SOPHOS

Security made simple.

Sophos Virtualization Scan Controller user guide

Product version: 2.0

Document date: October 2013

Contents

1 About this guide

The guide describes how to install and use the Virtualization Scan Controller 2.0 add-on tool for Sophos Enterprise Console 5.2 and later.

It is assumed that you are familiar with and already using Sophos Enterprise Console version 5.2 or later.

Please note that Virtualization Scan Controller 2.0 works with Enterprise Console 5.2.1 out of the box, but if you want to use it with Enterprise Console 5.2.0, you will need to perform certain prerequisite steps. For instructions, see *Appendix C: Prerequisite steps for Enterprise Console 5.2.0* (section 18).

Sophos documentation is published at *http://www.sophos.com/en-us/support/documentation.aspx*.

2 What is Virtualization Scan Controller?

Virtualization Scan Controller is a tool for managing scheduled scans of virtual computers.

You use the tool to ensure that scheduled scans on different computers are run in sequence, rather than all at the same time. This reduces the impact on your virtualization server.

The tool:

- Lets you manage scans with a single configuration file.
- Lets you specify initially how much time is allowed for a scan to be run on one computer before a scan starts on the next.
- Learns from previous scanning cycles how much time should be allowed for each scan.
- Lets you specify how often each computer can be scanned, how many can be scanned at the same time and other parameters.

Important: The tool does not let you specify which files or file types are scanned. This version of the product always runs a scan of the "Full system scan" type.

3 Where do I install it?

You install Virtualization Scan Controller alongside Sophos Enterprise Console (SEC) management server.

The computer(s) where you install it depends on the type of SEC installation you have:

If you have all the SEC components on a single server ("standalone" SEC), you install Virtualization Scan Controller on that server.

If you have some or all the SEC components on different servers ("distributed" SEC), you install:

- The Virtualization Scan Controller service on the computer where you have the Sophos management server.
- The Virtualization Scan Controller database on the computer where you have the Sophos management database.

This guide describes how to do either type of installation.

4 What are the key steps?

To install and use Virtualization Scan Controller, you carry out these steps:

- Download the installer.
- If you use Enterprise Console 5.2.0, before you install Virtualization Scan Controller, you must perform the prerequisite steps described in *Appendix C: Prerequisite steps for Enterprise Console 5.2.0* (section 18).
- Install Virtualization Scan Controller.
- Register Virtualization Scan Controller as a Windows service (optional).
- Create a configuration file.
- Apply the configuration.
- Start Virtualization Scan Controller.

These steps are described in the sections that follow.

5 What accounts do I need?

The commands **install** and **uninstall** should be run in the context of an account that has administrative rights to the Enterprise Console database. The installation process creates database objects used by Virtualization Scan Controller in a database schema with the name **vmscan**.

The commands **run** and **configure** should be run in the context of an account that has been granted EXECUTE and SELECT rights to the schema. Members of the **Sophos DB Admins** group are granted these rights by default.

6 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*

To download the installer:

1. 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 licenses.

3. Under your license name, find the **Console** downloads. Download the Virtualization Scan Controller installer.

If you use Enterprise Console 5.2.0, go to *Appendix C: Prerequisite steps for Enterprise Console 5.2.0* (section 18).

7 Install Virtualization Scan Controller

Important: Make sure the Virtualization Scan Controller computer and the endpoint computers have their clocks synchronized.

This section assumes that you have a standalone installation of Enterprise Console.

Note: If you have a distributed installation (Enterprise Console components on different servers), see *Appendix: Install with a distributed console* (section 16).

To install Virtualization Scan Controller:

1. Extract the Virtualization Scan Controller files to the computer where you have Sophos Enterprise Console installed, if you haven't done so already.
2. Open a command prompt window and change to the directory to which you extracted the Virtualization Scan Controller files.
3. Use a text editor to open the file **SavScanController.exe.config** and check the number of the port used to communicate with the local management server. The default port number is 80. If a different port number was specified during the management server installation, the same port number should be specified in **SavScanController.exe.config**.
4. Type **`SavScanController install`** and press Enter to start the installation.

We recommend that you register Virtualization Scan Controller as a Windows service, as described in the next section.

8 Register Virtualization Scan Controller

You can register Virtualization Scan Controller as a Windows service. If you do this, the Virtualization Scan Controller service will:

- Start automatically every time the computer starts.
- Run without a user logged on.
- Log its activity. For information on logging, see *Logging information* (section 13).

To register as a Windows service:

1. Go to the computer where you have the Sophos management server.

   If you have a standalone installation, this is the computer on which Enterprise Console is installed.

2. Type **`SavScanController register`** and press Enter.

   The service will be registered as Sophos Scan Controller and will be configured to run as Local System.

