Dell CEE

Using the Common Event Enabler on Windows Platforms

Version 8.x

Part Number: 302-002-456
June 2024
Rev. 16

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Additional resources

As part of an improvement effort, revisions of the software are periodically released. Therefore, some functions described in this document might not be supported by all versions of the software currently in use. The product release notes provide the most up-to-date information on product features. If a product does not function properly or does not function as described in this document, contact your Customer Support representative.

Where to get help

Support, product, and licensing information can be obtained as described below.

Product information

For product and feature documentation or release notes, go to Online Support at dell.com/support.

Troubleshooting

For information about products, software updates, licensing, and service, go to Online Support (registration required) at: dell.com/support. After logging in, locate the appropriate product page.

Dell E-Lab Interoperability Navigator

The Dell E-Lab Interoperability Navigator is a searchable, web-based application that provides access to product interoperability support matrices. It is available on Online Support at dell.com/support. After logging in:

- Click **Diagnostics & Tools**.
- Under **Dell Data Center Tools**, click **E-Lab Navigator**.

1

Introduction

Topics:

About CEE

The Dell Common Event Enabler (CEE) framework is used to provide a working environment for the following facilities:

- Common AntiVirus Agent (CAVA), also referred to as an antivirus agent
- Common Event Publishing Agent (CEPA), which includes sub-facilities for anti-ransomware, auditing, backup, content/quota management (CQM), Common Asynchronous Publishing Service (VCAPS), and indexing

CAVA provides an antivirus solution for Dell systems (for example, the PowerStore series). It uses the industry-standard Common Internet File System (CIFS) protocol or Server Message Block (SMB) protocol in a Microsoft Windows Server environment. CAVA uses third-party antivirus software to identify and eliminate known viruses before they infect files on the system.

Antivirus software is important because the storage system is resistant to the invasion of viruses because of its architecture. The NAS server runs data access in real-time using an embedded operating system. Third parties are unable to run programs containing viruses on this operating system. Although the operating system software is resistant to viruses, Windows clients that access the storage system require virus protection. Virus protection on clients reduces the chance that they will store an infected file on the server, and protects them if they open an infected file. This antivirus solution consists of a combination of the operating system software, CAVA agent, and a third-party antivirus engine. The CAVA software and a third-party antivirus engine must be installed on a Windows Server in the domain.

CEPA is a mechanism whereby applications can register to receive event notification and context from sources such as Dell PowerStore systems. The event publishing agent delivers to the application both event notification and associated context in one message. Context may consist of file metadata or directory metadata needed to decide business policy.

The CEPA sub-facilities include:

- Auditing—A mechanism for delivering post-events to registered consumer applications in a synchronous manner. Events are delivered individually in real-time.
- Backup—A mechanism for delivering post-events in bulk mode to backup applications. A backup-specific delivery cadence is based on either a time period or a number of events.
- CARA—A mechanism for delivering post-events in bulk mode to anti-ransomware applications. A specific delivery cadence is based on either a time period or a number of events.
- CQM—A mechanism for delivering pre-events to registered consumer applications in a synchronous manner. Events are delivered individually in real-time, allowing the consumer application to exercise business policy on the event.
- Index—A mechanism for delivering events to Splunk Enterprise or the Splunk Cloud in asynchronous mode. The delivery cadence is based on either a time period or a number of events.
- MessageExchange—A mechanism for delivering post-events in asynchronous mode, when needed, without consumer use of the CEPA API. Events are published from CEPA to the RabbitMQ CEE_Events exchange. A consumer application creates a queue for itself in the exchange from which it can retrieve events.

  NOTE: RabbitMQ is supported only for Dell Unity and VNX systems running CEE version 8.8.2.1 and earlier.
- VCAPS—A mechanism for delivering post-events in asynchronous mode. The delivery cadence is based on either a time period or a number of events.

NOTE: If both CQM events and Auditing events are present, CEPA delivers events to the CQM application first, and then delivers events to the Auditing application.

While the CEE framework includes the CAVA and CEPA facilities and their associated sub-facilities, they can run independently of each other or run together.

This document is intended for use by customers who want to use CEE with consumer applications (such as for quotas or content type) to manage content stored on file systems.

System requirements

System requirements describes the Dell software, hardware, network, and storage configurations.

Table 1. System requirements

Type	Requirements
Software	Microsoft Windows Server or any Windows operating system compatible with the vendor's consumer application software. Two kits are available: • EMC_CEE_Pack_Win32_*xxxx* for installation on Windows 32-bit operating systems • EMC_CEE_Pack_x64_*xxxx* for installation on Windows 64-bit operating systems where *xxxx* = software version number You cannot install both a 32-bit and a 64-bit version of the software on the same machine. **NOTE:** Running CEE in the Windows on Windows (WOW) environment on a 64-bit platform is not supported. Search the Dell E-Lab™ Interoperability Navigator for consumer applications supported when using CEE, CAVA, and CEPA.
Hardware	Recommend using 16 GB Memory with 2 core processors.
Network	The Windows network must contain a domain controller with both Active Directory and DNS enabled. Dell systems must be configured with the SMB or CIFS protocol. You cannot use a Virtual Data Mover (VDM) for the SMB or CIFS protocol.
Storage	No specific storage requirements.

