

NGS NPI/Data ONTAP/8.2.1 TOI/OB AV

NetApp Confidential

< NGS NPI | Data ONTAP | 8.2.1 TOI

TOI for Offboard Anti Virus for ONTAP 8.2.1

After completing this TOI, please take the time to help us evaluate its effectiveness. When ready, please go to the TOI Survey section and complete a short survey. Thank You!

Contents

- 1 General Instructions
- 2 Release Name
- 3 Overview
 - 3.1 Links
 - 3.2 Supported vendors
 - 3.3 ONTAP Configuration
 - 3.3.1 CLI
 - 3.3.1.1 vscan
 - 3.3.1.1.1 Syntax
 - 3.3.1.1.2 Examples
 - 3.3.1.2 vscan on-access-policy
 - 3.3.1.2.1 Syntax
 - 3.3.1.2.2 Examples
 - 3.3.1.3 vscan scanner-pool
 - 3.3.1.3.1 Syntax
 - 3.3.1.3.2 Examples
 - 3.3.1.4 vscan scanner-pool privileged-users
 - 3.3.1.4.1 Syntax
 - 3.3.1.4.2 Examples
 - 3.3.1.5 vscan scanner-pool servers
 - 3.3.1.5.1 Syntax
 - 3.3.1.5.2 Examples
 - 3.3.1.6 vscan connection-status
 - 3.3.1.6.1 Syntax
 - 3.3.1.6.2 Examples
 - 3.3.1.7 cifs share
 - 3.3.1.7.1 Syntax
 - 3.3.1.7.2 Examples
 - 3.3.2 ONTAPI
 - 3.4 AV Connector Configuration
 - 3.5 AV Connector FAQ
- 4 Theory of Operation
 - 4.1 Architectural Design
 - 4.2 Basic request/response flow
- 5 Hardware and Software Requirements
- 6 Licenses
- 7 Upgrade and Revert
- 8 Performance
- 9 Troubleshooting
 - 9.1 Common Problems
 - 9.2 How to isolate problem between AVSHIM and AV software
 - 9.3 Mhost Logging
 - 9.4 Avshim Logging
 - 9.5 Triage and Data Collection
 - 9.6 Tracing
 - 9.7 Diagnostics Tools
 - 9.8 Error Messages
 - 9.9 AutoSupport & EMS Logging
 - 9.10 Known Problems
 - 9.11 Fixed Problems
 - 9.12 Limitations
 - 9.13 Knowledge Base Articles
 - 9.14 Test Plans and Results
- 10 Functional, Design and Architectural Specifications
- 11 Reference Material
- 12 Support and Escalation Information
- 13 Contact Information

General Instructions

Mohana and AV Dev team have viewed the Supportability Blueprint based the content it and feedback from AV SMEs in Support.

https://wikid.netapp.com/w/Supportability/Supportability_Blueprints/VirusScanner_blueprint

Release Name

- Official Name: Clustered Data ONTAP Antivirus Connector for ONTAP 8.2.1
- Internal Name: Offbox AV / offboard AV
- Release Designation: Major

top

top

Overview

C-Mode Offbox-Vscan feature provides anti-virus scanning support to clustered ONTAP, wherein the virus-scanning is performed by non-ONTAP machines hosting virus-scanners from various vendors. This feature fills the gap which surfaced when Onboard AV solution was disabled. The feature is similar to 7-Mode vscan feature (http://web.netapp.com/engineering/projects/conga/virusscan_dl.html) .

Offbox-Vscan feature provides virus-scanning support by triggering in-band notifications to external vscan servers on various file-operations like open, close, rename; applicable as per the fileop profile configuration. Due to in-band nature of these notifications, the said file-operation will be suspended till the scan-status is reported back by the external vscan server. The vscan servers, on receiving these notification, will read the file under question over a privileged CIFS share, scan the file contents and may attempt to perform remedial operations on an infected file as per the configuration done on the vscan servers. After completing all necessary operations, vscan server will respond with the scan status to Offbox-Vscan module, which will allow or deny the suspended file operation, if the file is found clean or infected, respectively. In SN.1, this feature supports vscan only for CIFS traffic. But in future we plan to support NFS as well. On-demand scans will also be supported to enable bulk scanning during off-peak hours.

Benefits over On-board AV solution:

- Scalable — An arbitrary number of vscanners can serve an arbitrary number of vservers.
- Robust — Multiple vscanners provide redundancy.
- Flexible — Different vendors can be used on the same cluster, and if desired, a pool of vscanners can provide scanning for one or more entire clusters.
- Reduced resource footprint - Provides high performance with greatly reduced impact to ONTAP resources. It has almost zero M-host memory footprint and CPU requirements.
- It provides 100% compatibility for our AV vendor partners, trivially allowing them to provide the latest versions of vscan engines and update mechanisms for their software.
- It decouples AV vendor partners' development schedules from those of NetApp.

This feature also improve on the following areas as compared to 7-mode vscan feature:

- Manageability - The configuration is deigned is such a way that storage admins get better control over the feature. They also get much more information on the state of this solution.
- Security enhancements - ONTAP validates any incoming connection against the configuration to make sure that only valid scanners can connect. Also we no longer require the vscanner to open up a named pipe for anonymous access.
- Rolling update support for the AV scan engines - ONTAP maintains the version of the vscanner along with the scan-status of the file. This means that version update of one vscanner (out of a pool) does not require discarding scan-status of all scanned files.
- Feature improvements - Path and size based scan exclusion.

Links

- Off-box AV ERRD
- clustered ONTAP Off-box AV Architecture Specification
- clustered ONTAP Off-box AV Functional Specification
- clustered ONTAP off-box "avshim" Functional Specification
- Vscan named pipe notification wire protocol

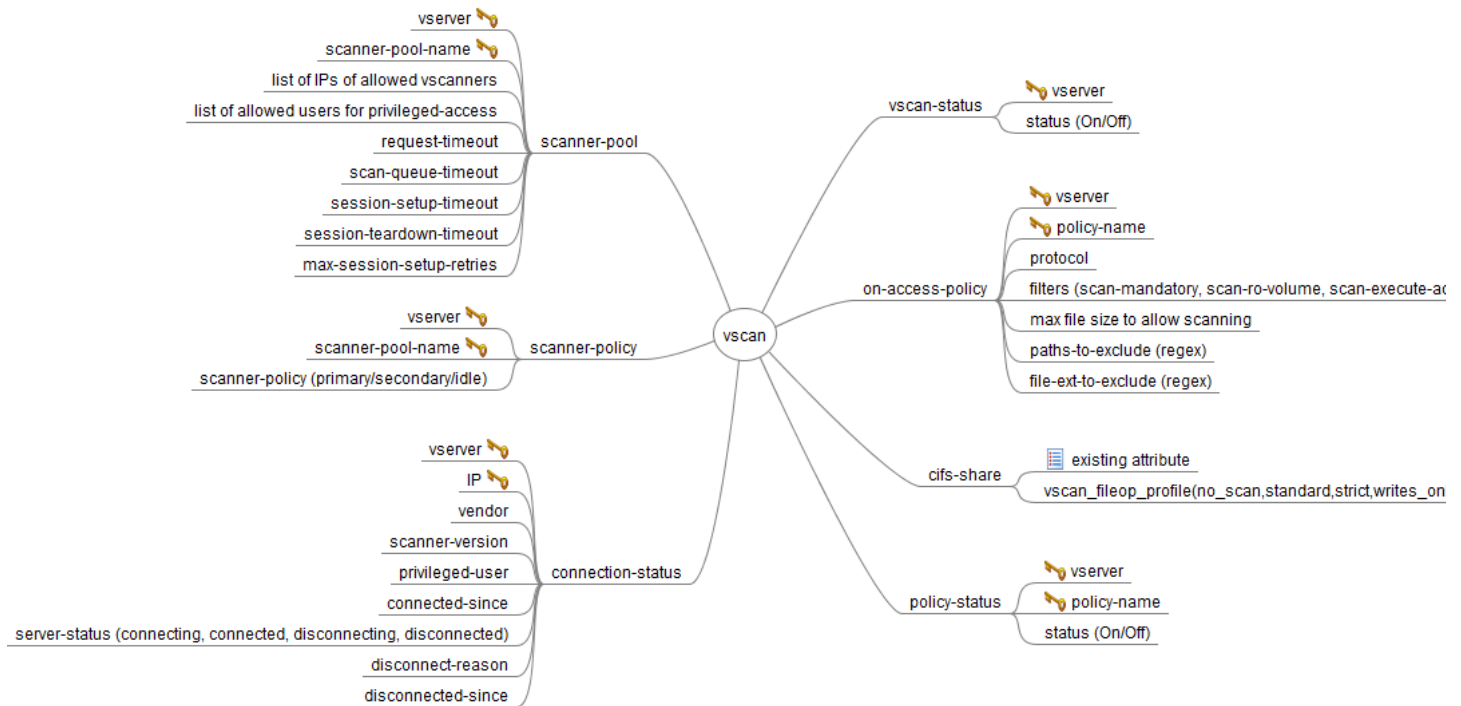
Supported vendors

Following vendors support their product for the clustered Data ONTAP 8.2.1:

- McAfee: VirusScan Enterprise for Storage - VSE-S 1.1.0
- TrendMicro:ServerProtect for Network Appliance filers 5.8 Service Pack 1 (SPNAF 5.8 SP1) (http://ngs-web.corp.netapp.com/service_readiness/product_ready/npi_toi/software/data_ontap/8/8.2.1/AntiVirus/SPNAF%20SP1%20Beta%20traning.pptx)
- Symantec:Symantec Protection Engine for Network Attached Storage (SPE for NAS), Version: 7.5 (support moved to March 2014)

ONTAP Configuration

- If the new feature is a command, provide the following: 1) command syntax 2) examples 3) command output



There are 2 major configuration-elements for Offbox-Vscan feature, namely On-Access policies and Scanner pools.

- On-Access Policies: This configuration defines the scope of On-Access scanning on file-objects. The scope parameter may be different for different Protocols. So, this is again categorized based on the Protocol. For SN.1, only CIFS is to be supported. The basic scoping parameters for CIFS are file-path, file-extension and max-file size. Apart from these, filters are also included that may be used to define the scope more precisely.
- Scanner pools: This configuration allows the administrator to provide the set of objects which are used for validating the vscanner connection (like allowed list of vscanner IPs, allowed list of authentication-parameters etc...) and other parameters like various timeouts for scan-notifications, responses (available in advanced mode).

Apart from that vscan-fileop profile is maintained per share basis (to provide more granular control compared to on-access policy) on what fileops are scanned.

All the configuration-elements are vserverized, i.e. to create a configuration-entry, a vserver must be specified. Configuration may be created with Cluster-Server-ID (CSID) as the vserver. Such configuration-entries will be available for all vservers. However, to activate such configuration for a vserver, specific action will be required, where the vserver-to-apply-to must be specified.

Following are the steps needed to enable virus-scanning on a vserver:

- Ensure that vserver-of-interest has LIFs on atleast one clustered ONTAP node, and that vscanners are accessible for this/these LIF(s).
- Provide a Scanner pool configuration, mentioning:
 - list of vscanners IPs
 - list of privileged-users, using which the virus-scan-engine accesses the files to be scanned
 - scan-request and connection-setup related parameters (timeouts and retry counts)
- Apply appropriate scanner policy to scanner pools for a vserver.
- Check the connection-status user-interface and ensure that vscanners are successfully connected to clustered ONTAP node(s).
- Create an On-Access policy for the vserver to specify an appropriate scope (file-paths and file-extensions to exclude) of files that need to be scanned.
- Enable the policy.
- Enable vscan for the vserver-of-interest.

CLI

All Vscan commands are rooted to the vserver directory.

