Vscan server installation and configuration

ONTAP 9

NetApp
January 29, 2024

Table of Contents

Vscan server installation and configuration

Vscan server installation and configuration

Set up one or more Vscan servers to ensure that files on your system are scanned for viruses. Follow the instructions provided by your vendor to install and configure the antivirus software on the server.

Follow the instructions in the README file provided by NetApp to install and configure the ONTAP Antivirus Connector. Alternatively, follow the instructions on the Install ONTAP Antivirus Connector page.

> For disaster recovery and MetroCluster configurations, you must set up and configure separate Vscan servers for the primary/local and secondary/partner ONTAP clusters.

Antivirus software requirements

- For information about antivirus software requirements, see the vendor documentation.
- For information about the vendors, software, and versions supported by Vscan, see the Vscan partner solutions page.

ONTAP Antivirus Connector requirements

- You can download the ONTAP Antivirus Connector from the **Software Download** page on the NetApp Support Site. NetApp Downloads: Software
- For information about the Windows versions supported by the ONTAP Antivirus Connector and interoperability requirements, see Vscan partner solutions.

> You can install different versions of Windows servers for different Vscan servers in a cluster.

- .NET 3.0 or later must be installed on the Windows server.
- SMB 2.0 must be enabled on the Windows server.

Install ONTAP Antivirus Connector

Install the ONTAP Antivirus Connector on the Vscan server to enable communication between the system running ONTAP and the Vscan server. When the ONTAP Antivirus Connector is installed, the antivirus software is able to communicate with one or more storage virtual machines (SVMs).

About this task

- See the Vscan partner solutions page for information about the supported protocols, antivirus vendor software versions, ONTAP versions, interoperability requirements and Windows servers.
- .NET 4.5.1 or later must be installed.
- The ONTAP Antivirus Connector can run on a virtual machine. However, for best performance, NetApp recommends using a dedicated virtual machine for antivirus scanning.
- SMB 2.0 must be enabled on the Windows server on which you are installing and running the ONTAP

Antivirus Connector.

Before you begin

- Download the ONTAP Antivirus Connector setup file from the Support Site and save it to a directory on your hard drive.
- Verify that you meet the requirements to install the ONTAP Antivirus Connector.
- Verify that you have administrator privileges to install the Antivirus Connector.

Steps

1. Start the Antivirus Connector installation wizard by running the appropriate setup file.
2. Select *Next*. The Destination Folder dialog box opens.
3. Select *Next* to install the Antivirus Connector to the folder that is listed or select *Change* to install to a different folder.
4. The ONTAP AV Connector Windows Service Credentials dialog box opens.
5. Enter your Windows service credentials or select **Add** to select a user. For an ONTAP system, this user must be a valid domain user and must exist in the scanner pool configuration for the SVM.
6. Select **Next**. The Ready to Install the Program dialog box opens.
7. Select **Install** to begin the installation or select **Back** if you want to make any changes to the settings. A status box opens and charts the progress of the installation, followed by the InstallShield Wizard Completed dialog box.
8. Select the Configure ONTAP LIFs check box if you want to continue with the configuration of ONTAP management or data LIFs. You must configure at least one ONTAP management or data LIF before this Vscan server can be used.
9. Select the Show the **Windows Installer log** check box if you want to view the installation logs.
10. Select **Finish** to end the installation and to close the InstallShield wizard. The **Configure ONTAP LIFs** icon is saved on the desktop to configure the ONTAP LIFs.
11. Add an SVM to the Antivirus Connector. You can add an SVM to the Antivirus Connector by adding either an ONTAP management LIF, which is polled to retrieve the list of data LIFs, or by directly configuring the data LIF or LIFs. You must also provide the poll information and the ONTAP admin account credentials if the ONTAP management LIF is configured.
    - Verify that the management LIF or the IP address of the SVM is enabled for `management-https`. This is not required when you are only configuring data LIFs.
    - Verify that you have created a user account for the HTTP application and assigned a role which has (at least read-only) access to the `/api/network/ip/interfaces` REST API. For more information about creating a user, see the security login role create and security login create ONTAP man pages.

> You can also use the domain user as an account by adding an authentication tunnel SVM for an administrative SVM. For more information, see the security login domain-tunnel create ONTAP man page or use the `/api/security/acccounts` and `/api/security/roles` REST APIs to configure the admin account and role.

Steps

a. Right-click on the **Configure ONTAP LIFs** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **Run as Administrator**.

b. In the Configure ONTAP LIFs dialog box, select the preferred configuration type, then perform the following actions:

To create this type of LIF…	Perform these steps…
Data LIF	a. Set "role" to "data" b. Set "data protocol" to "cifs" c. Set "firewall policy" to "data" d. Set "service policy" to "default-data-files"
Management LIF	a. Set "role* to "data" b. Set "data protocol" to "none" c. Set "firewall policy" to "mgmt" d. Set "service policy" to "default-management"

Read more about creating a LIF.