For the latest system requirements of CAVA, consult the website or documentation of the particular third-party anti-virus (AV) engine manufacturer. The AV engine version can be different depending on the operating system.

For minimum system requirements of AV engines, contact the appropriate third-party vendor. The 64-bit CAVA agent cannot work with a 32-bit AV engine. If you are using a 32-bit AV engine, you must use the 32-bit CAVA. Similarly, if you are using a 64-bit AV engine, you must use the 64-bit CAVA.

Windows does not allow loading a 32-bit driver on a 64-bit Windows operating system. When using CAVA with a 32-bit driver-based AV engine, you must load the AV engine and CAVA/CEE on a 32-bit Windows operating system.

AntiVirus partners

Dell has partnered with and supports the following AV engines:

- Computer Associates *e*Trust Threat Management Agent
- F-Secure AntiVirus
- Kaspersky Anti-Virus for Windows Servers Enterprise Edition
- Kaspersky Security 10 for Windows Servers
- Microsoft Defender
- Sophos Anti-Virus
- Sophos Endpoint Security and Control
- Symantec Endpoint Protection
- Symantec Protection Engine
- Trellix ENS
- Trend Micro ServerProtect for Storage

This list was correct at the time of publication. The Dell E-Lab Interoperability Navigator and the *Common Event Enabler Release Notes* provide the latest list of supported AV engines and versions.

Installing Third-Party Application Antivirus Engines contains further information about supported third-party antivirus software.

Support for third-party applications

CEPA provides event notifications and contexts to consumer applications that monitor the SMB/CIFS and NFS file system activity on the NAS Server. The consumer applications require event notifications from the NAS server to organize the access of information that is stored on the file systems. To provide this functionality, the CEPA API allows the consumer applications to obtain the required event information.

The consumer applications need to register for notifications by using the CEPA API. The CEPA API consists of an IDL file, when using XML/MSRPC, and an XML DTD file. These files contain information that is required by an application to interact with the event publishing agent. The consumer application can coexist with CEE framework on the same client or on the remote client. CEE facilitates the use of selected third-party applications with file systems. It provides events that contain the required context as defined by the consumer applications for each class. As more applications are added to each class, the events and associated contexts are modified to accommodate the applications.

Consumer applications can also acquire events when needed. This involves setting up a queue used to subscribe to a RabbitMQ Exchange. CEE forwards events to this exchange, and RabbitMQ routes the events into the correct subscriber queues.

NOTE: RabbitMQ is supported only for Dell Unity and VNX systems running CEE version 8.8.2.1 and earlier.

Restrictions

The following are known limitations at the time of publication.

Table 2. Restrictions

Type	Restrictions
AV engines	Currently, no known limitations exist for the number of AV engines configured in the NAS Server's CEE/CAVA pool. All AV engines are surveyed periodically by the NAS Server to determine which AV engines are online and available. This implies that configuration with many AV engines can cause some delays due to network latency.
CAVA pool	Each NAS Server should have a CAVA pool consisting of a minimum of two CAVA servers. This is specified in the configuration parameters for the NAS server.
CEPA pools	In Dell systems: • For pre-events, you can define only one CEPA pool. • For post-events and post-error events, you can define up to three CEPA pools.
Databases	Do not set up realtime scanning of databases. Accessing a database usually triggers a high number of scans, which in turn can cause a large amount of lag when accessing data. To ensure that the database files are virus free, use the AV engine to schedule regular scans when the database is not in use.
Non-SMB/CIFS protocols	The Dell antivirus solution is only for the clients running the SMB or CIFS protocol. If NFS or FTP protocols are used to move or modify files, the files are not scanned for viruses.
Restricted Group GPO	CAVA requires the antivirus domain account (AV user account) in whose context it is running to have access rights to the CHECK$ administrative share of any NAS Servers for which it is enabling AV protection.

Related information

Specific information related to third-party vendors described in this guide is included in:

- Microsoft website for Windows Management Instrumentation (WMI) information

- Computer Associates *e*Trust Threat Management Agent documentation
- F-Secure AntiVirus documentation
- Kaspersky Anti-Virus for Windows Servers Enterprise Edition documentation
- Sophos Anti-Virus documentation
- Symantec Endpoint Protection documentation
- Trellix ENS documentation
- Trend Micro ServerProtect for EMC documentation

Use of the term Windows Server

Unless otherwise noted in this guide, the term "Windows Server" refers to the following versions:

- Windows Server 2016
- Windows Server 2019
- Windows 10
- Windows Server 2022

2

Installing Third-Party Application Antivirus Engines

Topics:

Installation overview

Install one of the third-party AV engines on each participating AV machine before installing CAVA (as part of CEE). Installing the Common Event Enabler contains instructions on installing CEE.

