - List of Host Names of Allowed Vscan Servers

If you specify this parameter, the command displays information only about the scanner pools that have the specified host name or host names.

Examples

The following example displays the list of servers of all scanner pools.

```
cluster1::> vserver vscan scanner-pool servers show
Vserver         Scanner Pool      Servers
--------------- -----------------
-----------------------------------------
vs1             SP                1.1.1.1, 10.72.204.27
vs2             p1                10.72.204.29
6 entries were displayed.
```

The following example displays the list of servers and host names of all scanner pools.

```
cluster1::> vserver vscan scanner-pool servers show -instance
Vserver: vs1
                              Scanner Pool: SP
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-27.fsct.nb
Vserver: vs2
                              Scanner Pool: p1
       List of IPs of Allowed Vscan Servers: 10.72.204.29
List of Host Names of Allowed Vscan Servers: vmwin204-29.fsct.nb
2 entries were displayed.
```

Copyright information

Copyright © 2026 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.