SOPHOS

Security made simple.

Sophos Anti-Virus for NetApp Storage Systems user guide

Product version: 3.0
Document date: October 2016

Contents

1 About this guide

This guide explains how to:

- Install Sophos Anti-Virus for NetApp on a Windows computer to provide offboard antivirus scanning.

- Manage Sophos Anti-Virus for NetApp from a Microsoft Management Console (MMC) snap-in.

The guide applies to filers that are running Data ONTAP 7-Mode or Clustered Data ONTAP.

If you want to upgrade Sophos Anti-Virus for NetApp, version 1 in a Data ONTAP 7-Mode environment, download and run the installer as described in Installing Sophos Anti-Virus for NetApp (page 12).

Sophos documentation is published at www.sophos.com/en-us/support/documentation/.

Note: This guide refers to a virtual storage server as a vserver. NetApp now uses Storage Virtual Machines (SVMs) instead of vservers. See https://library.netapp.com/ecmdocs/ECMP1354558/html/GUID-E643017F-041B-4ECC-BEA1-E4D80E26A47E.html for more information on SVMs.

Note: Some of the links in this guide lead to information maintained by third parties and are provided for your convenience. Although we try to review the accuracy of the links periodically, the links may change without our knowledge.

# 2 About Sophos Anti-Virus for NetApp Storage Systems

What is Sophos Anti-Virus for NetApp Storage Systems for?

Sophos Anti-Virus for NetApp Storage Systems provides on-access scanning of files held on a Network Appliance™ filer running the NetApp® Data ONTAP® storage operating system.

How does it work?

Sophos Anti-Virus for NetApp uses the scanning capabilities of Sophos Endpoint Security and Control to scan the files. You install and run Sophos Endpoint Security and Control and Sophos Anti-Virus for NetApp on a Windows computer that will provide virus scanning. In this guide, this computer is referred to as the *antivirus server*.

When a workstation attempts to access a file held on a Network Appliance filer, Endpoint Security and Control intercepts the file and scans it. If the file is found to be clean, access to the file is granted. If the file is infected, access is denied.
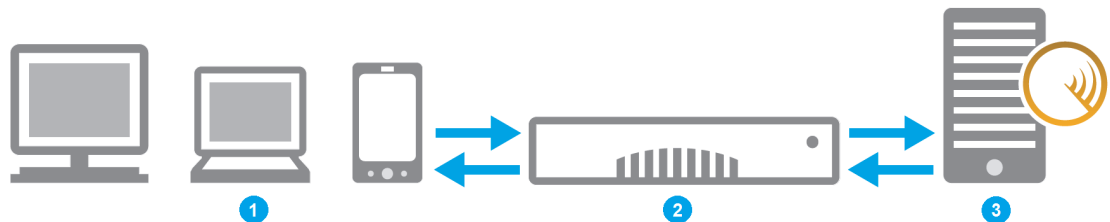
1 Endpoint devices

2 Filer

3 Antivirus scanning server protected by Sophos Endpoint Security and Control

You can use Sophos Anti-Virus for NetApp for scanning filers that are running Data ONTAP 7-Mode or Clustered Data ONTAP. It can work in a multi-filer and multi-AV machine modes.

How is it managed?

You manage Sophos Anti-Virus for NetApp from an MMC snap-in, which can be on the antivirus server itself, or on a different computer.

3 System requirements

In a Data ONTAP 7-Mode environment, Sophos Anti-Virus for NetApp runs on Windows 2003 R2 and later.

In a Clustered Data ONTAP environment, Sophos Anti-Virus for NetApp runs on Windows 2008 and later.

For a full list of system requirements, go to the system requirements page on the Sophos website (http://www.sophos.com/en-us/support/knowledgebase/118633.aspx).

You must have internet access in order to download the installation software from the Sophos website.

4 Before you install Sophos Anti-Virus for NetApp

Before installing Sophos Anti-Virus for NetApp, you need to do the following:

- Install Endpoint Security and Control (antivirus component only) on the computer you want to use as an antivirus server.
- Make sure Endpoint Security and Control is configured for use with the Network Appliance filer.
- Configure Windows security options on the antivirus server.
- Configure your NetApp Storage System:
  - In a Data ONTAP 7-Mode environment, make sure vscan is enabled on the Network Appliance filer.
  - In a Clustered Data ONTAP environment, install Clustered Data ONTAP Antivirus Connector on an antivirus server and create a scanner pool.

4.1 Installing Endpoint Security and Control

Before you install Sophos Anti-Virus, you must install Sophos Endpoint Security and Control on the computer that you want to use as an antivirus server, to provide virus scanning.

If Endpoint Security and Control has already been installed on the computer, go straight to Configuring Endpoint Security and Control for use with a Network Appliance filer (page 7).

Otherwise, do one of the following:

- Use Sophos Enterprise Console to create a managed installation of Endpoint Security and Control (antivirus component only).
- Create a standalone installation of Endpoint Security and Control (antivirus component only).