NOTE: All packages except Trend Micro ServerProtect must be installed prior to installing CAVA (as part of CEE). Install Trend Micro ServerProtect provides more information.

NOTE: If you intend to run CEE with a third-party antivirus/antimalware product in addition to MS Defender, check the interoperability requirements with the third-party vendor.

If you are installing one of the following third-party antivirus software applications, use the installation path shown in Basic installation procedure.

- Computer Associates *e*Trust
- Kaspersky Anti-Virus for Windows Servers Enterprise Edition
- McAfee VirusScan
- Sophos Anti-Virus
- Symantec Endpoint Protection
- Symantec Protection Engine

Table 3. Basic installation procedure

Step	Action	Procedure
1.	Create a domain user with the EMC virus-checking right.	Configuring the Domain User Account
2.	Configure virus-checking parameters on NAS servers.	See the AV documentation for the Dell platform you are using.
3.	Install the AV engine on the Windows AV machine.	This chapter
4.	Install CAVA (as part of CEE) on the Windows AV machines.	Installing the Common Event Enabler
5.	Start the virus-checking client on NAS servers.	See the AV documentation for the Dell platform you are using.
6.	Verify the CAVA installation.	Verify the CAVA installation

If you are installing F-Secure AntiVirus, use the installation path shown in F-Secure AntiVirus installation procedure.

Table 4. F-Secure AntiVirus installation procedure

Step	Action	Procedure
1.	Install F-Secure AntiVirus AV engine on the Windows AV machine.	F-Secure AntiVirus
2.	Start the virus-checking client on NAS servers.	See the AV documentation for the Dell platform you are using.
3.	Verify the CAVA installation.	Verify the CAVA installation

If you are installing McAfee Endpoint Security (ENS) Threat Prevention, use the installation path shown in McAfee Endpoint Security Threat Prevention installation procedure.

Table 5. McAfee Endpoint Security Threat Prevention installation procedure

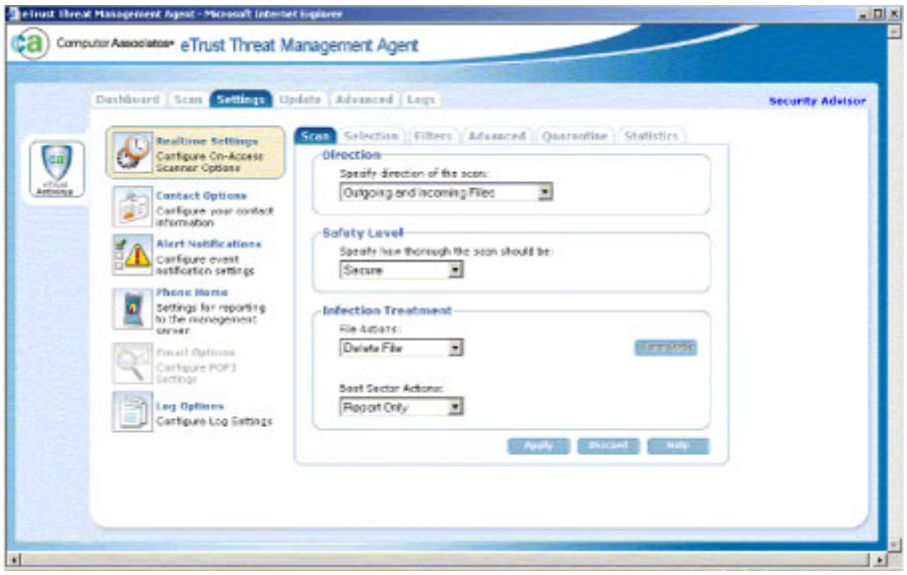
Step	Action	Procedure
1.	Install the McAfee ENS AV engine on the Windows AV machine.	McAfee Endpoint Security Threat Prevention
2.	Install CAVA (as part of CEE) on the Windows AV machines.	Installing the Common Event Enabler
3.	Start the virus-checking client on NAS servers.	See the AV documentation for the Dell platform you are using.
4.	Verify the CAVA installation.	Verify the CAVA installation