After you create a LIF, enter the data or management LIF or IP address of the SVM that you want to add. You can also enter the cluster management LIF. If you specify the cluster management LIF, all SVMs within that cluster that are serving SMB can use the Vscan server.

> When Kerberos authentication is required for Vscan servers, each SVM data LIF must have a unique DNS name, and you must register that name as a server principal name (SPN) with the Windows Active Directory. When a unique DNS name is not available for each data LIF or registered as an SPN, the Vscan server uses the NT LAN Manager mechanism for authentication. If you add or modify the DNS names and SPNs after the Vscan server is connected, you must restart the Antivirus Connector service on the Vscan server to apply the changes.

c. To configure a management LIF, enter the poll duration in seconds. The poll duration is the frequency at which the Antivirus Connector checks for changes to the SVMs or the cluster's LIF configuration. The default poll interval is 60 seconds.
d. Enter the ONTAP admin account name and password to configure a management LIF.
e. Click **Test** to check the connectivity and verify the authentication. Authentication is verified only for a management LIF configuration.
f. Click **Update** to add the LIF to the list of LIFs to poll or to connect to.
g. Click **Save** to save the connection to the registry.
h. Click **Export** if you want to export the list of connections to a registry import or registry export file. This is useful if multiple Vscan servers use the same set of management or data LIFs.

See the Configure the ONTAP Antivirus Connector page for configuration options.

Configure the ONTAP Antivirus Connector

Configure the ONTAP Antivirus Connector to specify one or more storage virtual machines (SVMs) that you want to connect to by either entering the ONTAP management LIF, poll information, and the ONTAP admin account credentials, or just the data LIF. You can also modify the details of an SVM connection or remove an SVM connection. By default, the ONTAP Antivirus Connector uses REST APIs to retrieve the list of data LIFs if

the ONTAP management LIF is configured.

Modify the details of an SVM connection

You can update the details of a storage virtual machine (SVM) connection, which has been added to the Antivirus Connector, by modifying the ONTAP management LIF and the poll information. You cannot update data LIFs after they have been added. To update data LIFs you must first remove them and then add them again with the new LIF or IP address.

Before you begin

Verify that you have created a user account for the HTTP application and assigned a role which has (at least read-only) access to the `/api/network/ip/interfaces` REST API. For more information about creating a user, see the security login role create and the security login create commands. You can also use the domain user as an account by adding an authentication tunnel SVM for an administrative SVM. For more information, see the security login domain-tunnel create ONTAP man page.

Steps

1. Right-click the **Configure ONTAP LIFs** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **Run as Administrator**. The Configure ONTAP LIFs dialog box opens.
2. Select the SVM IP address, and then click **Update**.
3. Update the information, as required.
4. Click **Save** to update the connection details in the registry.
5. Click **Export** if you want to export the list of connections to a registry import or a registry export file. This is useful if multiple Vscan servers use the same set of management or data LIFs.

Remove an SVM connection from the Antivirus Connector

If you no longer require an SVM connection, you can remove it.

Steps

1. Right-click the **Configure ONTAP LIFs** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **Run as Administrator**. The Configure ONTAP LIFs dialog box opens.
2. Select one or more SVM IP addresses, and then click **Remove**.
3. Click **Save** to update the connection details in the registry.
4. Click **Export** if you want to export the list of connections to a registry import or registry export file. This is useful if multiple Vscan servers use the same set of management or data LIFs.

Troubleshoot

Before you begin

When you are creating registry values in this procedure, use the right-side pane.

You can enable or disable Antivirus Connector logs for diagnostic purposes. By default, these logs are disabled. For enhanced performance, you should keep the Antivirus Connector logs disabled and only enable them for critical events.

Steps

1. Select **Start**, type "regedit" into the search box, and then select `regedit.exe` in the Programs list.
2. In **Registry Editor**, locate the following subkey for the ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Create registry values by providing the type, name, and values shown in the following table:

Type	Name	Values
String	Tracepath	c:\avshim.log

   This registry value could be any other valid path.

4. Create another registry value by providing the type, name, values, and logging information shown in the following table:

Type	Name	Critical logging	Intermediate logging	Verbose logging
DWORD	Tracelevel	1	2 or 3	4

   This enables Antivirus Connector logs that are saved at the path value provided in the TracePath in Step 3.

5. Disable Antivirus Connector logs by deleting the registry values you created in Steps 3 and 4.
6. Create another registry value of type "MULTI_SZ" with the name "LogRotation" (without quotes). In "LogRotation", provide "logFileSize:1" as an entry for rotation size (where 1 represents 1MB) and in the next line, provide "logFileCount:5" as an entry for rotation limit (5 is the limit).