4.1.1 Create a managed installation

Refer to the *Enterprise Console quick startup guide*, which is available at http://www.sophos.com/en-us/support/documentation/enterprise-console.aspx.

Put the antivirus server in a separate Enterprise Console group, so that you can apply a new antivirus policy to just that computer.

Now go to Configuring Endpoint Security and Control for use with a Network Appliance filer (page 7).

4.1.2 Create a standalone installation

Refer to the *Endpoint Security and Control standalone startup guide* , which is available at
http://www.sophos.com/en-us/support/documentation/endpoint-security-and-control-for-windows.aspx.

After you have installed Endpoint Security and Control, configure it for use with a Network Appliance
filer.

4.2 Configuring Endpoint Security and Control for use with a Network Appliance filer

You must configure Endpoint Security and Control to:

- Scan files when they are copied, moved or opened (on read).

- Scan files with an unknown filename extension.

- Scan remote files.

- Move all infected files to a quarantine folder.

- Move all suspicious files to a quarantine folder.

- Not display messages on the screen when scanning files.

How you do this depends on whether you have a *managed* installation of Endpoint Security and
Control or a *standalone* installation.

4.2.1 Configure a managed installation

1. At the computer that is running Enterprise Console, if Enterprise Console is not already open,
   click **Start** > **All Programs** > **Sophos** > **Enterprise Console**.
2. Create a new antivirus policy to contain settings for the antivirus server.
3. Double-click the policy to edit it.
4. In the **Anti-Virus and HIPS Policy** dialog box, in the **On-access scanning** panel, beside
   Enable on-access scanning, click **Configure**.
5. In the **On-access scan settings** dialog box, on the **Scanning** tab, ensure that the **Read** check
   box is selected. Otherwise, no files are scanned.
6. Click the **Extensions** tab. Click **Add**. In the extensions list box, type `???` and press ENTER.
7. Click the **Windows Exclusions** tab. Ensure that the **Exclude remote files** check box is not
   selected.
8. Click the **Cleanup** tab.
9. Ensure that the **Automatically clean up items that contain a virus/spyware** check box is
   cleared. Click **Deny access and move to (enter a full UNC path)**. Using the **Browse** button,
   specify the path of the folder to which infected files should be moved.

   The folder must be on the antivirus server, and should preferably be accessible to antivirus
   administrators only.

10. Under **Suspicious files**, click **Deny access and move to (enter a full UNC path)**. Using the **Browse** button, specify the path of the folder to which suspicious files should be moved.

    The folder must be on the antivirus server, and should preferably be accessible to antivirus administrators only.

11. Click **OK** to close the **On-access scan settings** dialog box.

12. In the **Anti-Virus and HIPS Policy** dialog box, click **Messaging**.

13. In the **Messaging** dialog box, on the **Desktop Messaging** tab, clear the **Enable desktop messaging** check box. Click **OK**.

14. Click **OK** to close the **Anti-Virus and HIPS Policy** dialog box.

15. Click the policy and drag it onto the group that contains the antivirus server. When prompted, confirm that you want to continue.

    The policy settings will be applied to Endpoint Security and Control on the antivirus server.

You have configured Endpoint Security and Control for use with a filer.

If the antivirus server is running Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2, you must configure the Windows security options. See .

4.2.2 Configure a standalone installation

1. At the antivirus server, if Endpoint Security and Control is not already open, in the notification area, right-click the Endpoint Security and Control icon, and then click **Open Sophos Endpoint Security and Control**.

2. In the **Sophos Endpoint Security and Control** window, on the **Configure** menu, point to **Anti-Virus**, and then click **On-access scanning**.

3. In the **On-access scan settings for this computer** dialog box, on the **Scanning** tab, ensure that the **Read** check box is selected. Otherwise, no files are scanned.

4. Click the **Extensions** tab. Click **Add**. In the extensions list box, type **???** and press ENTER.

5. Click the **Exclusions** tab. Ensure that the exclusions list does *not* contain **All remote files**.

6. Click the **Cleanup** tab.

7. Ensure that the **Automatically clean up items that contain virus/spyware** check box is cleared. Click **Deny access and move to**. Using the **Browse** button, specify the path of the folder to which infected files should be moved.

    The folder must be on this computer, and should preferably be accessible to antivirus administrators only.

8. Under **Suspicious files**, click **Deny access and move to**. Using the **Browse** button, specify the path of the folder to which suspicious files should be moved.

    The folder must be on this computer, and should preferably be accessible to antivirus administrators only.

9. Click **OK** to close the **On-access scan settings for this computer** dialog box.

10. On the **Configure** menu, point to **Anti-Virus**, and then click **Messaging**.

11. In the **Messaging** dialog box, on the **Desktop messaging** tab, clear the **Enable desktop messaging** check box. Click **OK**.

You have configured Endpoint Security and Control for use with a filer.

If the antivirus server is running Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2, you must configure the Windows security options.