Computer Associates *e*Trust

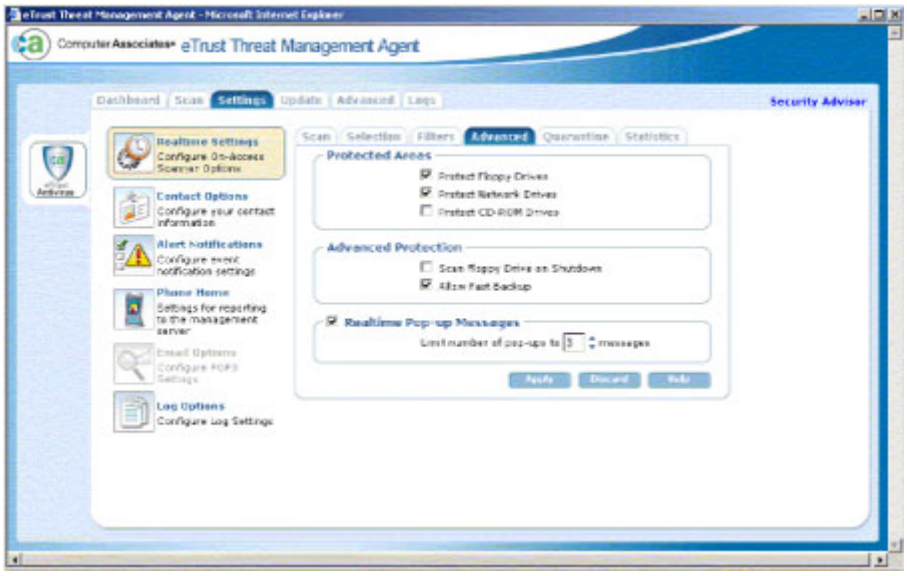
About this task

Steps

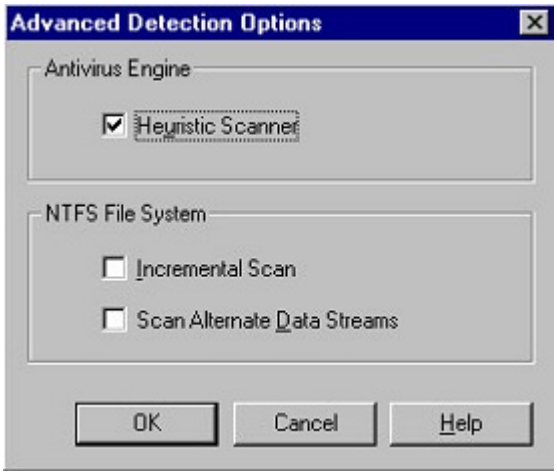
1. Install the *e*Trust application on an AV machine to interface with CAVA. Computer Associates documentation provides specific installation steps.
2. Start the application, and navigate to the **eTrust Threat Management Agent** window.
3. On the **eTrust Threat Management Agent** window, click the **Scan** tab.



4. On the **Scan** tab, select the following:
   - Under **Direction**, select **Incoming and Outgoing Files**
   - Under **Safety Level**, select **Secure**
   - Under **Infection Treatment**, select any of the options
5. Click the **Advanced** tab.



6. On the **Advanced** tab, select the following:
   - Under **Protected Areas**, select **Protect Network Drives**. You can also select **Protect Floppy Drives** and **Protect CD-ROM** if necessary.
   - Under **Advanced Protection** and **Realtime Pop-up Messages**, select the appropriate options.
7. Click **Selection**, and click **Advanced**. The **Advanced Detection Options** dialog box appears.



8. Under **Antivirus Engine**, select **Heuristic Scanner** for infections whose signatures have not yet been isolated and documented.

   NOTE: The settings under **NTFS File System** are optional.

9. Click **OK** to save the changes. Go to Installing the Common Event Enabler (to install CAVA as part of CEE).

F-Secure AntiVirus

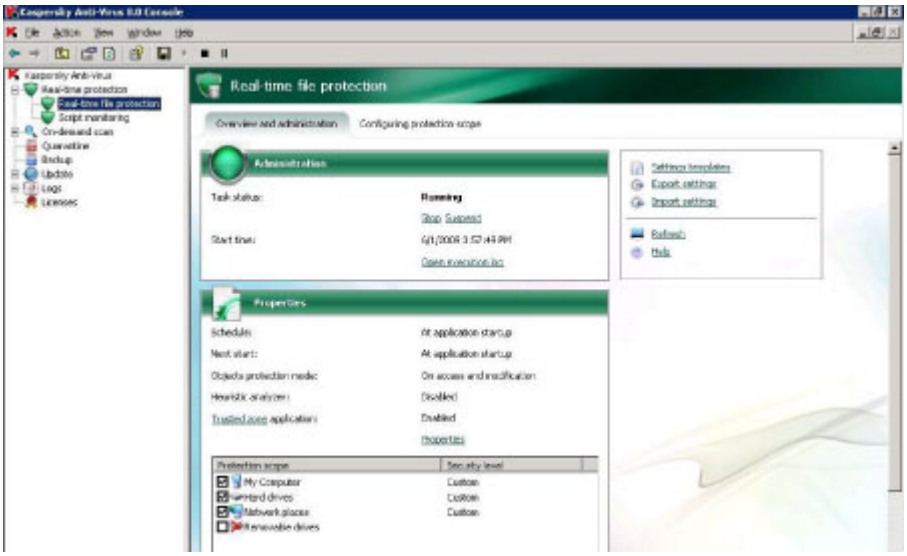
The necessary configuration options for using F-Secure AntiVirus with CAVA are incorporated into the F-Secure AntiVirus software installation. Refer to the appropriate F-Secure AntiVirus documentation for additional information.

After installing F-Secure AntiVirus, see the AV documentation for the Dell platform you are using for how to start the virus-checking client on NAS servers.