   These values are optional. If they are not provided, default values of 20MB and 10 files are used for the rotation size and rotation limit respectively. Provided integer values do not provide decimal or fraction values. If you provide values higher than the default values, the default values are used instead.

7. To disable the user-configured log rotation, delete the registry values you created in Step 6.

Customizable Banner

A custom banner allows you to place a legally binding statement and a system access disclaimer on the *Configure ONTAP LIF API* window.

Step

1. Modify the default banner by updating the contents in the `banner.txt` file in the install directory and then saving the changes. You must reopen the Configure ONTAP LIF API window to see the changes reflected in the banner.

Enable Extended Ordinance (EO) mode

You can enable and disable Extended Ordinance (EO) mode for secure operation.

Steps

1. Select **Start**, type "regedit" in the search box, and then select `regedit.exe` in the Programs list.
2. In **Registry Editor**, locate the following subkey for ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. In the right-side pane, create a new registry value of type "DWORD" with the name "EO_Mode" (without quotes) and value "1" (without quotes) to enable EO Mode or value "0" (without quotes) to disable EO Mode.

By default, if the `EO_Mode` registry entry is absent, EO mode is disabled. When you enable EO mode, you must configure both the external syslog server and mutual certificate authentication.

Configure the external syslog server

Before you begin

Take note that when you are creating registry values in this procedure, use the right-side pane.

Steps

1. Select **Start**, type "regedit" in the search box, and then select `regedit.exe` in the Programs list.
2. In **Registry Editor**, create the following subkey for ONTAP Antivirus Connector for syslog configuration: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Create a registry value by providing the type, name, and value as shown in the following table:

Type	Name	Value
DWORD	syslog_enabled	1 or 0

   Please note that a "1" value enables the syslog and a "0" value disables it.

4. Create another registry value by providing the information as shown in the following table:

Type	Name
REG_SZ	Syslog_host

   Provide the syslog host IP address or domain name for the value field.

5. Create another registry value by providing the information as shown in the following table:

Type	Name
REG_SZ	Syslog_port

   Provide the port number on which the syslog server is running in the value field.

6. Create another registry value by providing the information as shown in the following table:

Type	Name

REG_SZ	Syslog_protocol

Enter the protocol that is in use on the syslog server, either "tcp" or "udp", in the value field.

7. Create another registry value by providing the information as shown in the following table:

Type	Name	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Create another registry value by providing the information as shown in the following table:

Type	Name	Value
DWORD	syslog_tls	1 or 0

Please note that a "1" value enables syslog with Transport Layer Security (TLS) and a "0" value disables syslog with TLS.

Ensure a configured external syslog server runs smoothly

- If the key is absent or has a null value:
  - The protocol defaults to "tcp".
  - The port defaults to "514" for plain "tcp/udp" and defaults to "6514" for TLS.
  - The syslog level defaults to 5 (LOG_NOTICE).
- You can confirm that syslog is enabled by verifying that the `syslog_enabled` value is "1". When the `syslog_enabled` value is "1", you should be able to log in to the configured remote server whether or not EO mode is enabled.
- If EO mode is set to "1" and you change the `syslog_enabled` value from "1" to "0", the following applies:
  - You cannot start the service if syslog is not enabled in EO mode.
  - If the system is running in a steady state, a warning appears that says syslog cannot be disabled in EO mode and syslog is forcefully set to "1", which you can see in the registry. If this occurs, you should disable EO mode first and then disable syslog.
- If the syslog server is unable to run successfully when EO mode and syslog are enabled, the service stops running. This might occur for one of the following reasons:
  - An invalid or no syslog_host is configured.
  - An invalid protocol apart from UDP or TCP is configured.
  - A port number is invalid.
- For a TCP or TLS over TCP configuration, if the server is not listening on the IP port, the connection fails and the service shuts down.

Configure X.509 mutual certificate authentication

X.509 certificate based mutual authentication is possible for the Secure Sockets Layer (SSL) communication between the Antivirus Connector and ONTAP in the management path. If EO mode is enabled and the

certificate is not found, the AV Connector terminates. Perform the following procedure on the Antivirus Connector:

Steps

1. The Antivirus Connector searches for the Antivirus Connector client certificate and the certificate authority (CA) certificate for the NetApp server in the directory path from where the Antivirus Connector runs the install directory. Copy the certificates into this fixed directory path.
2. Embed the client certificate and its private key in the PKCS12 format and name it "AV_client.P12".
3. Ensure the CA certificate (along with any intermediate signing authority up to the root CA) used to sign the certificate for the NetApp server is in the Privacy Enhanced Mail (PEM) format and named "Ontap_CA.pem". Place it in the Antivirus Connector install directory. On the NetApp ONTAP system, install the CA certificate (along with any intermediate signing authority up to the root CA) used to sign the client certificate for the Antivirus Connector at "ONTAP" as a "client-ca" type certificate.

Copyright information

Trademark information