Otherwise, go straight to Installing Sophos Anti-Virus for NetApp (page 12).

4.3 Configure security options on Windows Server 2008 or later

If the antivirus server is running Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2, you must configure the Windows security options.

1. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Local Security Policy**.
2. In the **Local Security Policy** window, in the left-hand pane, double-click the **Local Policies** folder to expand it. Select **Security Options**.
3. Enable the option **Network access: Let Everyone permissions apply to anonymous users**.
4. Restart the computer.

You have configured the Windows Server security options.

Now configure your NetApp Storage System.

4.4 Configuring the NetApp Storage System

4.4.1 Configure a Data ONTAP 7-Mode environment

Before installing Sophos Anti-Virus for NetApp to scan a Network Appliance filer running Data ONTAP 7-Mode, make sure vscan is enabled.

1. To check if vscan is enabled, on the filer console at the command prompt type the following:

   `vscan`

   The console output will show whether virus scan is enabled or disabled.
2. If vscan is disabled, enable it. At the command prompt, type:

   `vscan on`

For more information, at the command prompt type:

`vscan help`

Alternatively, refer to your Network Appliance filer documentation.

4.4.2 Configure a Clustered Data ONTAP environment

Before installing Sophos Anti-Virus for NetApp to scan a Network Appliance filer running Clustered Data ONTAP, make sure that Clustered Data ONTAP Antivirus Connector is installed and running and create a scanner pool.

Note: For antivirus configuration instructions for Clustered Data ONTAP, see the NetApp Clustered Data ONTAP 8.2 Antivirus Configuration Guide.

For antivirus best practices for Clustered Data ONTAP, see the NetApp Best Practices Guide for Clustered Data ONTAP 8.2 Windows File Services, the Antivirus Architecture section.

4.4.2.1 Configure Clustered Data ONTAP Antivirus Connector

1. On the antivirus server, install Clustered Data ONTAP Antivirus Connector, as described in the NetApp Clustered Data ONTAP 8.2 Antivirus Configuration Guide, and make sure that it is running.

   The minimum operating system requirement for Cluster-Mode scanning (Clustered Data ONTAP Antivirus Connector) is Windows Server 2008.

   Clustered Data ONTAP Antivirus Connector and Sophos Anti-Virus communicate with each other on the loopback address (127.0.0.1).

   Note: When you create a scanner pool, you must add the service account credentials for running the Clustered Data ONTAP Antivirus Connector service as the privileged user in the scanner pool. Same service account must be used to run the antivirus scanning service.

2. To configure the connector, right-click the **Configure Data ONTAP Management LIFs for Polling** application shortcut created on the desktop during the installation and select **Run as administrator**. This will open the **Configure Data ONTAP Management LIFs for Polling** configuration dialog box.

3. Configure Data ONTAP management LIFs.

   Credentials used for polling must have at least read access to the network interface. You might want to use a separate user to poll the Data ONTAP management LIFs for security purposes. It is preferable to use the "cluster admin" or "vsadmin" accounts.

4. Click **Test** to verify the connectivity and authenticate the connection.

4.4.2.2 Create a scanner pool

1. Create a scanner pool. On the Cluster-Mode filer console at the command prompt type the following:

   ```
   vserver vscan scanner-pool create -vserver vs1 -scanner-pool SP1
   -servers <antivirus server IP address> -privileged-users
   netapp\administrator
   ```

   In this command:

   - **vs1** is the name of the Vserver on which you want to create a scanner pool.

   - **SP1** is the name of the scanner pool.

   - **<antivirus server IP address>** is the IP address of the antivirus server which is allowed to connect to the Vserver.

   - **netapp\administrator** is the privileged user who can connect to the Vserver.

   You must add the service account credentials for running the Clustered Data ONTAP Antivirus Connector service as the privileged user in the scanner pool. Same service account must be used to run the antivirus scanning service.

2. Apply the scanner pool configuration.

   ```
   vserver vscan scanner-pool apply-policy -vserver vs1 -scanner-pool
   SP1 -scanner-policy primary
   ```

3. Enable vscan.

   ```
   vserver vscan enable -vserver vs1
   ```

4. To check the scanner pool configuration, type:

   ```
   vserver vscan scanner-pool show
   ```

5 Installing Sophos Anti-Virus for NetApp

Sophos Anti-Virus for NetApp has two components:

- The Sophos Anti-Virus for NetApp service.

- An MMC snap-in, which is used to manage the Sophos Anti-Virus for NetApp service.

You can install the components on the same computer, or on separate computers.

5.1 Download the installer

This section assumes that you have a MySophos account and that you have associated your license credentials with it. If you need help, go to www.sophos.com/en-us/support/knowledgebase/111195.aspx.

1. At the Windows computer on which you want to install Sophos Anti-Virus for NetApp or another computer that has internet access, go to www.sophos.com/en-us/support/downloads.aspx.

2. Type your MySophos username and password.

   You see a web page that shows your license or licenses.