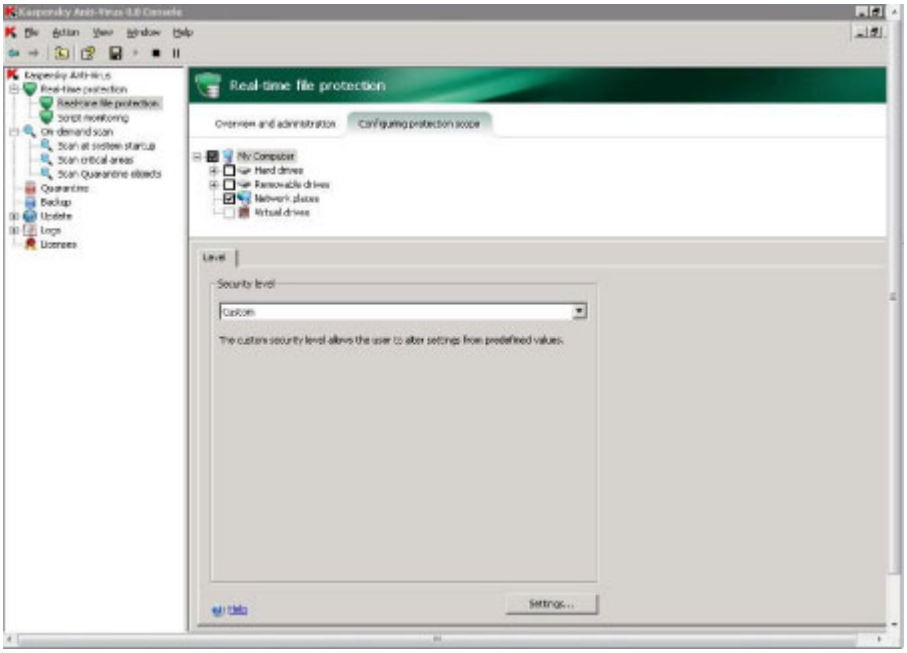
Kaspersky Anti-Virus

Steps

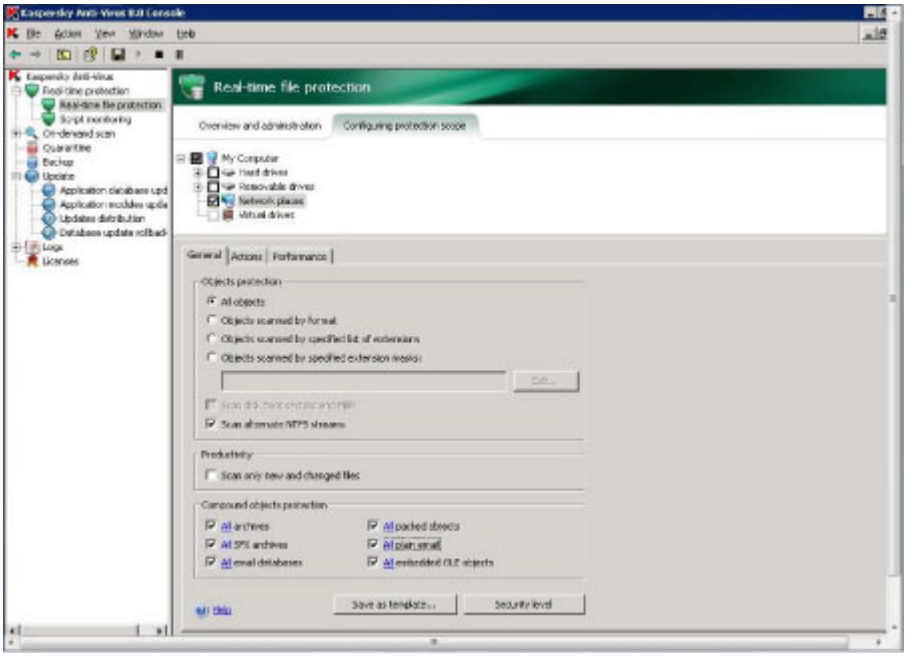
1. Install Kaspersky Anti-Virus for Windows Servers Enterprise Edition on a server that will interface with the AV machine. Kaspersky documentation provides specific installation steps.
2. Open the **Kaspersky Anti-Virus MMC Console**.
3. In the left pane, select **Real-time protection** and then **Real-time file protection**. The **Real-time file protection** window appears.