The commands are grouped in the following sub-directories:

- vserver vscan : top level Vscan directory; enable/disable the feature for a vserver
- vserver vscan on-access-policy : Manage Vscan on-access-policies
- vserver vscan scanner-pool : Manage Vscan scanner pool
- vserver vscan scanner-pool privileged-users : Manage list of privileged-users of a scanner pool
- vserver vscan scanner-pool servers : Manage list of servers of a scanner pool
- vserver vscan connection-status : Display connection-status of external vscanners

Other than these, a new attribute "vscan-fileop-profile" is added to the vserver cifs share.

vscan

Syntax

```

jrajesh-SN-2::> vscan ?
(vserver vscan)
connection-status>      Display connection status of Vscan servers
disable                 Disable Vscan on a Vserver
enable                 Enable Vscan on a Vserver
on-access-policy>       Manage Vscan On-Access policies
reset                  Discard cached scan information
  
```

```

scanner-pool>          Manage Vscan scanner pools
show                   Display Vscan status

jrajesh-SN-2::> vscan enable ?
(vserver vscan enable)
[-vserver] <vserver name>  Vserver

jrajesh-SN-2::> vscan disable ?
(vserver vscan disable)
[-vserver] <vserver name>  Vserver

jrajesh-SN-2::> vscan reset ?
(vserver vscan reset)
[-vserver] <vserver name>  Vserver

jrajesh-SN-2::> vscan show ?
(vserver vscan show)
[ -instance | -fields <fieldname>, ... ]
[[-vserver] <vserver name>]  Vserver
[ -vscan-status {on|off} ]  Vscan Status

jrajesh-SN-2::> vscan show -instance ?
(vserver vscan show)
[[-vserver] <vserver name>]  Vserver
[ -vscan-status {on|off} ]  Vscan Status

```

Examples

```

jrajesh-SN-2::> vscan enable -vserver vserver_2
(vserver vscan enable)

jrajesh-SN-2::> vscan show
(vserver vscan show)
Vserver          Vscan Status
-----
vserver_1        on
vserver_2        on
2 entries were displayed.

jrajesh-SN-2::>
jrajesh-SN-2::> vscan disable -vserver vserver_1
(vserver vscan disable)

jrajesh-SN-2::> vscan show
(vserver vscan show)
Vserver          Vscan Status
-----
vserver_1        off
vserver_2        on
2 entries were displayed.

jrajesh-SN-2::> vscan reset -vserver vserver_1
(vserver vscan reset)

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

```

vscan on-access-policy

Syntax

```

jrajesh-SN-2::> vscan on-access-policy ?
(vserver vscan on-access-policy)
create          Create an On-Access policy
delete          Delete an On-Access policy
disable         Disable an On-Access policy
enable          Enable an On-Access policy
modify          Modify an On-Access policy
show            Display On-Access policies

jrajesh-SN-2::> vscan on-access-policy create ?
(vserver vscan on-access-policy create)
-vserver <vserver name>          Vserver
[-policy-name] <policy name>    Policy
[[-protocol] <CIFS>]            File-Access Protocol (default: CIFS)
[[-filters] {scan-mandatory|scan-ro-volume|scan-execute-access}, ...] Filters (default: scan-mandatory)
[ -max-file-size {<integer>[KB|MB|GB|TB|PB]} ] Max File Size Allowed for Scanning (default: 2GB)
[ -paths-to-exclude <file path>, ... ] File-Paths Not to Scan
[ -file-ext-to-exclude <file extension>, ... ] File-Extensions Not to Scan

jrajesh-SN-2::> vscan on-access-policy modify ?
(vserver vscan on-access-policy modify)
-vserver <vserver name>          Vserver
[-policy-name] <policy name>    Policy
[[-filters] {scan-mandatory|scan-ro-volume|scan-execute-access}, ... ] Filters
[ -max-file-size {<integer>[KB|MB|GB|TB|PB]} ] Max File Size Allowed for Scanning
[ -paths-to-exclude <file path>, ... ] File-Paths Not to Scan
[ -file-ext-to-exclude <file extension>, ... ] File-Extensions Not to Scan

jrajesh-SN-2::> vscan on-access-policy show ?
(vserver vscan on-access-policy show)
[ -instance | -fields <fieldname>, ... ]
[ -vserver <vserver name> ]          Vserver
[[-policy-name] <policy name>]      Policy
[ -policy-status {on|off} ]         Policy Status
[ -owner <Configuration owner> ]    Policy Config Owner
[ -protocol <CIFS> ]                File-Access Protocol
[[-filters] {scan-mandatory|scan-ro-volume|scan-execute-access}, ... ] Filters
[ -max-file-size {<integer>[KB|MB|GB|TB|PB]} ] Max File Size Allowed for Scanning
[ -paths-to-exclude <file path>, ... ] File-Paths Not to Scan
[ -file-ext-to-exclude <file extension>, ... ] File-Extensions Not to Scan

jrajesh-SN-2::> vscan on-access-policy delete ?

```

```
(vserver vscan on-access-policy delete)
-vserver <vserver name>      Vserver
[-policy-name] <policy name> Policy

jrajesh-SN-2::> vscan on-access-policy enable ?
(vserver vscan on-access-policy enable)
-vserver <vserver name>      Vserver
[-policy-name] <policy name> Policy

jrajesh-SN-2::> vscan on-access-policy disable ?
(vserver vscan on-access-policy disable)
-vserver <vserver name>      Vserver
[-policy-name] <policy name> Policy
```

Examples

```
jrajesh-SN-2::vserver vscan on-access-policy> show
Policy
Vserver   Name      Owner      Protocol Paths Excluded  File-Ext  Policy
-----
jrajesh-SN-2      default_ cluster  CIFS      -          -          off
CIFS
vserver_1 default_ cluster  CIFS      -          -          off
CIFS
vserver_1 new       vserver  CIFS      \|vol1\tmp\, mp3        off
\vol2\abc
vserver_2 default_ cluster  CIFS      -          -          off
CIFS
4 entries were displayed.

jrajesh-SN-2::vserver vscan on-access-policy> create -vserver vserver_1 -policy-name test -protocol CIFS -filters scan-execute-access
-paths-to-exclude \|vol2\ -file-ext-to-exclude txt -max-file-size 10GB

jrajesh-SN-2::vserver vscan on-access-policy> show -instance -vserver vserver_1 -policy-name test

          Vserver: vserver_1
          Policy: test
          Policy Status: off
          Policy Config Owner: vserver
          File-Access Protocol: CIFS
          Filters: scan-execute-access
Max File Size Allowed for Scanning: 10GB
File-Paths Not to Scan: \|vol2\
File-Extensions Not to Scan: txt

jrajesh-SN-2::vserver vscan on-access-policy> modify -vserver vserver_1 -policy-name test -filters scan-ro-volume -paths-to-exclude ""
-file-ext-to-exclude mp*

jrajesh-SN-2::vserver vscan on-access-policy> show -instance -vserver vserver_1 -policy-name test

          Vserver: vserver_1
          Policy: test
          Policy Status: off
          Policy Config Owner: vserver
          File-Access Protocol: CIFS
          Filters: scan-ro-volume
Max File Size Allowed for Scanning: 10GB
File-Paths Not to Scan: -
File-Extensions Not to Scan: mp*

jrajesh-SN-2::vserver vscan on-access-policy> enable -vserver vserver_1 -policy-name test

jrajesh-SN-2::vserver vscan on-access-policy> show -instance -vserver vserver_1 -policy-name test

          Vserver: vserver_1
          Policy: test
          Policy Status: on
          Policy Config Owner: vserver
          File-Access Protocol: CIFS
          Filters: scan-ro-volume
Max File Size Allowed for Scanning: 10GB
File-Paths Not to Scan: -
File-Extensions Not to Scan: mp*

jrajesh-SN-2::vserver vscan on-access-policy> enable -vserver vserver_1 -policy-name new

Error: command failed: Cannot enable policy. Reason: Another policy ("test") for the "CIFS" protocol is currently enabled.
Disable the policy and try the command again.

jrajesh-SN-2::vserver vscan on-access-policy> disable -vserver vserver_1 -policy-name test

jrajesh-SN-2::vserver vscan on-access-policy> show -instance -vserver vserver_1 -policy-name test

          Vserver: vserver_1
          Policy: test
          Policy Status: off
          Policy Config Owner: vserver
          File-Access Protocol: CIFS
          Filters: scan-ro-volume
Max File Size Allowed for Scanning: 10GB
File-Paths Not to Scan: -
File-Extensions Not to Scan: mp*

jrajesh-SN-2::vserver vscan on-access-policy> delete -vserver vserver_1 -policy-name test
```

vscan scanner-pool

Syntax

```
jrajesh-SN-2::> vscan scanner-pool ?
(vserver vscan scanner-pool)
apply-policy          Apply scanner-policy to a scanner pool
```

```
create          Create a scanner pool
delete          Delete a scanner pool
modify          Modify a scanner pool
privileged-users> Manage list of privileged users of a scanner pool
servers>        Manage list of servers of a scanner pool
show            Display scanner pools
show-active     Display active scanner pools
```

```
rajesh-SN-2::> vscan scanner-pool create ?
(vserver vscan scanner-pool create)
  -vserver <vserver name>          Vserver
  [-scanner-pool] <scanner pool>   Scanner Pool
  [-servers] <IpAddress>, ...      List of IPs of Allowed Vscan Servers
  [-privileged-users] <Privileged user>, ... List of Privileged Users
```

```
rajesh-SN-2::> vscan scanner-pool modify ?
(vserver vscan scanner-pool modify)
  -vserver <vserver name>          Vserver
  [-scanner-pool] <scanner pool>   Scanner Pool
  [-servers <IpAddress>, ... ]     List of IPs of Allowed Vscan Servers
  [-privileged-users <Privileged user>, ... ] List of Privileged Users
```

```
rajesh-SN-2::> vscan scanner-pool delete ?
(vserver vscan scanner-pool delete)
  -vserver <vserver name>          Vserver
  [-scanner-pool] <scanner pool>   Scanner Pool
```

```
rajesh-SN-2::> vscan scanner-pool en
```

Error: "en" is not a recognized command

```
rajesh-SN-2::> vscan scanner-pool apply-policy ?
(vserver vscan scanner-pool apply-policy)
  -vserver <vserver name>          Vserver
  [-scanner-pool] <scanner pool>   Scanner Pool
  [-scanner-policy] <vscan scanner policy> Scanner Policy
```

```
rajesh-SN-2::> vscan scanner-pool show ?
(vserver vscan scanner-pool show)
  [-instance | -fields <fieldname>, ... ]
  [-vserver <vserver name> ]          Vserver
  [[-scanner-pool] <scanner pool>]    Scanner Pool
  [-scanner-policy <vscan scanner policy> ] Applied Policy
  [-current-status {on|off} ]          Current Status
  [-owner <Configuration owner> ]      Scanner Pool Config Owner
  [-servers <IpAddress>, ... ]          List of IPs of Allowed Vscan Servers
  [-privileged-users <Privileged user>, ... ] List of Privileged Users
```

```
rajesh-SN-2::> vscan scanner-pool show -instance ?
(vserver vscan scanner-pool show)
  [-vserver <vserver name> ]          Vserver
  [[-scanner-pool] <scanner pool>]    Scanner Pool
  [-scanner-policy <vscan scanner policy> ] Applied Policy
  [-current-status {on|off} ]          Current Status
  [-owner <Configuration owner> ]      Scanner Pool Config Owner
  [-servers <IpAddress>, ... ]          List of IPs of Allowed Vscan Servers
  [-privileged-users <Privileged user>, ... ] List of Privileged Users
```

```
rajesh-SN-2::> vscan scanner-pool show-active ?
(vserver vscan scanner-pool show-active)
  [-instance | -fields <fieldname>, ... ]
  [[-vserver] <vserver name>]          Vserver
  [-scanner-pools <scanner pool>, ... ] List of Enabled Scanner Pools
  [-servers <IpAddress>, ... ]          Merged List of IPs of Allowed Vscan Servers
  [-privileged-users <Privileged user>, ... ] Merged List of Privileged Users
```

```
rajesh-SN-2::> vscan scanner-pool show-active -instance ?
(vserver vscan scanner-pool show-active)
  [[-vserver] <vserver name>]          Vserver
  [-scanner-pools <scanner pool>, ... ] List of Enabled Scanner Pools
  [-servers <IpAddress>, ... ]          Merged List of IPs of Allowed Vscan Servers
  [-privileged-users <Privileged user>, ... ] Merged List of Privileged Users
```

```
rajesh-SN-2::> set advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

```
rajesh-SN-2::*> vscan scanner-pool ?
(vserver vscan scanner-pool)
  apply-policy      Apply scanner-policy to a scanner pool
  create            Create a scanner pool
  delete            Delete a scanner pool
  modify            Modify a scanner pool
  privileged-users> Manage list of privileged users of a scanner pool
  servers>          Manage list of servers of a scanner pool
  show              Display scanner pools
  show-active       Display active scanner pools
```

```
rajesh-SN-2::*> vscan scanner-pool create ?
(vserver vscan scanner-pool create)
  -vserver <vserver name>          Vserver
  [-scanner-pool] <scanner pool>   Scanner Pool
  [-servers] <IpAddress>, ...      List of IPs of Allowed Vscan Servers
  [-privileged-users] <Privileged user>, ... List of Privileged Users
  [[-request-timeout] <[<integer>h][<integer>m][<integer>s]>] *Request Service Timeout (default: 30s)
  [-scan-queue-timeout <[<integer>h][<integer>m][<integer>s]> ] *Scan Queue Timeout (default: 20s)
  [-session-setup-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Setup Timeout (default: 10s)
  [-session-teardown-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Teardown Timeout (default: 10s)
  [-max-session-setup-retries <integer> ] *Max Number of Consecutive Session Setup Attempts (default: 5)
```

```
rajesh-SN-2::*> vscan scanner-pool modify ?
(vserver vscan scanner-pool modify)
  -vserver <vserver name>          Vserver
  [-scanner-pool] <scanner pool>   Scanner Pool
  [-servers <IpAddress>, ... ]     List of IPs of Allowed Vscan Servers
  [-privileged-users <Privileged user>, ... ] List of Privileged Users
  [-request-timeout <[<integer>h][<integer>m][<integer>s]> ] *Request Service Timeout
  [-scan-queue-timeout <[<integer>h][<integer>m][<integer>s]> ] *Scan Queue Timeout
  [-session-setup-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Setup Timeout
  [-session-teardown-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Teardown Timeout
```