3. Under your license name, find the **Groupware and Network Storage Protection** downloads. Download the Anti-Virus for Network Storage installer.

4. Ensure that the installer is in a location that can be accessed from the computer on which you want to install Sophos Anti-Virus for NetApp.

5.2 Run the installer

At the Windows computer on which you want to install Sophos Anti-Virus for NetApp, you must log on as an administrator.

If you are installing the Sophos Anti-Virus for NetApp service (that is, if this computer will be an antivirus server), this section assumes you have installed and configured Sophos Endpoint Security and Control (as explained in Before you install Sophos Anti-Virus for NetApp (page 6)).

If you are installing the MMC snap-in, this section assumes that this computer is running MMC version 1.2 or later.

If you are upgrading from Sophos Anti-Virus for NetApp, version 1, the Sophos Anti-Virus for NetApp, version 3 installer will uninstall Sophos Anti-Virus for NetApp, version 1 and preserve your settings, such as antivirus server and filer names.

1. Locate the installer that you downloaded and double-click it.

2. In the installer window, click **Install**.

   A wizard guides you through installation.

3. On the **Welcome** page, click **Next**.

4. On the **End-user licence agreement** page, read the licence agreement. If you accept it, click **I accept the terms of the licence agreement**, and click **Next**.

5. On the **Custom setup** page, select the features to install.

   The selection depends on the use you want to make of this computer.

   - To use the computer as an antivirus server and to manage Sophos Anti-Virus for NetApp from MMC, click **Next** and continue to step 6.

   - To use the computer only as an antivirus server, click the drop-down arrow next to **MMC snap-in**. Select **Entire feature will be unavailable**. Click **Next** and continue to step 6.

   - To use the computer only to manage Sophos Anti-Virus for NetApp from MMC, click the drop-down arrow next to **Anti-virus service**. Select **Entire feature will be unavailable**. Click **Next** and go straight to step 8.

6. On the **Filer mode** page, select your Data ONTAP environment—Data ONTAP 7-Mode or Clustered Data ONTAP. Click **Next**.

7. On the **Account information** page, enter the details of an account in the domain containing the filer that this computer is serving.

   For Data ONTAP 7-Mode, the account must have Administrator or Backup Operator level rights on the filer.

   For Clustered Data ONTAP, the account must be a privileged user in the scanner pool.

   Click **Next**.

   Note: If the installation wizard then displays a warning that the account details are invalid, ensure that the local security setting **Network access: Sharing and security model for local accounts** is set to **Classic - local users authenticate as themselves**.

8. On the **Ready to install** page, click **Install** to begin the installation.

9. On the last page, click **Finish**.

You have installed Sophos Anti-Virus for NetApp.

If you want to install the Sophos Anti-Virus for NetApp service and/or the MMC snap-in on another computer, repeat this section.

You must ensure that the filer has been configured to send files for virus scanning. To find out how to do this, refer to the Data ONTAP documentation.

Note: To ensure that antivirus scanning can be carried out if the antivirus server is unavailable (for example, while Endpoint Security and Control is updating), install Endpoint Security and Control and Sophos Anti-Virus for NetApp on another computer as well. On a filer running Data ONTAP 7-Mode, define that computer as a secondary server. (To find out how to do this, refer to the Data ONTAP documentation.) Then, the secondary server can handle scanning requests if the primary server is unavailable.

On Clustered Data ONTAP, it is recommended that you add at least two antivirus servers to a scanner pool. It is also recommended that you create a backup scanner pool and assign a secondary scanner pool policy to it. Then, if none of the antivirus servers in the primary scanner pool are available, the secondary scanner pool will become active.

For information about how to manage Sophos Anti-Virus for NetApp from MMC, continue to the next section.

6 Managing Sophos Anti-Virus for NetApp from MMC

This section describes how to:

- Snap in Sophos Anti-Virus for NetApp to MMC.

- Add an antivirus server or servers to MMC.

- Add a filer or filers that will be scanned by an antivirus server.

- View antivirus server statistics.

- Switch Sophos Anti-Virus for NetApp to Cluster-Mode scanning.

- Stop or start the Sophos Anti-Virus for NetApp service on an antivirus server.

For more information about the options and statistics available in the **Properties** dialog box for an antivirus server in MMC, as well as Sophos Anti-Virus for NetApp registry keys, see knowledgebase article 58736 (http://www.sophos.com/en-us/support/knowledgebase/58736.aspx).

6.1 Snap in Sophos Anti-Virus for NetApp to MMC

This section assumes you installed the Microsoft Management Console (MMC) snap-in for Sophos Anti-Virus for NetApp during the Sophos Anti-Virus for NetApp installation procedure.

1. At the computer where you installed the MMC snap-in, double-click the **Sophos AV Machines** shortcut on the desktop.

   Alternatively, at the taskbar, click **Start**, and then click **Run**. If the computer is running a 32-bit version of Windows, in the **Run** dialog box, type `mmc`. Otherwise, type `mmc /32`. Click **OK**.