4. In the right pane, select **Configuring protection scope**. The **Configuring protection scope** tab appears.



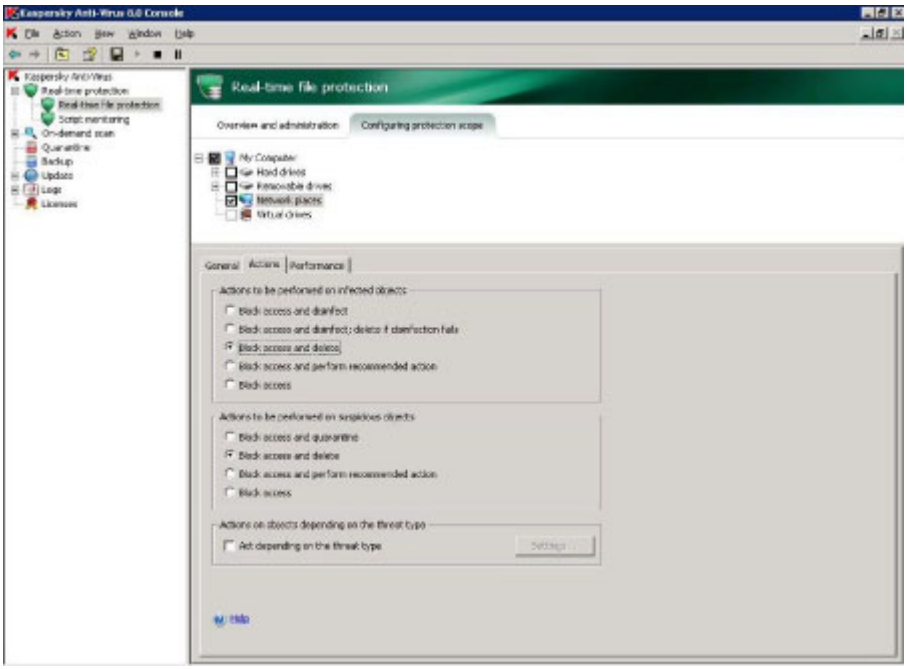
5. On the **Configuring protection scope** tab, select **Network places** and click **Settings**.
6. On the **General** tab:
   - In **Objects protection**, select **All objects** and **Scan alternate NTFS streams**.
   - In **Compound objects protection**, select all six checkboxes.



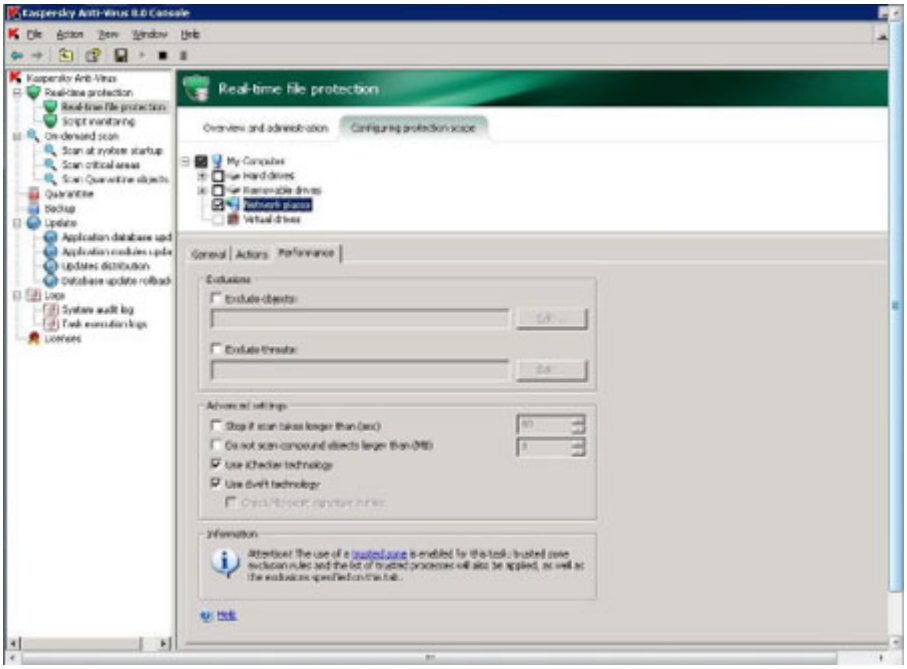
7. On the **Actions** tab, in **Actions to be performed on infected objects**, select one of the following options:
   - Block access and disinfect
   - Block access and disinfect, delete if disinfection fails
   - Block access and delete
   - Block access and perform recommended action

   NOTE: Block access does not work with CAVA.

   In **Actions to be performed on suspicious objects**, select one of the following options:
   - Block access and quarantine
   - Block access and delete
   - Block access and perform recommended action



8. On the **Performance** tab:
   - In **Exclusions**, clear **Exclude objects** and **Exclude threats**.
   - In **Advanced settings**, clear **Stop if scan takes longer than (sec)** and **Do not scan compound objects larger than (MB)**, and select **use iChecker technology** and **use iSwift technology**.



9. In the left pane, right-click **Real-time file protection** and select **Properties**. The **Real-time file protection Properties** dialog box appears.
10. On the **General** tab, select **On access and modification**.

11. On the **Schedule** tab, select one of the scheduling options.
12. Click **OK** to close the **Real-time file protection Properties** dialog box.
13. Close the Kaspersky Anti-Virus program. Go to Installing the Common Event Enabler (to install CAVA as part of CEE).