```

[ -max-session-setup-retries <integer> ] *Max Number of Consecutive Session Setup Attempts

rajesh-SN-2::*> vscan scanner-pool delete ?
(vserver vscan scanner-pool delete)
-vserver <vserver name> Vserver
[-scanner-pool] <scanner pool> Scanner Pool

rajesh-SN-2::*> vscan scanner-pool show ?
(vserver vscan scanner-pool show)
[ -instance | -fields <fieldname>, ... ]
[ -vserver <vserver name> ] Vserver
[[-scanner-pool] <scanner pool>] Scanner Pool
[ -scanner-policy <vscan scanner policy> ] Applied Policy
[ -current-status {on|off} ] Current Status
[ -owner <Configuration owner> ] Scanner Pool Config Owner
[ -servers <IPAddress>, ... ] List of IPs of Allowed Vscan Servers
[ -privileged-users <Privileged user>, ... ] List of Privileged Users
[ -request-timeout <[<integer>h][<integer>m][<integer>s]> ] *Request Service Timeout
[ -scan-queue-timeout <[<integer>h][<integer>m][<integer>s]> ] *Scan Queue Timeout
[ -session-setup-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Setup Timeout
[ -session-teardown-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Teardown Timeout
[ -max-session-setup-retries <integer> ] *Max Number of Consecutive Session Setup Attempts

rajesh-SN-2::*> vscan scanner-pool show -instance ?
(vserver vscan scanner-pool show)
[ -vserver <vserver name> ] Vserver
[[-scanner-pool] <scanner pool>] Scanner Pool
[ -scanner-policy <vscan scanner policy> ] Applied Policy
[ -current-status {on|off} ] Current Status
[ -owner <Configuration owner> ] Scanner Pool Config Owner
[ -servers <IPAddress>, ... ] List of IPs of Allowed Vscan Servers
[ -privileged-users <Privileged user>, ... ] List of Privileged Users
[ -request-timeout <[<integer>h][<integer>m][<integer>s]> ] *Request Service Timeout
[ -scan-queue-timeout <[<integer>h][<integer>m][<integer>s]> ] *Scan Queue Timeout
[ -session-setup-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Setup Timeout
[ -session-teardown-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Teardown Timeout
[ -max-session-setup-retries <integer> ] *Max Number of Consecutive Session Setup Attempts

rajesh-SN-2::*> vscan scanner-pool show-active ?
(vserver vscan scanner-pool show-active)
[ -instance | -fields <fieldname>, ... ]
[[-vserver] <vserver name>] Vserver
[ -scanner-pools <scanner pool>, ... ] List of Enabled Scanner Pools
[ -servers <IPAddress>, ... ] Merged List of Allowed Vscan Servers
[ -privileged-users <Privileged user>, ... ] Merged List of Privileged Users
[ -request-timeout <[<integer>h][<integer>m][<integer>s]> ] *Request Service Timeout
[ -scan-queue-timeout <[<integer>h][<integer>m][<integer>s]> ] *Scan Queue Timeout
[ -session-setup-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Setup Timeout
[ -session-teardown-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Teardown Timeout
[ -max-session-setup-retries <integer> ] *Max Number of Consecutive Session Setup Attempts

rajesh-SN-2::*> vscan scanner-pool show-active -instance ?
(vserver vscan scanner-pool show-active)
[[-vserver] <vserver name>] Vserver
[ -scanner-pools <scanner pool>, ... ] List of Enabled Scanner Pools
[ -servers <IPAddress>, ... ] Merged List of Allowed Vscan Servers
[ -privileged-users <Privileged user>, ... ] Merged List of Privileged Users
[ -request-timeout <[<integer>h][<integer>m][<integer>s]> ] *Request Service Timeout
[ -scan-queue-timeout <[<integer>h][<integer>m][<integer>s]> ] *Scan Queue Timeout
[ -session-setup-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Setup Timeout
[ -session-teardown-timeout <[<integer>h][<integer>m][<integer>s]> ] *Session Teardown Timeout
[ -max-session-setup-retries <integer> ] *Max Number of Consecutive Session Setup Attempts

```

Examples

```

rajesh-SN-2::vserver vscan scanner-pool> create -vserver jrajesh-SN-2 -scanner-pool test -servers 10.72.204.1 -privileged-users fsct\test

rajesh-SN-2::vserver vscan scanner-pool> show
Vserver      Scanner Pool      Owner      Servers      Privileged Users      Scanner Policy
-----
rajesh-SN-2      test      cluster 10.72.204.1      fsct\test      idle
vserver_1      new      vserver 10.72.204.27      fsct\administrator      idle
vserver_1      test      cluster 10.72.204.1      fsct\test      idle
vserver_2      test      cluster 10.72.204.1      fsct\test      idle
4 entries were displayed.

rajesh-SN-2::vserver vscan scanner-pool> modify -vserver vserver_1 -scanner-pool new -servers 10.72.204.29 -privileged-users fsct\administrator,fsct\jrajesh

rajesh-SN-2::vserver vscan scanner-pool> apply-policy -vserver vserver_1 -scanner-pool new -scanner-policy primary

rajesh-SN-2::vserver vscan scanner-pool> apply-policy -vserver vserver_1 -scanner-pool test -scanner-policy secondary

rajesh-SN-2::vserver vscan scanner-pool> apply-policy -vserver vserver_2 -scanner-pool test -scanner-policy primary

rajesh-SN-2::vserver vscan scanner-pool> show
Vserver      Scanner Pool      Owner      Servers      Privileged Users      Scanner Policy
-----
rajesh-SN-2      test      cluster 10.72.204.1      fsct\test      idle
vserver_1      new      vserver 10.72.204.29      fsct\administrator,fsct\jrajesh      primary
vserver_1      test      cluster 10.72.204.1      fsct\test      secondary
vserver_2      test      cluster 10.72.204.1      fsct\test      primary
4 entries were displayed.

rajesh-SN-2::vserver vscan scanner-pool> show-active
Vserver      Scanner Pools Servers      Privileged Users
-----
vserver_1      new      10.72.204.29      fsct\administrator,fsct\jrajesh

```

```

vserver_2 test 10.72.204.1 fsct\test
2 entries were displayed.

jrajesh-SN-2::vserver vscan scanner-pool> create -vserver jrajesh-SN-2 -scanner-pool test1 -servers 10.72.204.1 -privileged-users fsct\test

jrajesh-SN-2::vserver vscan scanner-pool> show

```

Vserver	Scanner Pool	Pool Owner	Servers	Privileged Users	Scanner Policy
jrajesh-SN-2	test	cluster	10.72.204.1	fsct\test	idle
jrajesh-SN-2	test1	cluster	10.72.204.1	fsct\test	idle
vserver_1	new	vserver	10.72.204.29	fsct\administrator, fsct\jrajesh	primary
vserver_1	test	cluster	10.72.204.1	fsct\test	secondary
vserver_1	test1	cluster	10.72.204.1	fsct\test	idle
vserver_2	test	cluster	10.72.204.1	fsct\test	primary
vserver_2	test1	cluster	10.72.204.1	fsct\test	idle

```

7 entries were displayed.

jrajesh-SN-2::vserver vscan scanner-pool> delete -vserver jrajesh-SN-2 -scanner-pool test1

jrajesh-SN-2::vserver vscan scanner-pool> set advanced

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

jrajesh-SN-2::vserver vscan scanner-pool*> show -instance -vserver vserver_1 -scanner-pool new

Vserver: vserver_1
Scanner Pool: new
Applied Policy: primary
Current Status: on
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 10.72.204.29, 1.1.1.1
List of Privileged Users: fsct\administrator, fsct\new
Request Service Timeout: 30s
Scan Queue Timeout: 20s
Session Setup Timeout: 10s
Session Teardown Timeout: 10s
Max Number of Consecutive Session Setup Attempts: 5

jrajesh-SN-2::vserver vscan scanner-pool*> modify -vserver vserver_1 -scanner-pool new -servers 10.72.204.29,1.1.1.1 -privileged-users fsct\administrator,fsct\new -request-timeout 20s -scan-queue-timeout 12s -session-setup-timeout 8s -session-teardown-timeout 9s -max-session-setup-retries 3

jrajesh-SN-2::vserver vscan scanner-pool*> show -instance -vserver vserver_1 -scanner-pool new

Vserver: vserver_1
Scanner Pool: new
Applied Policy: primary
Current Status: on
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 10.72.204.29, 1.1.1.1
List of Privileged Users: fsct\administrator, fsct\new
Request Service Timeout: 20s
Scan Queue Timeout: 12s
Session Setup Timeout: 8s
Session Teardown Timeout: 9s
Max Number of Consecutive Session Setup Attempts: 3

```

vscan scanner-pool privileged-users

Syntax

```

jrajesh-SN-2::> vscan scanner-pool privileged-users ?
(vserver vscan scanner-pool privileged-users)
add          Add to the list of privileged users
remove       Remove from the list of privileged users
show         Display list of privileged users

jrajesh-SN-2::> vscan scanner-pool privileged-users add ?
(vserver vscan scanner-pool privileged-users add)
-vserver <vserver name>      Vserver
[-scanner-pool] <scanner pool> Scanner Pool
[-privileged-users] <Privileged user>, ... List of Privileged Users

jrajesh-SN-2::> vscan scanner-pool privileged-users remove ?
(vserver vscan scanner-pool privileged-users remove)
-vserver <vserver name>      Vserver
[-scanner-pool] <scanner pool> Scanner Pool
[-privileged-users] <Privileged user>, ... List of Privileged Users

jrajesh-SN-2::> vscan scanner-pool privileged-users show ?
(vserver vscan scanner-pool privileged-users show)
[ -instance | -fields <fieldname>, ... ]
[ -vserver <vserver name> ]          Vserver
[[-scanner-pool] <scanner pool>]     Scanner Pool
[ -privileged-users <Privileged user>, ... ] List of Privileged Users

jrajesh-SN-2::> vscan scanner-pool privileged-users show -instance ?
(vserver vscan scanner-pool privileged-users show)
[ -vserver <vserver name> ]          Vserver
[[-scanner-pool] <scanner pool>]     Scanner Pool
[ -privileged-users <Privileged user>, ... ] List of Privileged Users

```

Examples

```

jrajesh-SN-2::vserver vscan scanner-pool privileged-users> add -vserver vserver_1 -scanner-pool new -privileged-users fsct\u1,fsct\u2

jrajesh-SN-2::vserver vscan scanner-pool privileged-users> show

```

```

Vserver          Scanner Pool      Privileged Users
-----
jrajesh-SN-2     test          fsct\test
vserver_1        new          fsct\administrator, fsct\new, fsct\ul,
                test          fsct\ul2
vserver_1        test          fsct\test
vserver_2        test          fsct\test
4 entries were displayed.

jrajesh-SN-2::vserver vscan scanner-pool privileged-users> remove -vserver vserver_1 -scanner-pool new -privileged-users fsct\new,fsct\ul

jrajesh-SN-2::vserver vscan scanner-pool privileged-users> show
Vserver          Scanner Pool      Privileged Users
-----
jrajesh-SN-2     test          fsct\test
vserver_1        new          fsct\administrator, fsct\ul2
vserver_1        test          fsct\test
vserver_2        test          fsct\test
4 entries were displayed.

```

vscan scanner-pool servers

Syntax

```

jrajesh-SN-2::> vscan scanner-pool servers ?
(vserver vscan scanner-pool servers)
add                Add to the list of servers
remove            Remove from the list of servers
show              Display list of servers

jrajesh-SN-2::> vscan scanner-pool servers add ?
(vserver vscan scanner-pool servers add)
-vserver <vserver name>      Vserver
[-scanner-pool] <scanner pool> Scanner Pool
[-servers] <IpAddress>, ...  List of IPs for Vscan Servers

jrajesh-SN-2::> vscan scanner-pool servers remove ?
(vserver vscan scanner-pool servers remove)
-vserver <vserver name>      Vserver
[-scanner-pool] <scanner pool> Scanner Pool
[-servers] <IpAddress>, ...  List of IPs for Vscan Servers

jrajesh-SN-2::> vscan scanner-pool servers show ?
(vserver vscan scanner-pool servers show)
[ -instance | -fields <fieldname>, ... ]
[ -vserver <vserver name> ]      Vserver
[[-scanner-pool] <scanner pool>] Scanner Pool
[ -servers <IpAddress>, ... ]    List of IPs of Allowed Vscan Servers

jrajesh-SN-2::> vscan scanner-pool servers show -instance ?
(vserver vscan scanner-pool servers show)
[ -vserver <vserver name> ]      Vserver
[[-scanner-pool] <scanner pool>] Scanner Pool
[ -servers <IpAddress>, ... ]    List of IPs of Allowed Vscan Servers

```

Examples

```

jrajesh-SN-2::vserver vscan scanner-pool servers> add -vserver vserver_1 -scanner-pool new 2.2.2.2,3.3.3.3

jrajesh-SN-2::vserver vscan scanner-pool servers> show
Vserver          Scanner Pool      Servers
-----
jrajesh-SN-2     test          10.72.204.1
vserver_1        new          1.1.1.1, 2.2.2.2, 3.3.3.3, 10.72.204.29
vserver_1        test          10.72.204.1
vserver_2        test          10.72.204.1
4 entries were displayed.

jrajesh-SN-2::vserver vscan scanner-pool servers> remove -vserver vserver_1 -scanner-pool new 2.2.2.2,3.3.3.3,1.1.1.1

jrajesh-SN-2::vserver vscan scanner-pool servers> show -instance

                Vserver: jrajesh-SN-2
                Scanner Pool: test
List of IPs of Allowed Vscan Servers: 10.72.204.1

                Vserver: vserver_1
                Scanner Pool: new
List of IPs of Allowed Vscan Servers: 10.72.204.29

                Vserver: vserver_1
                Scanner Pool: test
List of IPs of Allowed Vscan Servers: 10.72.204.1

                Vserver: vserver_2
                Scanner Pool: test
List of IPs of Allowed Vscan Servers: 10.72.204.1
4 entries were displayed.

```

vscan connection-status

Syntax

```

jrajesh-SN-2::> vscan connection-status ?
(vserver vscan connection-status)
show              Display Vscan servers connection status summary
show-all         Display Vscan servers connection status
show-connected    Display connection status of connected Vscan servers
show-not-connected Display connection status of Vscan servers which are allowed to connect but not yet connected

```

```
rajesh-SN-2::> vscan connection-status show ?
(vserver vscan connection-status show)
[ -instance | -fields <fieldname>, ... ]
[[[-node] <nodename>]                Node
[ -vserver <vserver name> ]          Vserver
[ -servers <IpAddress>, ... ]       List of Connected Vscan Servers
[ -connection-count <integer> ]     Number of Connected Vscan Servers Serving the Vserver
```