2. In the **Console1** console, on the **File** menu, click **Add/Remove Snap-in**.

   For MMC versions earlier than 2.0, this command is on the **Console** menu.

3. If the computer is running Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Server 2012, or Windows Server 2012 R2, in the **Add or Remove Snap-ins** dialog box, in the **Available snap-ins** list box, select **Sophos Anti-Virus for NetApp Storage Systems**. Click **Add**.

   Otherwise, in the **Add/Remove Snap-in** dialog box, on the **Standalone** tab, click **Add**. In the **Add Standalone Snap-in** dialog box, in the **Available Standalone Snap-ins** list box, select Sophos Anti-Virus for NetApp Storage Systems. Click **Add**, then **Close**.

4. Click **OK** to return to the **Console1** console. On the **File** menu, click **Save**. In the **Save As** dialog box, choose a location and type a filename for the console settings. Click **Save**.

For MMC versions earlier than 2.0, the **Save** command is on the **Console** menu.
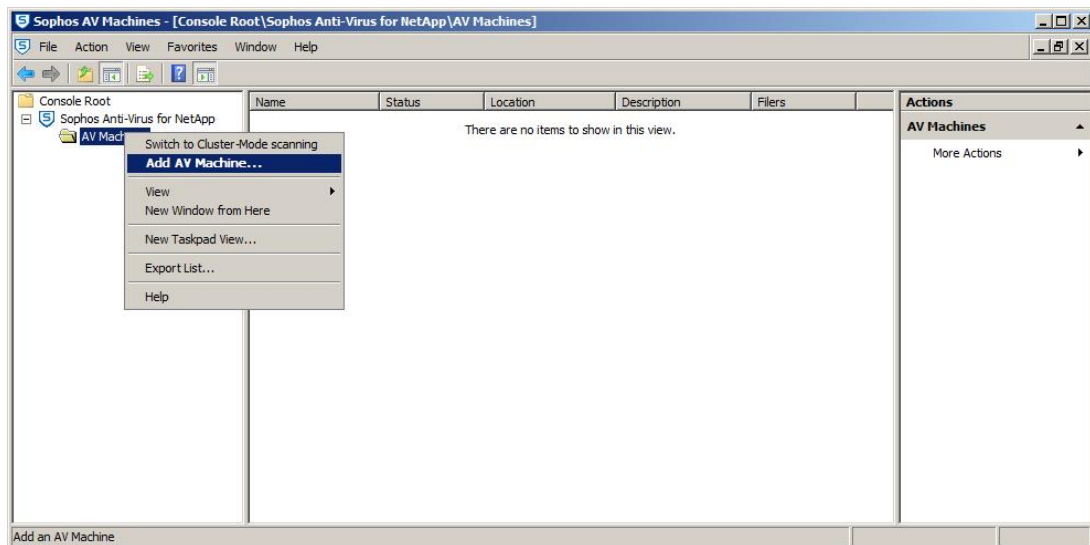
You have snapped in Sophos Anti-Virus for NetApp to MMC.

Now add an antivirus server to MMC.
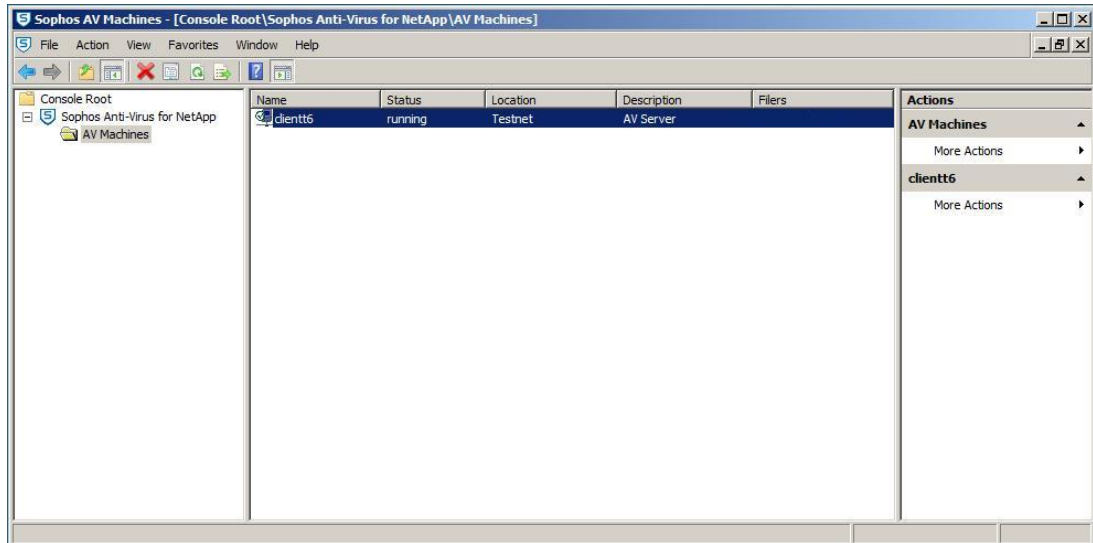
6.2 Add an antivirus server to MMC

If you have installed the Sophos Anti-Virus for NetApp service on this computer or other computers, you must add these to MMC to enable it to manage Sophos Anti-Virus for NetApp on these computers.