Trellix ENS

The necessary configuration options for using Trellix ENS with CAVA are incorporated into the Trellix ENS installation. Refer to the appropriate Trellix ENS documentation and Knowledgebase articles for additional information.

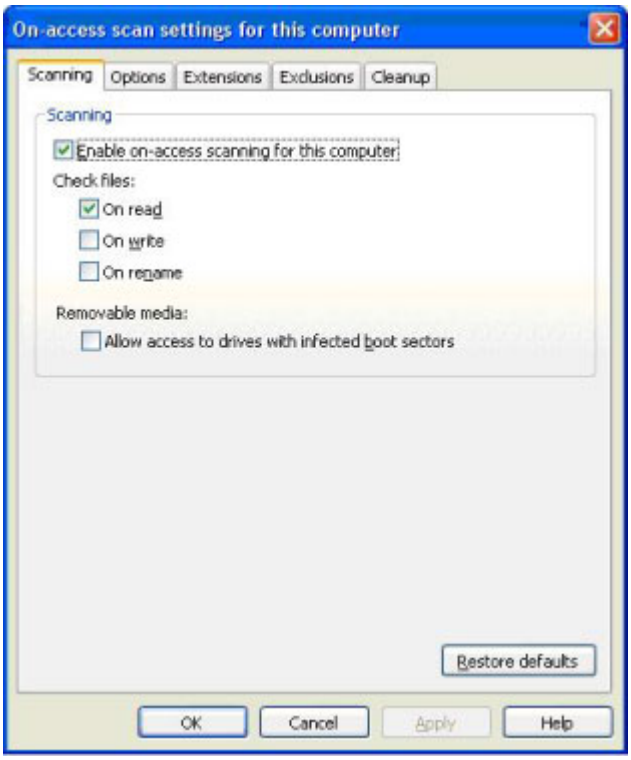
After installing Trellix ENS, go to Installing the Common Event Enabler.

Sophos Anti-Virus

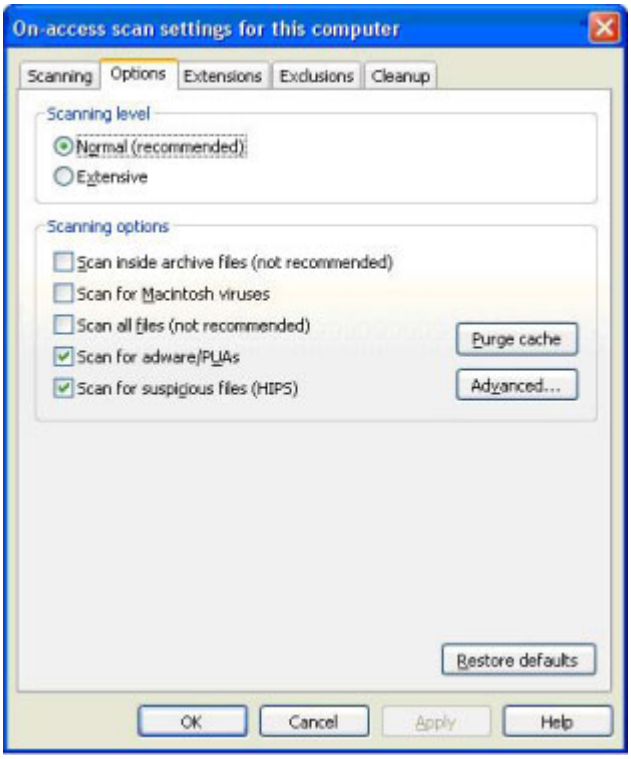
About this task

Steps

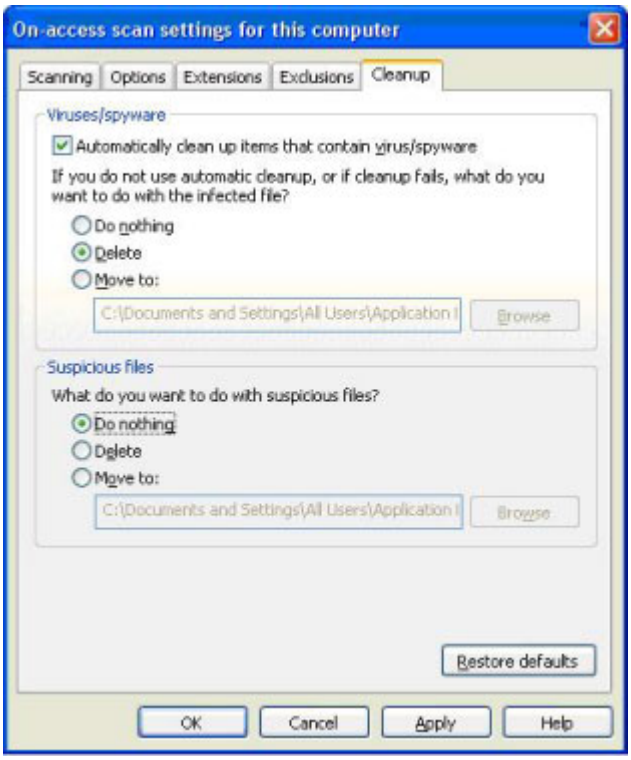
1. Install Sophos Anti-Virus on a server that will interface with the AV machine. Sophos documentation provides specific installation steps.
2. Right-click the Sophos icon (a blue shield) in the system tray and select **Open Sophos Anti-Virus**.
3. On the Sophos Anti-Virus home page, click **Configure Sophos**.
4. Select **On-access scanning**. The **On-access scan settings for this computer** dialog box appears.
5. On the **Scanning** tab, ensure that **Enable on-access scanning for this computer** is selected and select **On read**.