```
rajesh-SN-2::> vscan connection-status show -instance ?
(vserver vscan connection-status show)
[[[-node] <nodename>]                Node
[ -vserver <vserver name> ]          Vserver
[ -servers <IpAddress>, ... ]       List of Connected Vscan Servers
[ -connection-count <integer> ]     Number of Connected Vscan Servers Serving the Vserver
```

```
rajesh-SN-2::> vscan connection-status show-connected ?
(vserver vscan connection-status show-connected)
[ -instance | -fields <fieldname>, ... ]
[[[-node] <nodename>]                Node
[ -vserver <vserver name> ]          Vserver
[[[-server] <IpAddress>]            Server
[ -vendor <text> ]                  Vscan Server Vendor
[ -version <text> ]                 Vscan Server Version
[ -privileged-user <text> ]         Privileged User Used for Connection
[ -connected-since <"MM/DD/YYYY HH:MM:SS"> ] Time When Vscan Server Was Connected
[ -server-type <Type> ]            Server Type
```

```
rajesh-SN-2::> vscan connection-status show-connected -instance ?
(vserver vscan connection-status show-connected)
[[[-node] <nodename>]                Node
[ -vserver <vserver name> ]          Vserver
[[[-server] <IpAddress>]            Server
[ -vendor <text> ]                  Vscan Server Vendor
[ -version <text> ]                 Vscan Server Version
[ -privileged-user <text> ]         Privileged User Used for Connection
[ -connected-since <"MM/DD/YYYY HH:MM:SS"> ] Time When Vscan Server Was Connected
[ -server-type <Type> ]            Server Type
```

```
rajesh-SN-2::> vscan connection-status show-not-connected ?
(vserver vscan connection-status show-not-connected)
[ -instance | -fields <fieldname>, ... ]
[[[-node] <nodename>]                Node
[ -vserver <vserver name> ]          Vserver
[[[-server] <IpAddress>]            Server
[ -server-status <Status> ]         Server Status
[ -disconnect-reason <reason> ]     Server Disconnect Reason
[ -disconnected-since <"MM/DD/YYYY HH:MM:SS"> ] Time When Vscan Server Was Disconnected
[ -server-type <Type> ]            Server Type
```

```
rajesh-SN-2::> vscan connection-status show-not-connected -instance ?
(vserver vscan connection-status show-not-connected)
[[[-node] <nodename>]                Node
[ -vserver <vserver name> ]          Vserver
[[[-server] <IpAddress>]            Server
[ -server-status <Status> ]         Server Status
[ -disconnect-reason <reason> ]     Server Disconnect Reason
[ -disconnected-since <"MM/DD/YYYY HH:MM:SS"> ] Time When Vscan Server Was Disconnected
[ -server-type <Type> ]            Server Type
```

```
rajesh-SN-2::> vscan connection-status show-all ?
(vserver vscan connection-status show-all)
[ -instance | -fields <fieldname>, ... ]
[[[-node] <nodename>]                Node
[ -vserver <vserver name> ]          Vserver
[[[-server] <IpAddress>]            Server
[ -server-status <Status> ]         Server Status
[ -server-type <Type> ]            Server Type
[ -vendor <text> ]                  Vscanner Vendor
[ -version <text> ]                 Vscanner Version
[ -disconnect-reason <reason> ]     Server Disconnect Reason
[ -disconnected-since <"MM/DD/YYYY HH:MM:SS"> ] Time When Vscanner Was Disconnected
[ -privileged-user <text> ]         Privileged User Used for Connection
[ -connected-since <"MM/DD/YYYY HH:MM:SS"> ] Time When Vscanner Was Connected
```

```
rajesh-SN-2::> vscan connection-status show-all -instance ?
(vserver vscan connection-status show-all)
[[[-node] <nodename>]                Node
[ -vserver <vserver name> ]          Vserver
[[[-server] <IpAddress>]            Server
[ -server-status <Status> ]         Server Status
[ -server-type <Type> ]            Server Type
[ -vendor <text> ]                  Vscanner Vendor
[ -version <text> ]                 Vscanner Version
[ -disconnect-reason <reason> ]     Server Disconnect Reason
[ -disconnected-since <"MM/DD/YYYY HH:MM:SS"> ] Time When Vscanner Was Disconnected
[ -privileged-user <text> ]         Privileged User Used for Connection
[ -connected-since <"MM/DD/YYYY HH:MM:SS"> ] Time When Vscanner Was Connected
```

```
rajesh-SN-2::> set diag
```

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

```
rajesh-SN-2::*> vscan connection-status ?
(vserver vscan connection-status)
show                Display Vscan servers connection status summary
show-all           Display Vscan servers connection status
show-connected      Display connection status of connected Vscan servers
show-extended-stats *Display Vscan servers' extended statistics
show-not-connected  Display connection status of Vscan servers which are allowed to connect but not yet connected
```

```
rajesh-SN-2::*> vscan connection-status show-extended-stats ?
(vserver vscan connection-status show-extended-stats)
[ -instance | -fields <fieldname>, ... ]
[[[-node] <nodename>]                *Node
[ -vserver <vserver name> ]          *Vserver
[[[-server] <IpAddress>]            *Server
[ -server-status <Status> ]         *Server Status
[ -server-type <Server type> ]      *Server Type
[ -vendor <text> ]                  *Vscanner Vendor
```

Examples

```
rajesh-SN-2::vserver vscan connection-status> show-not-connected -instance
```

Server: 1.1.1.1
Server Status: disconnected
Server Disconnect Reason: manual-disconnect
Time When Vscanner Was Disconnected: 3/12/2013 05:09:11

Node: jrajesh-SN-2-01
Vserver: vserver_2
Server: 10.12.2.2
Server Status: disconnected
Server Disconnect Reason: manual-disconnect
Time When Vscanner Was Disconnected: 3/14/2013 05:09:11
2 entries were displayed.

jrajesh-SN-2::vserver vscan connection-status> show-all

Vserver	Node	Server	Connection Status	Disconnect Reason
vserver_1	jrajesh-SN-2-01	1.1.1.1	disconnected	manual-disconnect
vserver_1	jrajesh-SN-2-01	2.2.2.2	connected	-
vserver_1	jrajesh-SN-2-01	3.3.3.3	connected	-
vserver_2	jrajesh-SN-2-01	3.4.2.3	connected	-
vserver_2	jrajesh-SN-2-01	10.12.2.2	disconnected	manual-disconnect
vserver_2	jrajesh-SN-2-01	10.72.204.1	connected	-
vserver_2	jrajesh-SN-2-01	10.72.238.1	connected	-

7 entries were displayed.

jrajesh-SN-2::vserver vscan connection-status> show-all -instance

Node: jrajesh-SN-2-01
Vserver: vserver_1
Server: 1.1.1.1
Server Status: disconnected
Vscanner Vendor: vendor
Vscanner Version: 1234
Server Disconnect Reason: manual-disconnect
Time When Server Was Disconnected: 3/12/2013 05:09:11

Node: jrajesh-SN-2-01
Vserver: vserver_1
Server: 2.2.2.2
Server Status: connected
Vscanner Vendor: McAfee
Vscanner Version: 1.2.22.1
Server Disconnect Reason: -
Time When Server Was Disconnected: -

Node: jrajesh-SN-2-01
Vserver: vserver_1
Server: 3.3.3.3
Server Status: connected
Vscanner Vendor: McAfee
Vscanner Version: 1.2.22.1
Server Disconnect Reason: -
Time When Server Was Disconnected: -

Node: jrajesh-SN-2-01
Vserver: vserver_2
Server: 3.4.2.3
Server Status: connected
Vscanner Vendor: Symantec
Vscanner Version: 5.1.43
Server Disconnect Reason: -
Time When Server Was Disconnected: -

Node: jrajesh-SN-2-01
Vserver: vserver_2
Server: 10.12.2.2
Server Status: disconnected
Vscanner Vendor: vendor
Vscanner Version: 1234
Server Disconnect Reason: manual-disconnect
Time When Server Was Disconnected: 3/14/2013 05:09:11

Node: jrajesh-SN-2-01
Vserver: vserver_2
Server: 10.72.204.1
Server Status: connected
Vscanner Vendor: Symantec
Vscanner Version: 5.1.43
Server Disconnect Reason: -
Time When Server Was Disconnected: -

Node: jrajesh-SN-2-01
Vserver: vserver_2
Server: 10.72.238.1
Server Status: connected
Vscanner Vendor: Symantec
Vscanner Version: 5.1.43
Server Disconnect Reason: -
Time When Server Was Disconnected: -
7 entries were displayed.

jrajesh-SN-2::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

jrajesh-SN-2::vserver vscan connection-status*> show-extended-stats -vserver vserver_1 -server 2.2.2.2

Vserver	Node	Server	Connection Status	Extended Stats
vserver_1	jrajesh-SN-2-01	2.2.2.2	connected	ts=3:37:36 AM Aug 13, 2013 scans=sent:6534,compok:6534,comperr:0,compnotfnd:0,ms/comp:7 mempage/s=29, procs=58, threads=741, %cpu=13.95, procqlen=0, diskio/s=0, smbbytes/s=0, ifmac=00:14:5E:16:35:7E, tcpstat=retrans:683,connfail:293,connreset:4785,inerr:0 cfg=Host Name:WIN209-199 OS Name:Microsoft Windows Server 2008 R2 Standard OS Version:6.1.7600 N/A Build 7600 System Boot Time:8/8/2013, 9:44:56 PM System Manufacturer:IBM System Model:IBM System x3550 -[797842A]-

```
System Type:x64-based PC
Processor(s):2 Processor(s) Installed.
[01]:Intel64 Family 6 Model 15 Stepping 6 GenuineIntel ~2000 Mhz
```

cifs share

Syntax

```
rajesh-SN-2::> cifs share create ?
-vserver <vserver name>                                Vserver
[-share-name] <Share>                                   Share
[-path] <text (size 1..256)>                             Path
[[-share-properties] <share properties>, ...]          Share Properties (default: oplocks,browsable,changenotify)
[-symlink-properties {enable|hide|read_only}, ...]      Symlink Properties (default: enable)
[-file-umask <Octal Permission> ]                     File Mode Creation Mask
[-dir-umask <Octal Permission> ]                       Directory Mode Creation Mask
[-comment <text (size 1..256)> ]                         Share Comment
[-attribute-cache-ttl <[<integer>h][<integer>m][<integer>s]> ] File Attribute Cache Lifetime
[-offline-files {none|manual|documents|programs} ]      Offline Files (default: manual)
[ -vscan-fileop-profile {no_scan|standard|strict|writes_only} ] Vscan File-Operations Profile (default: standard)

rajesh-SN-2::> cifs share modify ?
-vserver <vserver name>                                Vserver
[-share-name] <Share>                                   Share
[-path <text (size 1..256)> ]                             Path
[-symlink-properties {enable|hide|read_only}, ...]      Symlink Properties
[-file-umask <Octal Permission> ]                     File Mode Creation Mask
[-dir-umask <Octal Permission> ]                       Directory Mode Creation Mask
[-comment <text (size 1..256)> ]                         Share Comment
[-attribute-cache-ttl <[<integer>h][<integer>m][<integer>s]> ] File Attribute Cache Lifetime
[-offline-files {none|manual|documents|programs} ]      Offline Files
[ -vscan-fileop-profile {no_scan|standard|strict|writes_only} ] Vscan File-Operations Profile

rajesh-SN-2::> cifs share show ?
[ -fileopProfile | -instance | -shadowcopy | -umask | -fields <fieldname>, ... ]
[-vserver <vserver name> ]                             Vserver
[[-share-name] <Share>]                                   Share
[-cifs-server <NetBIOS> ]                                CIFS Server NetBIOS Name
[-path <text (size 1..256)> ]                             Path
[-share-properties <share properties>, ...]             Share Properties
[-symlink-properties {enable|hide|read_only}, ...]       Symlink Properties
[-file-umask <Octal Permission> ]                       File Mode Creation Mask
[-dir-umask <Octal Permission> ]                       Directory Mode Creation Mask
[-comment <text (size 1..256)> ]                         Share Comment
[-acl <text>, ... ]                                     Share ACL
[-attribute-cache-ttl <[<integer>h][<integer>m][<integer>s]> ] File Attribute Cache Lifetime
[-volume <volume name> ]                               Volume Name
[-offline-files {none|manual|documents|programs} ]      Offline Files
[ -vscan-fileop-profile {no_scan|standard|strict|writes_only} ] Vscan File-Operations Profile
```

Examples

```
rajesh-SN-2::vserver cifs share> create -vserver vserver_1 -share-name sh_new -path / -vscan-fileop-profile strict

rajesh-SN-2::vserver cifs share> show -instance -vserver vserver_1 -share-name sh_new

      Vserver: vserver_1
      Share: sh_new
CIFS Server NetBIOS Name: JRAJESH-SN-2
      Path: /
      Share Properties: oplocks
                        browsable
                        changenotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
      Volume Name: root_vol_1
      Offline Files: manual
Vscan File-Operations Profile: strict

rajesh-SN-2::vserver cifs share> modify -vserver vserver_1 -share-name sh_new -vscan-fileop-profile writes_only

rajesh-SN-2::vserver cifs share> show -instance -vserver vserver_1 -share-name sh_new