1. In the console tree, double-click **Sophos Anti-Virus for NetApp**. Click the **AV Machines** folder. On the **Action** menu, click **Add AV Machine**.

2. In the **Add Sophos Anti-Virus server** dialog box, click **Browse**.
3. In the **Browse for Computer** dialog box, locate the antivirus server and click **OK**.

15

4. In the **Add Sophos Anti-Virus server** dialog box, type a location and description for the antivirus server if you wish, and click **OK**. The antivirus server is shown in the right-hand pane of the **AV Machines** console, with the Sophos Anti-Virus for NetApp service running.
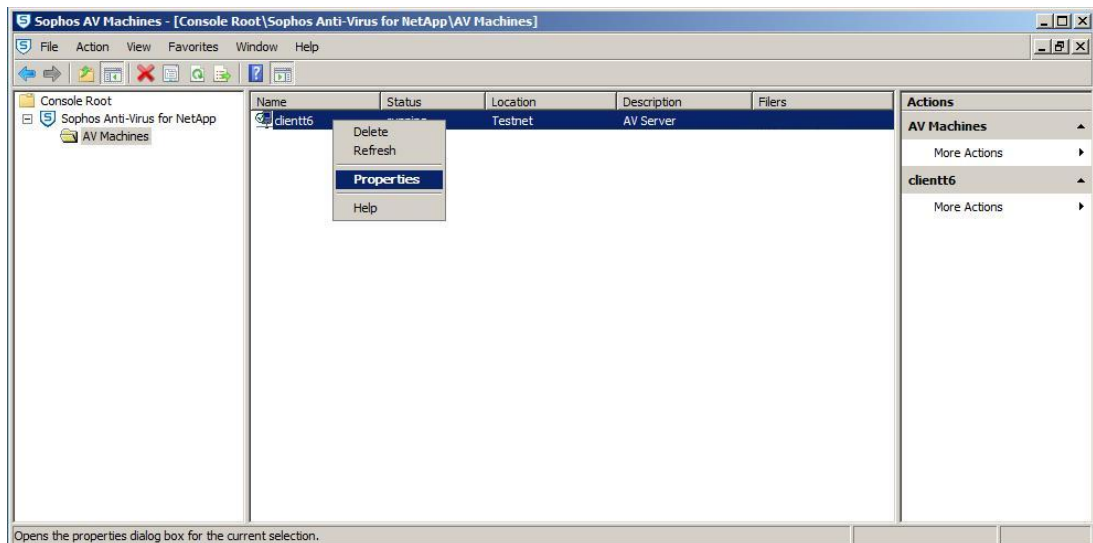

You have added an antivirus server to MMC.

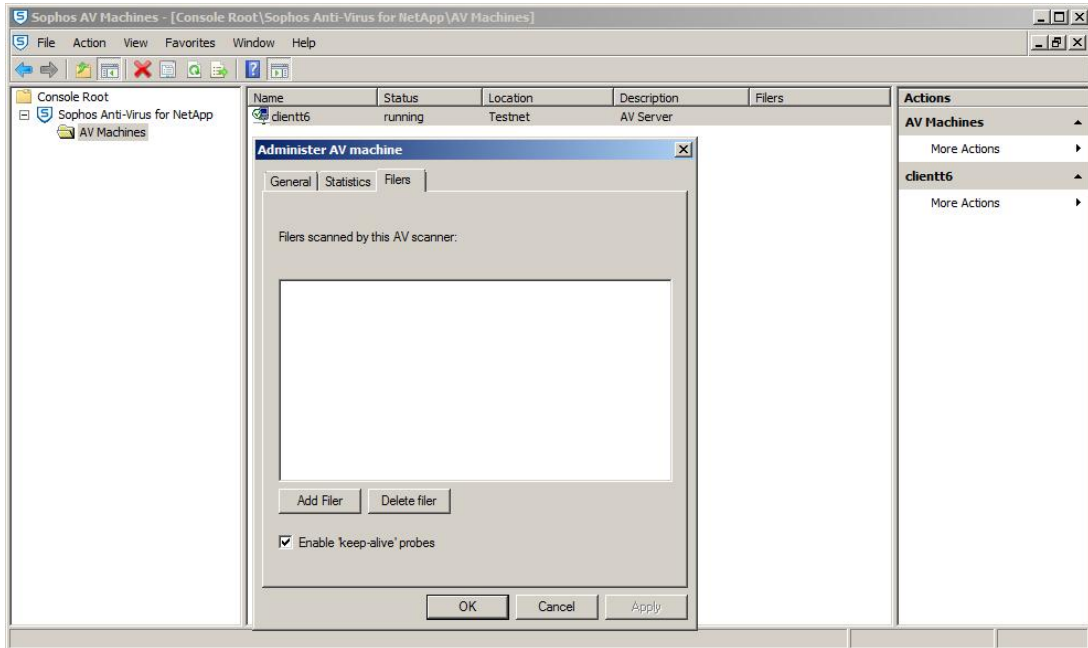To add another antivirus server, repeat the above steps.