3. If your installation of Enterprise Console prevents Local System from accessing its management server or database, or if you want to restrict the service's rights, ensure that the service can run as another user. To do this:

   a) Create a domain user account to run the Virtualization Scan Controller service. Make sure it has the **Log on as a service** right in the Group Policy for the domain.

   b) Edit the sub-estate settings in SEC and provide full access to the whole default estate for the user account created in step a. Assign the user to a role.

   c) Add the user account created in step a to the **Sophos Console Administrators** and **Sophos DB Admins** groups.

   In a distributed SEC installation, the **Sophos Console Administrators** group is on the computer where you have the Sophos management server, and the **Sophos DB Admins** group is on the computer where you have the Sophos management database.

   d) Make sure that the user account created in step a has read and write access to the directory where the Virtualization Scan Controller files are installed in order to write to its log files.

   e) Open **Control Panel** and double-click **Administrative Tools**. In the list of services double-click **Sophos Scan Controller** service. In the properties for **Sophos Scan Controller** service, click on the **Log on** tab and select **This account**. Click **Browse** and select the user account created in step a.

9 Create a configuration file

You must create a configuration file at the computer where you have the Sophos management server.

Note: If you have a standalone installation, this is the computer on which Enterprise Console is installed.

Create a text file that specifies which endpoint computers should be controlled by the Virtualization Scan Controller.

This file should put the computers into a number of lists. Typically, there will be one list of computers for each virtual machine host.

The following is a sample configuration file. It defines two lists. Both lists currently use the default settings.

```
[VM Host 1]
COMPUTERA.domain.name
COMPUTERB.domain.name
COMPUTERC.domain.name

[VM Host 2]
COMPUTER1.domain.name
COMPUTER2.domain.name
COMPUTER3.domain.name
...
...
COMPUTER12.domain.name
```

The following sections tell you how to:

- List computers using DNS or NetBIOS names.
- Specify how scans are run.

9.1 List computers using DNS or NetBIOS names

When you enter the computer names in the configuration file, you can use one of these name types:

- The NetBIOS name. Unless you specify otherwise, all names are treated as NetBIOS names.
- DNS name.

If you want to use DNS names, you can specify each computer name individually or, if you have a large number of computers, you can configure the file to treat all names as DNS names.

To specify an individual DNS name, use the following:

```
[VM Host 1]
dns|computer.domain.name
```

To specify that all names are DNS hostnames, add the following section at the start of the configuration file:

```
[defaults]
 Names=dns
```

Note: If you set this, you do not need to use the 'dns|' prefix for computers that are specified by their DNS hostname, but you must use a 'netbios|' prefix for computers that are specified by their NetBIOS name, as follows:

```
[VM Host 1]
netbios|COMPUTER
```

9.2 Specify how scans are run

The following settings can be specified for each list of computers in the configuration file.

Note: Any time specified in the configuration file must be in Universal Coordinated Time (UTC) 24-hour clock format.

Tip: You can test Virtualization Scan Controller's performance in a non-production environment. Edit your Enterprise Console Anti-Virus and HIPS policy to exclude folders, and use the DefaultWaitHint option (discussed in this section) to reduce the time allowed for a scan. Depending on the results, you can decide on the best settings.

- **DefaultWaitHint**

  This setting controls how much time is allowed for a scan to be run on one computer before a scan starts on the next. The value is set in minutes and must be greater than 0, the default is 30 minutes.

  This setting applies the first time that scans are run on the computers. After the first run, Virtualization Scan Controller uses information from previous runs to determine how much time is allowed.

  Example:

  ```
  [Group X]
  DefaultWaitHint=40
  COMPUTER1.domain.name
  COMPUTER2.domain.name
  COMPUTER3.domain.name
  ```

- **MaxScanTime**

  This setting defines how long Virtualization Scan Controller will allow for a scan to run successfully. The value is set in minutes and must be greater than 0, the default is 180 minutes. If a scan takes longer, Virtualization Scan Controller assumes that the scan has terminated, and starts a scan on another computer.

  Example:

```
[Group X]
MaxScanTime=120
COMPUTER1.domain.name
COMPUTER2.domain.name
COMPUTER3.domain.name
```

- **MinTimeBeforeNext**

  This setting controls how often a scan can be run on each computer in a list. The value is set in minutes, and controls the minimum time allowed between successive scans on the same computer. The value must be greater than 30, the default is 1440 minutes or 1 day.

  The MinTimeBeforeNext setting should be set to a value which is greater than the duration of the longest scan in the list. It should also, therefore, be greater than the MaxScanTime setting for the list.

  Example:

```
[Group X]
MinTimeBeforeNext=90
COMPUTER1.domain.name
COMPUTER2.domain.name
COMPUTER3.domain.name
```

- **MaxConcurrentScans**

  This setting controls the maximum number of computers in a list that can be running a scan at the same time. The value must be 1 or greater, the default is 1.