      Vserver: vserver_1
      Share: sh_new
CIFS Server NetBIOS Name: JRAJESH-SN-2
      Path: /
      Share Properties: oplocks
                        browsable
                        changenotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
      Volume Name: root_vol_1
      Offline Files: manual
Vscan File-Operations Profile: writes_only
```

ONTAPI

Following APIs are created to manage this feature. For details on the input/output refer to the c-mode ontapi zapidoc.

- **vscan-status-get-iter** - Returns Vscan status information.

- **vscan-status-status-modify** - Modify Vscan status.
- **vscan-on-access-policy-get-iter** - Returns list of On-Access policies.
- **vscan-on-access-policy-create** - Create an On-Access policy.
- **vscan-on-access-policy-delete** - Delete an On-Access policy.
- **vscan-on-access-policy-modify** - Modify an On-Access policy.
- **vscan-on-access-policy-status-modify** - Modify On-Access policy status.
- **vscan-scanner-pool-get-iter** - Returns list of scanner pools. Scanner pool is a set of attributes which are used to validate and manage connections between clustered Data ONTAP and Vscan servers (virus scanners).
- **vscan-scanner-pool-create** - Create a virus scanner pool, which is used for validating and managing connections between clustered Data ONTAP and Vscan servers.
- **vscan-scanner-pool-delete** - Delete a scanner pool.
- **vscan-scanner-pool-modify** - Modify a scanner pool.
- **vscan-scanner-pool-apply-policy** - Apply scanner-policy to a scanner pool.
- **vscan-active-scanner-pool-get-iter** - Returns active scanner pool configuration of a vserver.
- **vscan-reset** - Discard cached information of files that have been successfully scanned.
- **vscan-connection-status-all-get-iter** - Returns connection status.

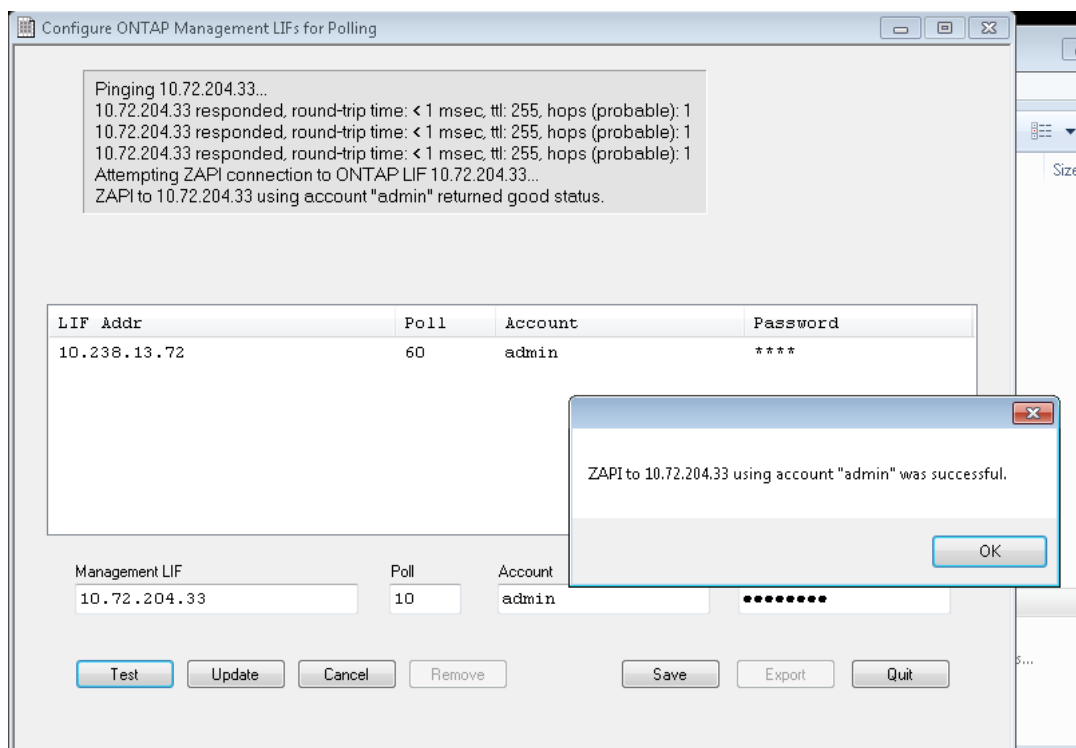
Three existing APIs are modified to accommodate new parameter (vscan-fileop-profile)

- **cifs-share-get-iter** (Modified) - Gives information about one or more CIFS shares.
- **cifs-share-create** (Modified) - Creates a new CIFS share rooted at the specified path.
- **cifs-share-modify** (Modified) - Modifies settings of a CIFS share, even if the shares are in use.

AV Connector Configuration

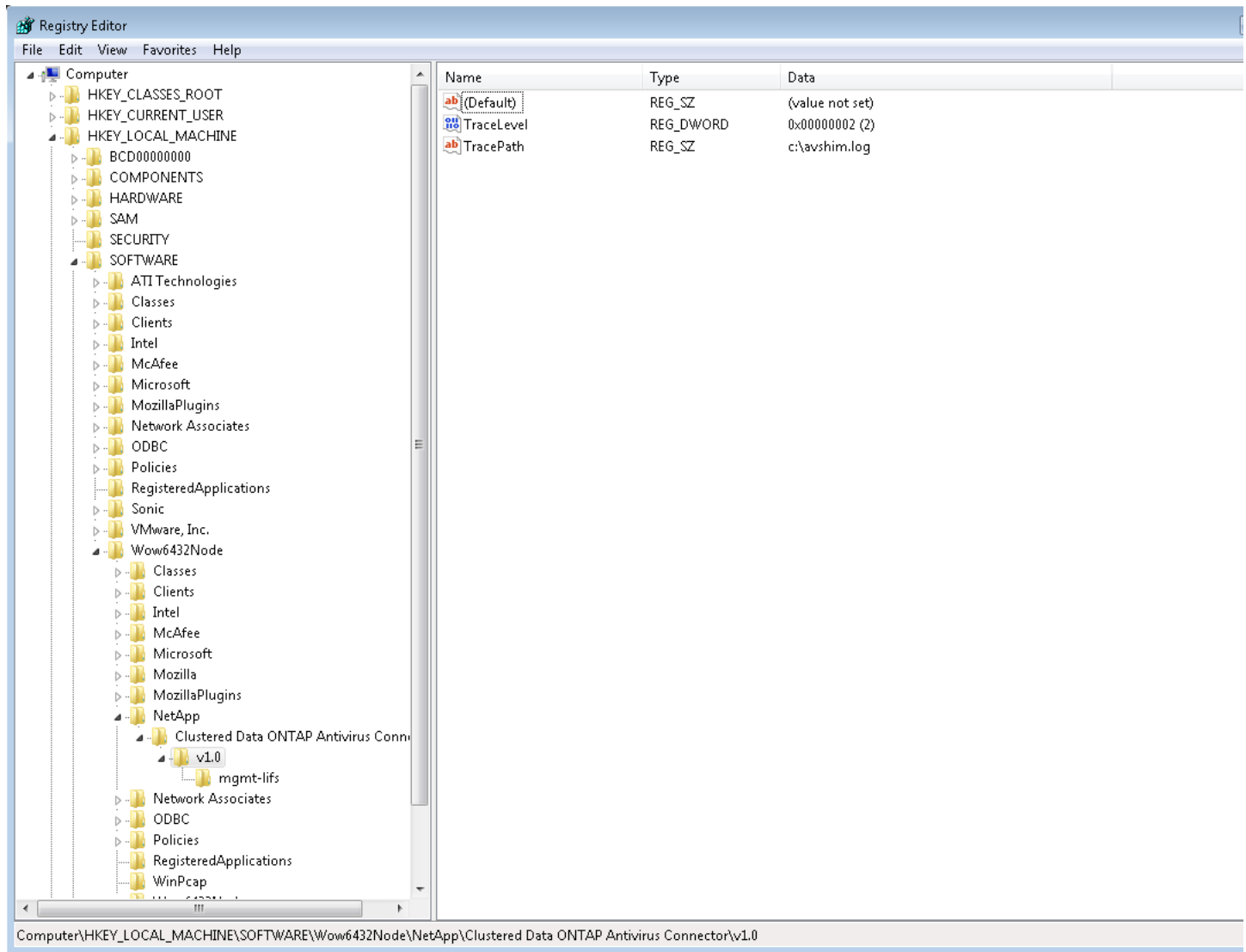
AV Connector (avshim) is an "off-tap" program which runs in a Windows server and interfaces between clustered Data ONTAP and a slightly modified version of the 7-mode vscan API that our AV partners currently provide. It is mostly a pass-through module that abstracts the cluster so that it looks like a single 7-mode filer. The primary function is to establish and maintain connections to the `vscan` named pipes on the configured vservers, and to pass along scan requests and scan responses from the partners' vscan engines.

NetApp will make this component available as a download to customers, who will be required to install it alongside the vendor's AV solution. Once installed, avshim starts running as a service called "ontapavc". The step by step installation procedure as screen shots is available here (<http://web.btc.netapp.in/~jrajesh/AV%20Connector>). The installation also creates a desktop shortcut to a GUI application to configure the ontapavc service with the network address of one or more management LIFs (logical network interfaces) that ontapavc uses to determine which data LIFs are serving files that require virus scanning. The application also has "Test" button which can be used to verify the input configuration.



By default, the ontapavc service does not do any tracing, but this can be changed by adding values to the “v1.0” registry key:

- A TracePath string value may be created which has the local path to a file which will receive trace output.
- By default, when running as a service, the trace level is 0, QUIET. To control the level of tracing, A TraceLevel DWORD value may be created which can be 0 (QUIET), 1 (INFO), 2 (VERBOSE), or 3 (DEEP).
- The trace file is truncated whenever the service starts, so it must be preserved if you want to keep a trace file across reboots or service restarts.
- These values can be added/changed at any time via regedit, and the updates take immediate effect.



top

AV Connector FAQ

- **What configuration information is needed for the avshim? And how is off-box vscan configured on the cluster?**

The avshim must be provided with the IP address or FQDN of one or more management hosts, each of which can be for a single vservers, or an entire cluster. This is done using registry entries, as described above. The avshim queries each management host for a list of vservers data LIFs, which the avshim will attempt to register with, at least one connection per vservers per node. Each vservers must be provided with the IP address or FQDN of one or more vscanners. It is possible to set up a cluster-wide list of available vscanners and vscan policies. ONTAP will reject any attempt to register as a vscanner if the client is not in the list of allowed vscanners. Additionally, the account used by the vscanner for privileged access (ontap_admin\$) must be one of a set of configured accounts.

In addition to the registry mechanism, it is possible to provide a list of one or more vservers data LIF IP addresses on the command line when avshim is started. It will then attempt to establish a connection to those IP addresses, regardless of any other configuration in the registry.

- **If the avshim is talking to multiple nodes on a cluster, how can the vscan engine monitor the status of all those nodes?**

The avshim will respond to the VS_FilerStatus() API to indicate its own health, as well as that of the components of the cluster that it is serving. If the avshim cannot communicate with the vservers LIFs that it is configured to serve, it will return non-zero status. This basic status may be sufficient for some purposes. We also support a new VS_AvshimStatus() API which will report information about the avshim and the nodes it is connected to.

- **Can a vscanner handle requests from more than one vservers? Does it work if all the vservers are not in the same cluster?**

Yes to both, as long as the account used to authenticate to the ontap_admin\$ share is valid for all vservers that are configured to use the vscanner. The UNC path sent from the avshim to the vscan engine includes everything needed to handle multiple NetApp vservers, even if they are in different clusters. Naturally, all vservers handled by a given vscanner must be in the same IP space.

- **Can a vscanner handle 7-mode requests when the avshim is installed?**

It is theoretically possible, if the vscan engine is configured to support multi-filer operation. In that case, the loopback connection would be used for all cluster requests, and the 7-mode connections would be handled as previously.

- Can more than one avshim be installed?

No. There is no provision for that, nor is there any need. A single avshim can be configured to handle an arbitrary number of vservers, and that is transparent to the vscan engine.

- What happens if a node fails over or a LIF is moved to a new node?

The avshim deals with all notification traffic between the cluster and the vscanner. Some cluster events may be transparent except for a temporary delay, while others may result in dropping SMB sessions. The avshim handles reconnecting after failover, and if any I/O from the vscan engine is disrupted by the failover, the vscan engine should just report the error response as usual. The avshim and/or cluster will deal with retries in this situation.

- How can the vscan engine detect that an incoming scan request is from the avshim?

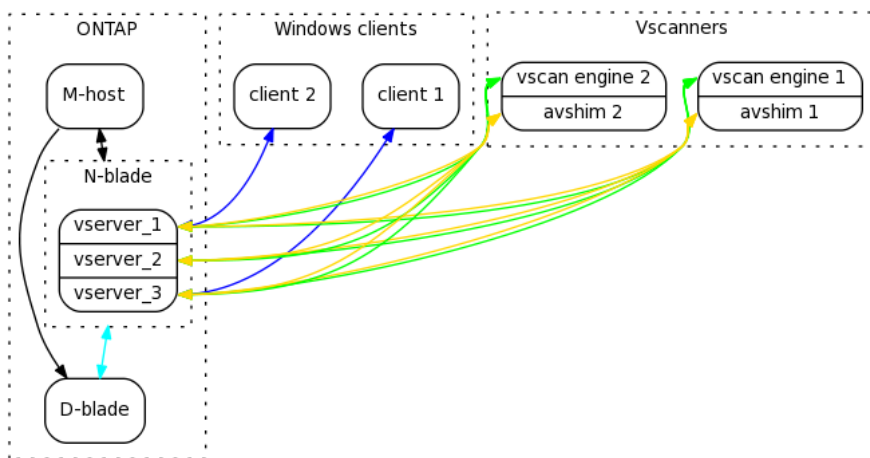
Incoming requests can be examined by the server using the `RpcServerInqCallAttributes` function, which returns, among other fields, the “`IsClientLocal`” value. However, to avoid the overhead of that call, the vscan engine can rely on the behavior described above, where we guarantee that the path that the avshim sends will always be prefixed with the string “`\\?\UNC\`”, and that non-avshim callers will not send that prefix.

top

Theory of Operation

Architectural Design

- High level (technical and architectural) concept how this product/feature works in normal operation.



Legend:

The **ONTAP** box comprises the standard M-host, N-blade, and D-blade components of Data ONTAP. They are not necessarily on a the same node, and multiple nodes are supported.

The **Windows clients** box represents normal SMB1, SMB2, or SMB3 Windows clients, connecting to CIFS shares over vserver data LIFs.

The **Vscanners** box comprises one or more vscanners, which are Windows boxes, each of which has both the NetApp-supplied *avshim* component, and the AV-partner-supplied *vscan engine*. Those two components communicate with each other on the same vscanner using a slightly modified version of the 7-mode vscan MSRPCs, over an in-memory loopback connection. There is no pre-set limit to the number of vscanners that can be configured. One or more vscanners can be configured to service only a single vserver, or they may service multiple vservers, or even all the vservers on a cluster, as long as the accounts used for connecting to all vservers are valid. In fact, there is no requirement for a vscanner to service only vservers on a single cluster, as long as all the vservers on all the clusters have compatible security information and are configured for those vscanners.

The **blue** lines show TCP connections between Windows SMB clients and vserver LIFs. These are normal client connections.

The **gold** lines show TCP connections between the avshim component on a vscanner, and the vservers. At least one connection will exist between each avshim component and each vserver which has LIFs on a node, for each node in the cluster. These are SMB connections which are authenticated as a special user account which is allowed to access the `vscan` named pipe which is used for the notification protocol.

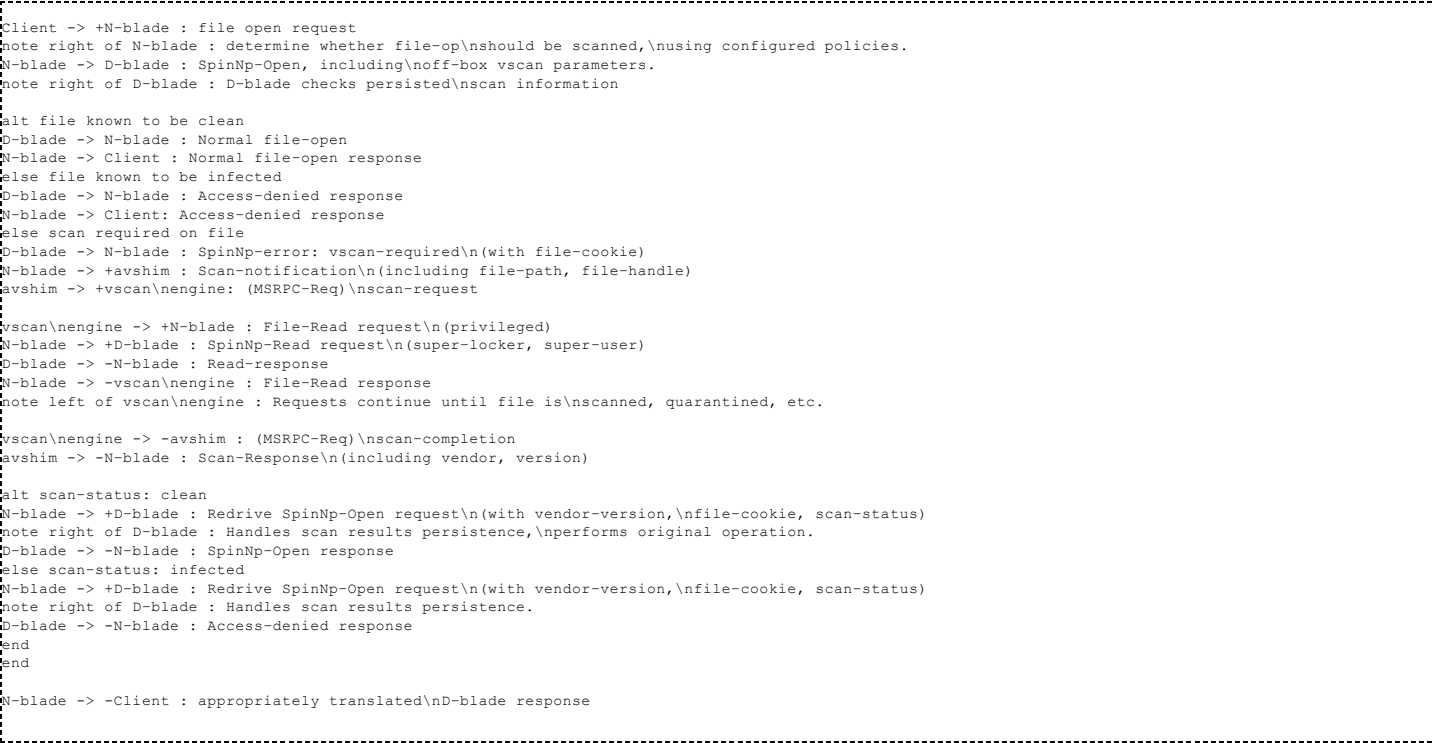
The **green** lines show TCP connections between the vscan engine component on a vscanner, and the vservers. At least one connection will exist between each vscan component and each vserver which has LIFs on a node, for each node in the cluster. If multiple data LIFs are available for a given vserver on a node, the avshim may use a round-robin among those LIFs when creating scan requests. These are SMB connections authenticated using a specially configured administrative user account which is allowed to access the `ontap_admin$` share, granting supercred and superlock privileges to the vscan engine.

The **cyan** line represents the normal SpinNp connection between the N-blade and the D-blade.

The **black** lines show intra-node communications which use KSMF to retrieve and send configuration information from the M-host. Both N-blade and D-blade require various pieces of this configuration information, and status information can also flow up to the M-host from the N-blade, via KSMF. In this design, it is never necessary for an N-blade or D-blade to contact the M-host of another node, as the configuration information is replicated cluster-wide.

Basic request/response flow

The following diagram shows the way requests are handled as they move from the client to the N-blade, the D-blade, possibly to the vscanner (avshim and vscan engine), and back to the N-blade and the original client. A note on terminology in the chart: "alt" means multiple alternative flows follow, with the alternatives labeled inside square brackets. Because of a bug in the wiki, the chart may not be rendered. If that happens, try re-loading the page.



Refer to Off-board AV FS for more detail.

top

Hardware and Software Requirements

- AV connector uses SMB2 and above for communicating with clustered Data ONTAP and so supported only on Windows 2008/R2, Windows 2012.

top

Licenses

- No additional license is required to enable Offbox-Vscan feature on Clustered ONTAP.
- For data access by virus-scan-engine over CIFS (data channel), CIFS license will be required.
- Appropriate vendor-licenses may be required for installing these on external vscanner. Engineering teams use the test licenses provided by the vendors. Support teams should contact product management for getting the licenses.

top

Upgrade and Revert

Offbox-Vscan feature is being introduced in SN.1 and will work only when all the nodes in the clustered ONTAP are at SN.1 or higher. This is taken care by leveraging the capability manager framework.

- The feature needs to be turned-off before any revert operation on any of the nodes of the cluster. Capability manager ensures that:
 - for the feature to be enabled, all nodes must be at SN.1 or above.
 - if the feature is enabled, no node running a release without this feature can join the cluster.

top

Performance

Performance is one of the key requirements for the feature as this directly impacts the data-access latency. The expectation is that the performance impact should be comparable to 7-mode vscan feature. The performance testing is yet to be done. The page will be updated once we have the results.

To assist the admin in monitoring the performance, many performance counters are added. This include the basic statistics collected from vscan-server as well. (Vscan-server extended stats are available in diag mode. Refer vsrver vscan connection-status section for more details.)

Vscan relevant counters are categorized as follows:

- offbox_scan_status: Collected in dblade per node basis. Available in diag mode.
- offbox_vscan: Collected in nblade per vsrver basis. Available in admin mode.
- offbox_vscan_server: Collected in nblade per [vsrver,server,node] basis. Available in diag mode. This contains basic stats collected from vscan-server.

The complete list of counters are given below:

```

jrajesh-SN-1::*> statistics show -object offbox_scan_status -sample-id status1

```

```

Object: offbox_scan_status
Instance: offbox_scan_status
Start-time: 8/13/2013 14:58:15
End-time: 8/13/2013 15:47:54
Cluster: jrajesh-SN-1

```

Counter	Value
av_status_cleared	988
file_size_exceeded	0
get_scan_status	13889
get_status_clean	9005
get_status_fherror	0
get_status_infected	0
get_status_scan_necessary	3466
get_status_scan_not_required	1418
instance_name	offbox_scan_status
node_name	jrajesh-SN-1-01
node_uuid	966ceb9c-e77e-11e2-9207-dfac764e5ba7
process_name	-
set_scan_status	3153

```

Object: offbox_scan_status
Instance: offbox_scan_status
Start-time: 8/13/2013 14:58:15
End-time: 8/13/2013 15:47:54
Cluster: jrajesh-SN-1

```

Counter	Value
set_status_clean	3151
set_status_fherror	0
set_status_infected	0
set_status_rescan_required	2

17 entries were displayed.

```

jrajesh-SN-1::*> statistics show -object offbox_vscan -sample-id vs1

```

```

Object: offbox_vscan
Instance: vserver_1
Start-time: 8/13/2013 14:57:48
End-time: 8/13/2013 15:47:17
Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)

```

Counter	Value
connections_accepted	0
connections_active	2
connections_filer_disconnected	0
connections_filer_disconnected_on_error	0
connections_filer_disconnected_timedout	0
connections_received	0
connections_rejected	0
connections_remote_disconnected	0
connections_total_disconnected	0
dispatch_latency	3us
dispatch_latency_base	3085
dispatch_latency_histogram	-
<20us	3084
<40us	0
<60us	0
<80us	0
<100us	0
<200us	0
<400us	0
<600us	0
<800us	0
<1ms	0
<2ms	0
<4ms	0
<6ms	0
<8ms	0
<10ms	1
<12ms	0
<14ms	0
<16ms	0
<18ms	0
<20ms	0
<40ms	0
<60ms	0
<80ms	0
<100ms	0
<200ms	0
<400ms	0
<600ms	0
<800ms	0
<1s	0
<2s	0
<4s	0
<6s	0
<8s	0
<10s	0
<20s	0
<30s	0
<60s	0
<90s	0
<120s	0
>=120s	0

```

Object: offbox_vscan
Instance: vserver_1
Start-time: 8/13/2013 14:57:48
End-time: 8/13/2013 15:47:17
Cluster: jrajesh-SN-1

```

```

Number of Constituents: 1 (complete_aggregation)
Counter                                     Value
-----
instance_name                             vserver_1

Object: offbox_vscan
Instance: vserver_1
Start-time: 8/13/2013 14:57:48
End-time: 8/13/2013 15:47:17
Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)
Counter                                     Value
-----
instance_uuid                             4
node_name                                jrajesh-SN-1-01
node_uuid                                966ceb9c-e77e-11e2-9207-dfac764e5ba7
process_name                             -
scan_latency                             16381us
scan_latency_base                         3074
scan_latency_histogram
<20us                                   1579
<40us                                   0
<60us                                   0
<80us                                   0
<100us                                  0
<200us                                  0
<400us                                  0
<600us                                  0
<800us                                  0
<1ms                                    0
<2ms                                    0
<4ms                                    0
<6ms                                    0
<8ms                                    0
<10ms                                   661
<12ms                                   741
<14ms                                   0
<16ms                                   0
<18ms                                   0
<20ms                                   46
<40ms                                   42
<60ms                                   1
<80ms                                   0
<100ms                                  1
<200ms                                  0
<400ms                                  2
<600ms                                  0
<800ms                                  0
<1s                                     0
<2s                                     0
<4s                                     0
<6s                                     0
<8s                                     0
<10s                                    0
<20s                                    0
<30s                                    0
<60s                                    1
<90s                                    0
<120s                                   0
>=120s                                  0

Object: offbox_vscan
Instance: vserver_1
Start-time: 8/13/2013 14:57:48
End-time: 8/13/2013 15:47:17
Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)
Counter                                     Value
-----
scan_noti_dispatched                      3085

Object: offbox_vscan
Instance: vserver_1
Start-time: 8/13/2013 14:57:48
End-time: 8/13/2013 15:47:17
Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)
Counter                                     Value
-----
scan_noti_dispatched_rate                 1
scan_noti_pending                         0
scan_noti_received                       3085
scan_noti_received_rate                   1
scan_noti_timedout                        0
scan_on_close                             3071
scan_on_open                              14
scan_on_read                              0
scan_on_rename                            0
scan_request_dispatched                   3085
scan_request_dispatched_rate               1
scan_request_pending                      0
scan_request_queued                       0
scan_request_timedout                     12

Object: offbox_vscan
Instance: vserver_1
Start-time: 8/13/2013 14:57:48
End-time: 8/13/2013 15:47:17
Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)
Counter                                     Value
-----
scan_resp_clean                           3074
scan_resp_failed                          0
scan_resp_failed_access_denied             0
scan_resp_failed_bad_reputation            0
scan_resp_failed_bad_reputation_quarantined 0
scan_resp_failed_block                     0
scan_resp_failed_block_file_access_generic 0
scan_resp_failed_busy                      0

```