6.3 Add a filer for scanning by the antivirus server

Specify which filer or filers will be scanned by the antivirus server.

1. In the right-hand pane of the **AV Machines** console, right-click the name of the antivirus server, and then click **Properties**.

2. In the **Administer AV machine** dialog box, click the **Filers** tab, and then click **Add Filer**.

Fill in the filer details. Repeat to add another filer.

6.4 View antivirus server statistics

To view antivirus server statistics:

1. In the right-hand pane of the **AV Machines** console, right-click the name of the antivirus server, click **Properties**, and then click the **Statistics** tab.
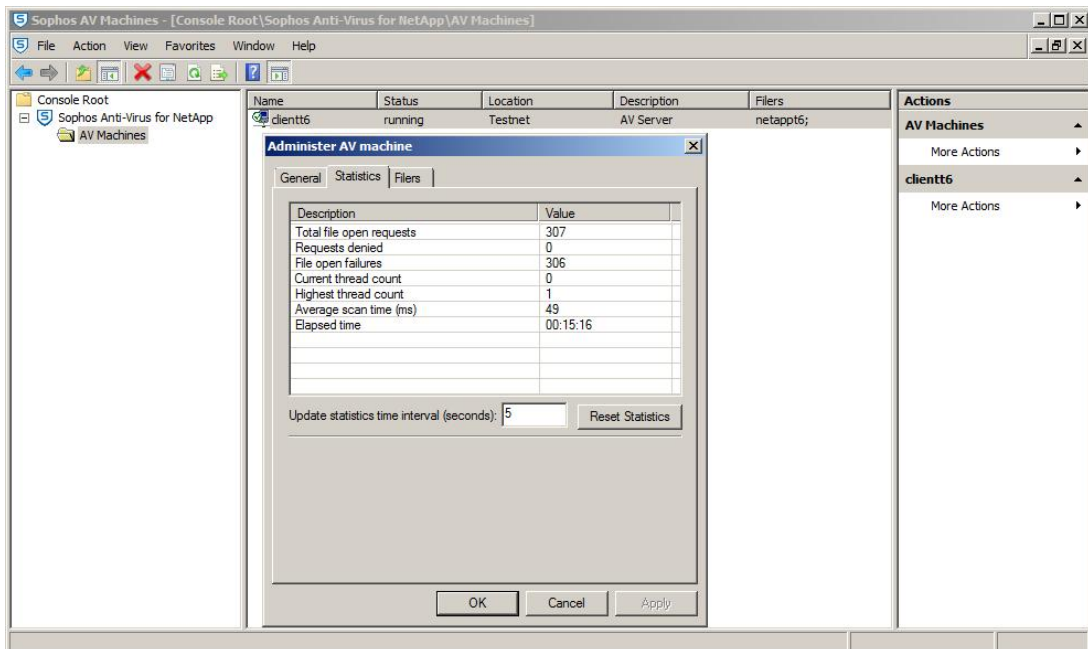
6.5 Switch Sophos Anti-Virus for NetApp to Cluster-Mode scanning

Before switching to Cluster-Mode scanning, make sure that Clustered Data ONTAP Antivirus Connector is installed and running and that you have created a scanner pool. See Configure a Clustered Data ONTAP environment (page 9).

Important: Switching **Sophos Anti-Virus for NetApp** to Cluster-Mode scanning cannot be undone. After you have switched to Cluster-Mode scanning, you can go back to 7-Mode scanning only by uninstalling and then reinstalling **Sophos Anti-Virus for NetApp** and choosing the Data ONTAP 7-Mode option during the installation.