  Example:

```
[Group X]
MaxConcurrentScans=3
MinTimeBeforeNext=90
ALPHA
BETA
GAMMA
```

- **EarliestScanStart** and **LatestScanStart**

These settings control the time when scans are allowed to run. You must set the time in Universal Coordinated Time (UTC). If you want to use these settings, you must use both. If you use only one, the setting will not be applied. The default is to allow scans to run at any time of day.

Example:

```
[Group X]
EarliestScanStart=04:00
LatestScanStart=23:30
```

- **AllowedDays**

  This setting controls which days of the week scans are allowed to run. The value is a comma separated list of names. Any of the following values can be included in the list:

Name	Meaning
Sun	Sunday
Mon	Monday
Tue	Tuesday
Wed	Wednesday
Thu	Thursday
Fri	Friday
Sat	Saturday
WkE	Weekends (equivalent to 'Sat,Sun')
WkD	Weekdays (equivalent to 'Mon,Tue,Wed,Thu,Fri')

  If this setting is not specified, scans are allowed to run on any day.

  Example:

```
[Group X]
AllowedDays=Mon,Wed,Fri
```

10 Apply the configuration

Before you apply the configuration, ensure that there are no scheduled scans configured for the group containing the virtual machines that will be controlled by the Virtualization Scan Controller. This is to prevent multiple scheduled scans taking place simultaneously.

To apply the configuration, do as follows.

Note: If you update the configuration file in future, you must repeat this procedure each time.

1. Go to the computer where you have the Sophos management server.
2. Open a command prompt window and change to the directory where you have the Virtualization Scan Controller files.

   Note: The command prompt should be open in the context of an account that has sufficient rights to the database schema **vmscan**. See *What accounts do I need?* (section 5).

3. Type **`SavScanController configure <my configuration>`** where <my configuration> is the name of the configuration file you created earlier. Then press Enter to apply the configuration.

   Example: SavScanController configure settings.txt

   Errors may be reported if your configuration file lists computers that are not managed by Enterprise Console or if it uses the wrong syntax for configuration options.

You are ready to start Virtualization Scan Controller.

11 Start Virtualization Scan Controller

Before you start Virtualization Scan Controller, ensure you have applied the configuration, as described in *Apply the configuration* (section 10).

To start Virtualization Scan Controller:

1. Type **`SavScanController start`** if you have registered as a Windows service. Otherwise, type **`SavScanController run`**

   Note: If you are using the **run** command, the command prompt should be open in the context of an account that has sufficient rights to the database schema **vmscan**. See *What accounts do I need?* (section 5).

   Press Enter to start Virtualization Scan Controller.

   Note: If you make changes to the configuration later, you do not need to stop and start the service in order for the changes to take effect.

When Virtualization Scan Controller requests a scan, it works as though a full system scan of endpoint computers is started from Enterprise Console. The settings used for a full system scan depend on which Anti-Virus and HIPS policies apply. The following Anti-Virus and HIPS settings are used:

- Authorizations.
- On-demand exclusions.
- On-demand extensions.
- All other default scheduled scanning options.

12 Stop Virtualization Scan Controller

To stop Virtualization Scan Controller:

1. Type **`net stop SavScanController`** if you have registered as a Windows service. Otherwise, press Ctrl+C.

13 Logging information

When you are running the Virtualization Scan Controller, it reports activity in the command prompt window.

If you are running Virtualization Scan Controller as a Windows service, it reports activity in the SavScanController.log file. The log file will be created in the directory that has the SavScanController.exe file.

If the log file reaches its maximum size, the file is renamed to SavScanController.log.1, SavScanController.log.2 and so on. Up to 4 old log files are saved.

14 Troubleshooting

You can use SavScanController in diagnostic mode. The '-d' and '-t' command line switches enable extended debugging and tracing logging information. They can be used with any of the commands.

Examples:

SavScanController -d -t register

SavScanController -d -t install

SavScanController start -d -t

15 Uninstall Virtualization Scan Controller

Uninstallation does not delete the SEC database. It will only undo the changes made by the Virtualization Scan Controller.

Uninstalling also unregisters the Virtualization Scan Controller service.

Note: If you just wish to unregister the Virtualization Scan Controller as a Windows service you can use the command **`SavScanController unregister`**

This section assumes that you have a standalone installation of Enterprise Console.

Note: If you have a distributed installation (Enterprise Console components on different servers), see *Appendix: Uninstall with a distributed console* (section 17).

To uninstall Virtualization Scan Controller:

1. Open a command prompt window at the directory where you have the Virtualization Scan Controller files.
2. Ensure Virtualization Scan Controller is not running on the computer.