```

scan_resp_failed_encrypted_container      0
scan_resp_failed_expired_license          0
scan_resp_failed_extract_depth            0
scan_resp_failed_extract_size             0
scan_resp_failed_extract_time             0
scan_resp_failed_infected_replace_failure 0

Object: offbox_vscan
Instance: vserver_1
Start-time: 8/13/2013 14:57:48
End-time: 8/13/2013 15:47:17
Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)
Counter                                     Value
-----
scan_resp_failed_internal_error            0
scan_resp_failed_internal_error_block      0
scan_resp_failed_internal_timeout          0
scan_resp_failed_internal_timeout_block    0
scan_resp_failed_malformed_container       0
scan_resp_failed_no_license                0
scan_resp_infected_action_unknown           0
scan_resp_infected_deleted                 0
scan_resp_infected_noblock                 0
scan_resp_infected_quarantined              0
scan_resp_infected_renamed                 0
scan_resp_infected_repair_failed           0
scan_resp_infected_repair_failed_quarantined 0
scan_resp_infected_repair_failed_readonly  0

Object: offbox_vscan
Instance: vserver_1
Start-time: 8/13/2013 14:57:48
End-time: 8/13/2013 15:47:17
Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)
Counter                                     Value
-----
scan_resp_infected_repair_quarantine_failed 0
scan_resp_infected_repaired                 0
scan_resp_internal_error_noblock            0
scan_resp_internal_timeout_noblock          0
67 entries were displayed.

jrajesh-SN-1::*> statistics show -object offbox_vscan_server -sample-id server1

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.27:jrajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36
Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)
Counter                                     Value
-----
connections_accepted                       0
connections_active                         1
connections_filer_disconnected              0
connections_filer_disconnected_on_error     0
connections_filer_disconnected_timedout     0
connections_received                       0
connections_rejected                       0
connections_remote_disconnected             0
connections_total_disconnected              0
instance_name                             vserver_1:10.72.204.27:jrajesh-SN-1-01
instance_uuid                             vserver_1:10.72.204.27:jrajesh-SN-1-01
node_name                                 jrajesh-SN-1-01

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.27:jrajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36
Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)
Counter                                     Value
-----
node_uuid                                966ceb9c-e77e-11e2-9207-dfac764e5ba7
process_name                             -
scan_latency                             4945us
scan_latency_base                         1563
scan_latency_histogram                    -
<20us                                    898
<40us                                    0
<60us                                    0
<80us                                    0
<100us                                   0
<200us                                   0
<400us                                   0
<600us                                   0
<800us                                   0
<1ms                                     0
<2ms                                     0
<4ms                                     0
<6ms                                     0
<8ms                                     0
<10ms                                    308
<12ms                                    315
<14ms                                    0
<16ms                                    0
<18ms                                    0
<20ms                                    22
<40ms                                    18
<60ms                                    0
<80ms                                    0
<100ms                                   1
<200ms                                   0
<400ms                                   0
<600ms                                   1

```

<800ms	0
<1s	0
<2s	0
<4s	0
<6s	0
<8s	0
<10s	0
<20s	0
<30s	0
<60s	0
<90s	0
<120s	0
>=120s	0

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.27:rajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36
Cluster: rajesh-SN-1

Number of Constituents: 1 (complete_aggregation)

Counter	Value
scan_on_close	1554
scan_on_open	9
scan_on_read	0
scan_on_rename	0
scan_request_dispatched	1563

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.27:rajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36
Cluster: rajesh-SN-1

Number of Constituents: 1 (complete_aggregation)

Counter	Value
scan_request_dispatched_rate	0
scan_request_pending	0
scan_request_requeued	0
scan_request_timedout	0
scan_resp_clean	1563
scan_resp_failed	0
scan_resp_failed_access_denied	0
scan_resp_failed_bad_reputation	0
scan_resp_failed_bad_reputation_quarantined	0
scan_resp_failed_block	0
scan_resp_failed_block_file_access_generic	0
scan_resp_failed_busy	0
scan_resp_failed_encrypted_container	0
scan_resp_failed_expired_license	0

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.27:rajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36
Cluster: rajesh-SN-1

Number of Constituents: 1 (complete_aggregation)

Counter	Value
scan_resp_failed_extract_depth	0
scan_resp_failed_extract_size	0
scan_resp_failed_extract_time	0
scan_resp_failed_infected_replace_failure	0
scan_resp_failed_internal_error	0
scan_resp_failed_internal_error_block	0
scan_resp_failed_internal_timeout	0
scan_resp_failed_internal_timeout_block	0
scan_resp_failed_malformed_container	0
scan_resp_failed_no_license	0
scan_resp_infected_action_unknown	0
scan_resp_infected_deleted	0
scan_resp_infected_noblock	0
scan_resp_infected_quarantined	0

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.27:rajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36
Cluster: rajesh-SN-1

Number of Constituents: 1 (complete_aggregation)

Counter	Value
scan_resp_infected_renamed	0
scan_resp_infected_repair_failed	0
scan_resp_infected_repair_failed_quarantined	0
scan_resp_infected_repair_failed_readonly	0
scan_resp_infected_repair_quarantine_failed	0
scan_resp_infected_repaired	0
scan_resp_internal_error_noblock	0
scan_resp_internal_timeout_noblock	0
scanner_stats_is_queue_full	0
scanner_stats_pct_cpu_used	0
scanner_stats_pct_dropped_requests	0
scanner_stats_pct_input_queue_avg	0
scanner_stats_pct_input_queue_hiwatemark	0
scanner_stats_pct_mem_used	14

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.27:rajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36
Cluster: rajesh-SN-1

Number of Constituents: 1 (complete_aggregation)

Counter	Value
scanner_stats_pct_network_used	0

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.29:rajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36

Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)

Counter	Value
connections_accepted	0
connections_active	1
connections_filer_disconnected	0
connections_filer_disconnected_on_error	0

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.29:jrajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36

Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)

Counter	Value
connections_filer_disconnected_timedout	0
connections_received	0
connections_rejected	0
connections_remote_disconnected	0
connections_total_disconnected	0
instance_name	vserver_1:10.72.204.29:jrajesh-SN-1-01
instance_uuid	vserver_1:10.72.204.29:jrajesh-SN-1-01
node_name	jrajesh-SN-1-01
node_uuid	966ceb9c-e77e-11e2-9207-dfac764e5ba7
process_name	-
scan_latency	27929us

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.29:jrajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36

Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)

Counter	Value
scan_latency_base	1552
scan_latency_histogram	-
<20us	701
<40us	0
<60us	0
<80us	0
<100us	0
<200us	0
<400us	0
<600us	0
<800us	0
<1ms	0
<2ms	0
<4ms	0
<6ms	0
<8ms	0
<10ms	362
<12ms	436
<14ms	0
<16ms	0
<18ms	0
<20ms	25
<40ms	24
<60ms	1
<80ms	0
<100ms	0
<200ms	0
<400ms	2
<600ms	0
<800ms	0
<1s	0
<2s	0
<4s	0
<6s	0
<8s	0
<10s	0
<20s	0
<30s	0
<60s	1
<90s	0
<120s	0
>=120s	0

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.29:jrajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36

Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)

Counter	Value
scan_on_close	1558
scan_on_open	5
scan_on_read	0
scan_on_rename	0
scan_request_dispatched	1563
scan_request_dispatched_rate	0
scan_request_pending	0
scan_request_requeued	0
scan_request_timedout	12

Object: offbox_vscan_server
Instance: vserver_1:10.72.204.29:jrajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36

Cluster: jrajesh-SN-1
Number of Constituents: 1 (complete_aggregation)

Counter	Value
scan_resp_clean	1552
scan_resp_failed	0

scan_resp_failed_access_denied	0
scan_resp_failed_bad_reputation	0
scan_resp_failed_bad_reputation_quarantined	0
scan_resp_failed_block	0
scan_resp_failed_block_file_access_generic	0
scan_resp_failed_busy	0
scan_resp_failed_encrypted_container	0
scan_resp_failed_expired_license	0
scan_resp_failed_extract_depth	0
scan_resp_failed_extract_size	0
scan_resp_failed_extract_time	0
scan_resp_failed_infected_replace_failure	0

Object: offbox_vscan_server
Instance: vsver_1:10.72.204.29:rajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36
Cluster: rajesh-SN-1

Number of Constituents: 1 (complete_aggregation)	
Counter	Value

scan_resp_failed_internal_error	0
scan_resp_failed_internal_error_block	0
scan_resp_failed_internal_timeout	0
scan_resp_failed_internal_timeout_block	0
scan_resp_failed_malformed_container	0
scan_resp_failed_no_license	0
scan_resp_infected_action_unknown	0
scan_resp_infected_deleted	0
scan_resp_infected_noblock	0
scan_resp_infected_quarantined	0
scan_resp_infected_renamed	0
scan_resp_infected_repair_failed	0
scan_resp_infected_repair_failed_quarantined	0
scan_resp_infected_repair_failed_readonly	0

Object: offbox_vscan_server
Instance: vsver_1:10.72.204.29:rajesh-SN-1-01
Start-time: 8/13/2013 14:58:02
End-time: 8/13/2013 15:47:36
Cluster: rajesh-SN-1

Number of Constituents: 1 (complete_aggregation)	
Counter	Value

scan_resp_infected_repair_quarantine_failed	0
scan_resp_infected_repaired	0
scan_resp_internal_error_noblock	0
scan_resp_internal_timeout_noblock	0
scanner_stats_is_queue_full	0
scanner_stats_pct_cpu_used	0
scanner_stats_pct_dropped_requests	0
scanner_stats_pct_input_queue_avg	0
scanner_stats_pct_input_queue_hiwatermark	1
scanner_stats_pct_mem_used	13
scanner_stats_pct_network_used	0

130 entries were displayed.

top

Troubleshooting

Common Problems

- **Symptom:** Vscanners are not able to connect to the clustered data ONTAP nodes

Possible Cause: Vsver data lif is not present or is down.

How to determine if this is the cause

Run 'network interface show' command to check if the vsver data lif is present on the node and is up.

How to resolve this problem

If the lif is not present on the node and a connection is required from this node, a vsver data lif needs to be created on this node.

Command Example: network interface create -vsver vsver_1 -lif vsver_1.data -data-protocol cifs,nfs,fcache -home-node rajesh-SN-1-01 -home-port e0c -address 10.238.12.196 -netmask 255.255.192.0

If the lif is down, issue command 'network interface modify' and set '-status-admin' field to up.

Command Example: network interface modify -vsver vsver_1 -lif vsver_1.data -home-node rajesh-SN-1-01 -status-admin up

Possible Cause: Vscanner is not reachable from the vsver data lif.

How to determine if this is the cause

Run command 'network ping -lif <vsver_data_lif> -destination <vscanner IP address> -lif-owner <vsver_name>' to see the vscanner is reachable.

Command Example: network ping -lif vsver_1.data -destination 10.72.204.27 -lif-owner vsver_1

How to resolve this problem

Check the routing table entries using command 'routing-groups route show' to check route is available for the vsver. If not add a route using 'routing-groups route create' command.

Command example: routing-groups route create -vsver vsver_1 -routing-group d10.238.0.0/18 -destination 0.0.0.0/0 -gateway 10.238.0.1

Possible Cause: Scanner pool configuration does not specify the vscanner IPs and/or users in the allowed list or is not active at the moment.

How to determine if this is the cause

Run command 'vsver vscan connection-status show-connected -vsver <vsver_name>' to see if at least one vscanner is connected to all the node where data lif for that vsver is present. If enabled ON-Access policy for the vsver has scan-mandatory filter added

and no vscanner is connected to the node on which client request has landed, then client access is denied.
Command Example: vscan scanner-pool show-active -vserver vserver_1

How to resolve this problem

If the active scanner pool configuration is empty (or does not include the required scanner pool), then activate one or more scanner pool by marking those primary/secondary as required.

Command example: vserver vscan scanner-pool apply-policy -vserver vserver_1 -scanner-pool pl -scanner-policy primary

If the active scanner pool configuration applied to the vserver does not have the vscanner's IP or the user, then add those to any of the active scanner pools.
Command example: vserver vscan scanner-pool modify -vserver vserver_1 -scanner-pool pl -servers 10.72.204.27,10.72.204.29 -privileged-users fsct\administrator

■ Symptom: Client-access is denied

Possible Cause: No vscanner is connected to the node on which client request has landed.

How to determine if this is the cause

Run 'vserver vscan connection-status show-connected -vserver <vserver_name>' command to check if at least one vscanner is connected to all the nodes on which the vserver data lifs are hosted. If no vscanner is connected to any such node and enabled On-Access policy has scan-mandatory filter added, the client access is denied.

Command example: vserver vscan connection-status show-connected -vserver vserver_1
vserver vscan on-access-policy show -vserver vserver_1 -policy-status on -instance

How to resolve this problem

If the vscanner should be connected but is not, then refer to 1st symptom.

If you want to let the client access go through even though no vscanner is connected, then remove the scan-mandatory filter from the enabled On-Access policy using command "vserver vscan on-access-policy modify".

Command Example: vserver vscan on-access-policy modify -vserver vserver_1 policy1 -filters ""

■ Symptom: Vscanners are connected, but still file is not getting scanned

Possible Cause: On-Access policy is not configured properly.

How to determine if this is the cause

Run 'vserver vscan on-access-policy show -vserver <vserver_name> -policy-status on -instance' command to check if the scope of scanning is properly defined.
Command Example: vserver vscan on-access-policy show -vserver vserver_1 -policy-status on -instance

How to resolve this problem

Modify the enabled On-Access policy to define the scope more precisely using "vserver vscan on-access-policy modify" command.

Command Example: vserver vscan on-access-policy modify -vserver vserver_1 -policy-name pl -paths-to-exclude \vol1\tmp -file-ext-to-exclude txt,mp3

Possible Cause: CIFS share using which file is accessed has wrong configuration for vscan-fileop-profile parameter.

How to determine if this is the cause

Run 'vserver cifs share show -vserver <vserver_name> -instance' command to check if the vscan-fileop-profile is set as required.
If it is set as no_scan then no fileop on this share will trigger the virus scan.

Command Example: vserver cifs share show -vserver vserver_1 -instance

How to resolve this problem

Modify the vscan-fileop-profile parameter of the CIFS share as required using "vserver cifs share modify" command.

Command Example: vserver cifs share modify -vserver vserver_1 -share-name sh1 -vscan-fileop-profile standard

■ Symptom: Client are observing high latency

Possible Cause: Vscanners are overloaded.

How to determine if this is the cause

Check the vscanner's stats and latency using "statistics show -object offbox_vscan_server" from diag mode.
The vscanner's extended stats can also be seen using "vserver vscan connection-status show-extended-stats -vserver <vserver_name>".
If the latency figures are on the higher side and resource utilization of vscanner is high, that means vscanner is getting overloaded.

Command Example: statistics show -object offbox_vscan_server -sample-id <sample_id>

How to resolve this problem

Configure one or more vscanners to serve the vserver. Add the IP of new vscanner to any of the primary scanner pools.

Command Example: vserver vscan scanner-pool modify -vserver vserver_1 -scanner-pool pl -servers 10.72.204.27,10.72.204.29,10.72.204.30
-privileged-users cifs\administrator,fsct\new

How to isolate problem between AVSHIM and AV software

Following is the general categorization of problems

- AVSHIM:
 - All connection related.
- AV software:
 - High latency.
 - Issues related to failures in quarantine actions of infected files.

- Data access related.

This section will be updated as and when some other kind of issues are seen.

top

Mhost Logging

- What Mhost logs are used by this feature?

Vscan configuration and job related logs are logged in mgwd.log* files.

- How is the signature in the MHost log that the log message is related to this feature?

Logs logged by configuration in mgwd.log can be found by signature "tables::vscan", "tables::vscan_replay" and "Vscan::Auto_Job".

- Does this feature log to the Mhost log when there are no errors or problems? If yes, please provide the log entries that are normally logged by this feature.

Some important event triggers debug or info level of logs but the default log level of all the sub components is warning or more, so no message will be

top

Avshim Logging

By default, the avshim (ontapavc service) does not do any logging, but this can be changed by adding values to the “v1.0” registry key. Details are available here.

top

Triage and Data Collection

Triage and data collection is crucial to all levels of support but is especially important to front-line support personnel whose job it is to do problem isolation and diagnosis. In order to do this, they need to know what questions to ask and what data needs to be collect. Sample questions to consider answering:

- How do I determine if what the customer is reporting is a problem with this feature or product?

When properly deployed, vscan feature should trigger virus scanning for the files which come under the scope of scanning as defined in On-Access policy. The following must be collected and analyzed:

- Vscan configuration information and log files (mgwd.log* and sktlogd.log*). If possible trigger an autosupport(full) to collect vscan configuration and
- Ems messages or ems logs file for any ems logged by vscan feature.
- Performance counters (Admin mode: offbox_vscan, Diag mode: offbox_vscan_server and offbox_scan_status).
- VScan extended-statistics (Diag mode: 'vscan connection-status show-extended-stats)

- How do I isolate a customer reported problem to this feature or product?

- Check if vscan is enabled on any vservers in the cluster. If not, more chances are that this is not vscan specific.
- Check for configuration, log files, ems.

- What data do I collect and how do I collect it?

- Vscan configuration information and log files (mgwd.log* and sktlogd.log*). If possible trigger an autosupport(full) to collect vscan configuration and
- Ems messages or ems logs file.
- Performance counters (Admin mode: offbox_vscan, Diag mode: offbox_vscan_server and offbox_scan_status).
- VScan extended-statistics (Diag mode: 'vscan connection-status show-extended-stats)

To collect the data:

Generate autosupport (callhome.invoke.all, callhome.ondemand.invoke.all) if not already generated and collect vscan configuration, ems messages, log files

- How do I determine the version of the product?

This feature is being introduced in SN.1, so currently there is only one version.

- How do I determine if the customer is running a supported configuration?

Currently there is only one version.

- Where is error messages logged and how do I collect the log files?

Log files are present in /mroot/etc/mlog/ directory. These can be collected just like any other mhost log file. Also full autosupport can be triggered f

top

Tracing

INTERNAL ONLY

- What tracing tools are used with this feature? RASrTrace, SKTrace, MTrace, etc...

SKTrace is used for Nblade/Dblade tracing.

- What tracing is enabled with this feature?
- How would tracing be enabled, logged, and correlated? Please provide examples.

Nblade tracing can be enabled using the command "sudo sysctl sysvar.sktrace.NBLADE_OFFBOX_VSCAN_enable=63".
Dblade tracing can be enabled using the command "sudo sysctl sysvar.dbg.avoa=26".
Both the commands must be run from FreeBSD shell.

INTERNAL ONLY

top

Diagnostics Tools

No new diagnostic tool is developed.

top

Error Messages

All the CLI and corresponding ZAPI errors are updated here (https://wikid.netapp.com/w/User:Jrajesh/Off-board_AV/Error_Messages) .

top

AutoSupport & EMS Logging

AutoSupport

List new, updated or deprecated AutoSupport Messages in table format if possible. If the AutoSupport is not new but the output has changed (added or deleted content), add that content as well.

- What new AutoSupport messages have been defined?
- What does the AutoSupport mean?
- What is the message severity?
- How frequently is it sent?
- What action is required from Technical Support or the Customer, if any, to recover?
- What data is collected and where to find it?

No new autosupport messages are defined. Content is added to existing autosupport messages.

- For existing AutoSupports, what new content, if any, has been removed or added?

New content is added to following existing autosupports:

- 1) Weekly autosupport (callhome.weekly)
Content: All the vscan configuration.
- 2) User triggered/On demand (callhome.invoke, callhome.ondemand.invoke)
Content: All the vscan configuration.
- 3) User triggered/On demand Full (callhome.invoke.all, callhome.ondemand.invoke.all)
Content: All the vscan configuration.
- 4) Performance counters are also defined which will be sent as per autosupport policy for counters (hourly,weekly or event triggered).

Below is the link to generated autosupport message from CLI:

```
system node autosupport invoke -node local -type all -force true -message "VSCAN_ASUP_TEST"

http://asup-tools-eprod.rtp.netapp.com/asup-search/AsupConsole?AsupId=2013061015300020&BizKey=C%7C03BCCB80-C2CA-11E2-ACC5-123478563412%7C8629107448%7C40
```

- Are there any changes (new or updated AutoSupports) that will affect the AutoSupport parsing software (xterra)? INTERNAL ONLY

NO

- What data (commands, logs, tool output, etc...) is not collected by Autosupport that would need to be collected to troubleshoot this feature?

NA

- What data (commands, logs, tool output, etc...) is not collected by Autosupport that would need to be collected to file a BURT against this feature?

NA

EMS Logging

- What new messages have been added?

Message Type - Vscan is enabled.
When - When a Vserver or cluster administrator enables Vscan on a Vserver.
Source - vscan.enabled
Sample Message - Vscan is enabled on Vserver 'vserver_1'.

Message Type - Vscan is disabled.
When - When a Vserver or cluster administrator disables Vscan on a Vserver.
Source - vscan.disabled
Sample Message - Vscan is disabled on Vserver 'vserver_1'.

Message Type - Creation of ONTAP_ADMIN share failed.
When - When a privileged share \$ONTAP_ADMIN creation fails
Source - vscan.privShareCreate.failed
Sample Message - Failed to create privileged share \$ONTAP_ADMIN for Vserver 'vserver_1'.

Message Type - RDB updated callback registration failed.
When - When the Vscan configuration replication mechanism fails to register RDB update callback.
Source - vscan.rdbUpdRegister.failed
Sample Message - Vscan configuration replication mechanism failed to register RDB update callback. Modification in the Vscan configuration might not be

Message Type - Vscan job failed.
When - When the Vscan job fails.
Source - vscan.job.failed
Sample Message - Vscan job failed. It will automatically be retried.

Message Type - Scanner pool auto activated.
When - When the Vscan scanner pool is automatically activated.
Source - vscan.pool.autoActivated
Sample Message - Vscan scanner pool 'spl' is automatically activated on Vserver 'vserver_1'.

Message Type - Scanner pool auto deactivated.
When - When the Vscan scanner pool is automatically deactivated.
Source - vscan.pool.autoDeactivated
Sample Message - Vscan scanner pool 'spl' is automatically deactivated on Vserver 'vserver_1'.

Message Type - New Version-ID allocated.
When - When the Vscan version mechanism allocates a new version-ID corresponding to the Vscan server version.
Source - vscan.newVersion.allocated
Sample Message - Vscan version mechanism added new version-ID for Vserver 'vserver_1' corresponding to vendor 'McAfee', version '5.62'.

- What new messages have been changed?

None

- What new messages have been deprecated?

None

- How frequently are these messages logged?

EMS is logged when any of these events occur, there is no timer suppression.

top

Known Problems

INTERNAL ONLY

List all open bugs in this release. Include those with customer cases and those without. (cnt_call_rec field in BURT >= 0)

http://burtweb-prd.eng.netapp.com/burt/burt-bin/start?burt-id=&button=&google_text=&sel_report=&report=offbox-vscan-known-issues&report_user=jrajesh&fz=

List all open bugs with customer cases. Include only those bugs that have customer cases. (cnt_call_rec field in BURT > 0)

None

INTERNAL ONLY

Fixed Problems

INTERNAL ONLY

List all bugs fixed in this release. Include those with customer cases and those without. (*cnt_call_rec field in BURT >= 0*)

http://burtweb-prd.eng.netapp.com/burt/burt-bin/start?burt-id=&button=&google_text=&sel_report=&report=offbox-vscan-fixed-issues&report_user=jrajesh&fz=

List bugs fixed in this release. Include only those bugs that have customer cases. (*cnt_call_rec field in BURT > 0*)

None

INTERNAL ONLY

Limitations

- AV connector is supported only on SMB2 and above.
- Only CIFS protocol based traffic results in virus scanning.
- Scan status of already scanned file is not saved on-disk. This means that rebooting a node may generate spike in scan requests.

Knowledge Base Articles

KB ID: 2018449 [CMODE] [NEW] Troubleshooting Workflow: Clustered Data ONTAP Antivirus Connector (Offbox \ Offboard AV) <https://kb.netapp.com/support/index?page=content&id=2018449>

TTT: KB ID: 1014454 Triage Template: Clustered Data ONTAP Antivirus Connector (Offbox \ Offboard AV) <https://kb.netapp.com/support/index?page=content&id=1014454>

Test Plans and Results

ALM location:

- Test plan: ONTAP\Protocols\CIFS\Clustered\SN.1\Off-Box AV\
- Test results: /root/ONTAP/SierraNevada/sierranevada.1/RSierranevada/05_FST/Protocols/CIFS/Cmode/New_Features/Off-Box_AV

Functional, Design and Architectural Specifications

- clustered ONTAP Off-box AV Architecture Specification
- clustered ONTAP Off-box AV Functional Specification
- clustered ONTAP off-box "avshim" Functional Specification
- Vscan named pipe notification wire protocol

Reference Material

- Provide links to user documentation (e.g., Admin Guide, Configuration Guide, Release Notes, etc.)

http://nbrls02.eng.btc.netapp.in/techpubs/working/Manish/Antivirus/SN.1/PDF/Antivirus_Configuration_Guide_for_Cluster-Mode.pdf

- Provide links to technical documentation such as Best Practices Guides, Technical Reports and White Papers

Not Available currently.

- Provide links to relevant third party documentation (e.g., Veritas, VMWare, Microsoft, Emulex, QLogic, etc).

Not Available currently.

- Provide links to interoperability (e.g., IMT) or other matrices

Not Available currently.

- Provide link to engineering project page

https://wikid.netapp.com/w/CIFS/clustered_ONTAP/Off-box_AV

- Provide link to PRD

<https://wikid.netapp.com/w/User:Mohana/Cmode-Offboard-Vscan-Requirements>

top

Support and Escalation Information

- CSS is only responsible for the AV Connector and ONTAP. For specific questions on the 3rd party Anti-Virus software (Virus pattern files, etc) customers should be directed back to the AV software partner.
- Engineering escalations: dl-cmode-offbox-vscan-case-esc (was dl-cmode-offbox-vscan before 11/20/2013)
- Engineering contact list for Escalations to NetApp Engineering: https://wikid.netapp.com/w/AntiVirus_C-mode_off-box_Contacts
- BURT
 - C-mode offbox AV: Type: NG Subtype: av_offbox
 - cDOT AV connector: Type:SW_AVSHIM Subtype: avshim

top

Contact Information

< INTERNAL ONLY >

- Mark Muhlestein (<mailto:Mark.Muhlestein@netapp.com>)
- Sunil Bhargo (<mailto:Sunil.Bhargo@netapp.com>)
- Mankawaldeep Singh (<mailto:Mankawal.Singh@netapp.com>)
- Rajesh Jaiswal (<mailto:Rajesh.Jaiswal@netapp.com>)

< INTERNAL ONLY >

top

Retrieved from "https://wikid.netapp.com/wikid/index.php?title=NGS_NPI/Data_ONTAP/8.2.1_TOI/OB_AV&oldid=6547050"

-
- This page was last modified on 25 November 2013, at 16:47.