1. In the MMC console tree, double-click **Sophos Anti-Virus for NetApp**. Click the **AV Machines** folder. On the **Action** menu, click **Switch to Cluster-Mode scanning**.
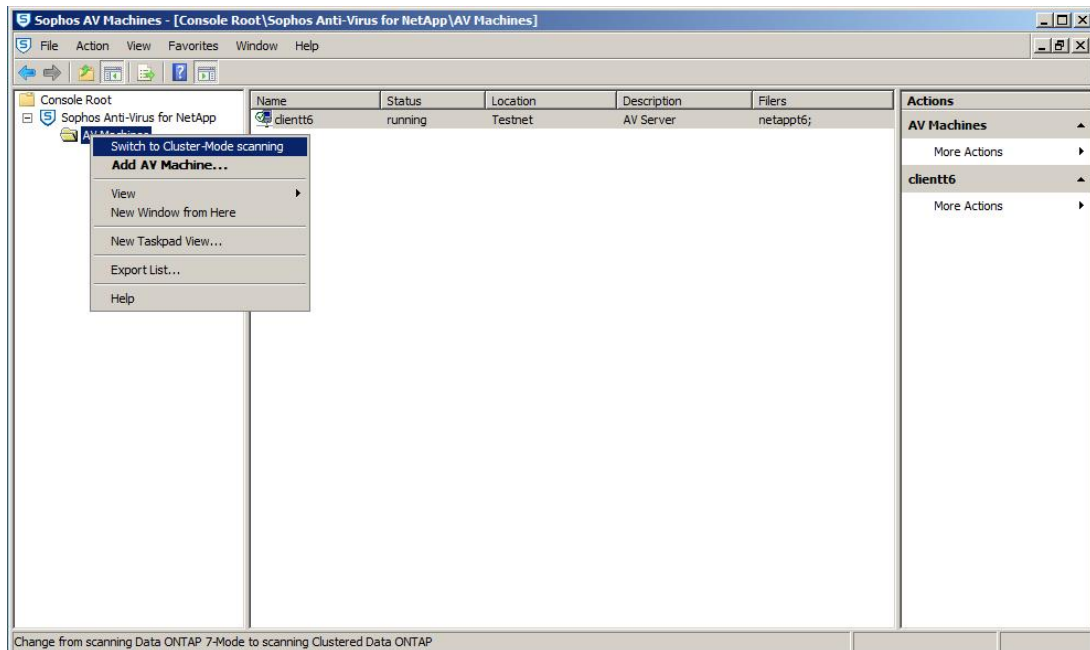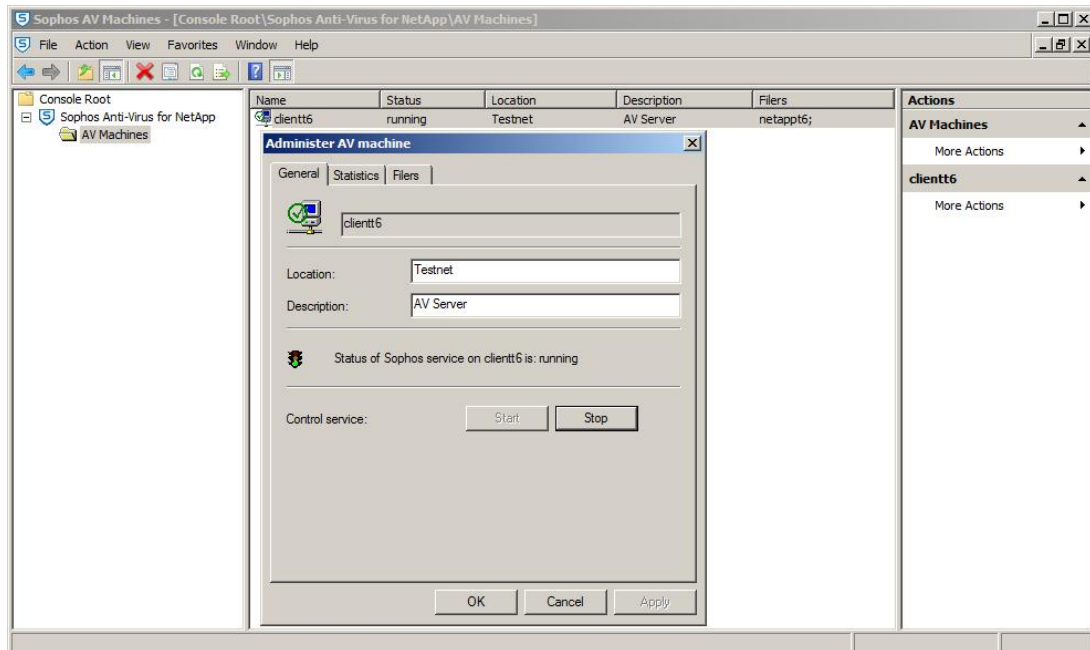

6.6 Stop the Sophos Anti-Virus for NetApp service on an antivirus server

If you need to stop the Sophos Anti-Virus for NetApp service on an antivirus server:

1. In the right-hand pane of the **AV Machines** console, right-click the name of the antivirus server, and then click **Properties**.

2. In the **Administer AV machine** dialog box, on the **General** tab, click **Stop**, and then click **OK**.

In the right-hand pane of the console, you should see that the service is not running on the selected antivirus server.

6.7 Start the Sophos Anti-Virus for NetApp service on an antivirus server

1. In the right-hand pane of the **AV Machines** console, right-click the name of the antivirus server, and then click **Properties**.

2. In the **Administer AV machine** dialog box, on the **General** tab, click **Start**. Click **OK**.

In the right-hand pane of the console, you should see that the service is running on the selected antivirus server.

7 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.

- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.

- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.

- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

8 Legal notices