   To stop it, type **`net stop SavScanController`** if you have registered as a Windows service. Otherwise, press Ctrl+C.
3. Type **`SavScanController uninstall`** and press Enter.

16 Appendix A: Install with a distributed console

Important: Make sure the Virtualization Scan Controller computer and the endpoint computers have their clocks synchronized.

This section assumes that you have a distributed installation of Enterprise Console.

Note: If you have a standalone installation (all Enterprise Console components on a single server), see *Install Virtualization Scan Controller* (section 7).

Installation involves two steps:

- Install the service.
- Install the database.

16.1 Install the service

To install the Virtualization Scan Controller service:

1. Extract the Virtualization Scan Controller files to the computer where you have the Sophos management server.
2. Open a command prompt window and change to the directory to which you extracted the Virtualization Scan Controller files.
3. Type **`SavScanController install`** and press Enter.

   The service is installed. An error message indicates that you now need to install the Virtualization Scan Controller database on the computer where you have the Sophos management database. Make a note of the **Database server** and **Database name** shown in the message.

   ```
   Error: Sophos Enterprise Console is configured to use a remote database.

   Please refer to the Virtualization Scan Controller User Guide.

   You will need the following information:

   Database server: Hostname\Instance

   Database name: Database
   ```

16.2 Install the database

To install the Virtualization Scan Controller database:

1. Go to the computer where you have the Sophos management database and extract the Virtualization Scan Controller files.

2. Open a command prompt window and change to the directory to which you extracted the Virtualization Scan Controller files.
3. Type **`SavScanController install <Hostname>\<Instance> <Database>`**

   Make sure you enter the *Hostname**Instance* and *Database* values as they were displayed on the computer where you have the Sophos management server.

   Press Enter to create the required tables in the database for Virtualization Scan Controller.

You should now continue to set up Virtualization Scan Controller in the same way as for a standalone installation of Enterprise Console. Go to *Register Virtualization Scan Controller* (section 8).

17 Appendix B: Uninstall with a distributed console

Uninstallation does not delete the SEC database. It will only undo the changes made by the Virtualization Scan Controller.

Uninstalling also unregisters the Virtualization Scan Controller service.

Note: If you just wish to unregister the Virtualization Scan Controller as a Windows service you can use the command **`SavScanController unregister`**

This section assumes that you have a distributed installation of Enterprise Console.

Note: If you have a standalone installation of Enterprise Console, see *Uninstall Virtualization Scan Controller* (section 15).

To uninstall Virtualization Scan Controller:

1. On the computer where you have the Sophos management server, open a command prompt window at the directory where you have the Virtualization Scan Controller files.
2. Ensure Virtualization Scan Controller is not running on the computer.

   To stop it, type **`net stop SavScanController`** if you have registered as a Windows service. Otherwise, type Ctrl+C.
3. Type **`SavScanController uninstall`** and press Enter.
4. On the computer where you have the Sophos management database, open a command prompt window and type **`SavScanController uninstall <Hostname>\<Instance> <Database>`**

   The *Hostname**Instance* and *Database* values must be the same values used for installation.

18 Appendix C: Prerequisite steps for Enterprise Console 5.2.0

If you want to use Virtualization Scan Controller with Enterprise Console 5.2.0, you must perform the following prerequisite steps.

Note: If you have already been using Virtualization Scan Controller 1.0 with Enterprise Console 5.2.0, please note that it does not work with **Auditing** enabled (*http://www.sophos.com/en-us/support/knowledgebase/119066.aspx*). Therefore, we recommend that you upgrade Virtualization Scan Controller to version 2.0.

1. If you have been using Virtualization Scan Controller 1.0:
   a) Back up your configuration file or copy it to a safe location. You can reapply it after you have upgraded Virtualization Scan Controller.
   b) Uninstall Virtualization Scan Controller 1.0 as described in *Uninstall Virtualization Scan Controller* (section 15).
2. Extract the Virtualization Scan Controller 2.0 files to the computer where you have Enterprise Console installed. By default, the files are extracted into the folder `C:\svsc_20`.
3. Download *Sophos.Management.Helpers.dll* to the Sophos Virtualization Scan Controller folder created in the previous step. For information on where to find the DLL, see *http://www.sophos.com/en-us/support/knowledgebase/119066.aspx*.
4. Open a command prompt and set the current directory to the Sophos Virtualization Scan Controller folder.
5. Run the following command:

```
%WINDIR%\Microsoft.Net\Framework\v4.0.30319\RegAsm
 Sophos.Management.Helpers.dll /tlb /codebase
```

You are now ready to install Virtualization Scan Controller 2.0. Go to *Install Virtualization Scan Controller* (section 7).

19 Technical support

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

- Visit the SophosTalk 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/*.
- Send an email to *support@sophos.com*, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

20 Legal notices