6. On the **Options** tab, select **Scan for adware/PUAs** and **Scan for suspicious files (HIPS)**.



7. On the **Cleanup** tab in **Viruses/spyware**, select **Automatically clean up items that contain virus/spyware**. Select **Delete** to delete items that cannot be cleaned up.



8. Click **OK** to close the dialog box.
9. Close the Sophos program. Go to Installing the Common Event Enabler.

Symantec Endpoint Protection

About this task

Symantec Endpoint resides on an AV machine and interfaces with CAVA version 4.5.2.2 (or later) for Symantec Endpoint Protection versions 11.04, 11.06, and 12.1:

Steps

1. Install the **Symantec Endpoint** software. The Symantec documentation provides specific installation steps.
2. Open the **Windows Registry Editor** and navigate to:
   - **For 32-bit operating systems:**

     ```
     HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint
     Protection\AV\Storages\Filesystem\RealTimeScan
     ```

   - **For 64-bit operating systems:**

     ```
     HKEY_LOCAL_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint
     Protection\AV\Storages\Filesystem\RealTimeScan
     ```

3. Set the RealTimeScan value:
   - For Symantec Endpoint Protection version 11.04, right-click **RealTimeScan** and select **New** > **Binary Value**.
   - For Symantec Endpoint Protection versions 11.06 and 12.1, right-click **RealTimeScan** and select **New** > **DWORD Value**.
4. In the **Value name** text box, type **DisableAlertSuppression**.
5. In **Value data**, type a value of **01**.
6. Click **OK**.

Set Symantec Endpoint Protection options

About this task

For Symantec Endpoint Protection versions 11.04, 11.06, and 12.1, perform the following steps:

Steps

1. Open **Symantec Endpoint Protection**.
2. For Symantec Endpoint Protection versions 11.04 and 11.06, click **Antivirus and Antispyware Protection Options**.
   For Symantec Endpoint Protection version 12.1, click **Virus and Spyware Protection Options**.
3. Click **Change Settings**.
4. For Symantec Endpoint Protection versions 11.04 and 11.06, select the **File System Auto-Protect** tab.
   For Symantec Endpoint Protection version 12.1, select the **Auto-Protect** tab.
5. Select **Enable File System Auto-Protect**.
6. In the **File Types** section, select **All Types**.
7. For Symantec Endpoint Protection versions 11.04 and 11.06, in the **Options** section, ensure that **Scan files on network drives** is selected.
   For Symantec Endpoint Protection version 12.1, in the **Options** section, ensure that:
   a. **Scan files on remote computers** is selected.
   b. **Only when files are executed** is cleared.
8. Click **Advanced**.
9. In the **Scan files when** section, select **Scan when a file is accessed or modified**.
10. Click **OK** to close the **Auto-Protect Advanced Options** window.
11. Click **OK** to close the **Protection Settings** window.

Set Windows Service Control Manager options

About this task

For Symantec Endpoint Protection versions 11.04 and 11.06 only, perform the following steps:

Steps

1. Open the Microsoft Windows **Service Control Manager** and navigate to **Symantec Endpoint Protection**.
2. Right-click **Symantec Endpoint Protection** and select **Properties**.
3. Click the **Log On** tab.
4. Set **This account** to the same EMC CAVA Service user who has EMC virus checking rights.
5. Click **OK**.

Symantec Protection Engine

Symantec Protection Engine resides on an AV machine and interfaces with CAVA by using the Internet Content Adaptation Protocol (ICAP) protocol. The application that requires antivirus scanning links to the Symantec library of scanning API calls by using this protocol.

About this task

NOTE: You must change the Symantec Protection Engine service from SYSTEM to the same user that is running CAVA, otherwise access problems can result. Domain user account overview provides more information about configuring the domain user and assigning access rights.

Steps

1. Install the Symantec Protection Engine software. The Symantec documentation provides specific installation steps.
2. Navigate to the Symantec Protection Engine **Status** page. Click **Configuration**.
3. Select **ICAP** protocol, and type **1344** in the **Port number** box.

   NOTE: In order for Symantec Protection Engine to interface with a Dell device, ICAP needs to accept requests from IP address 127.0.0.1. This can be done by either leaving the bind address field blank that includes all addresses, or by specifying 127.0.0.1.

4. Perform the following:
   a. Stop the Scan Engine Service.
   b. Open a command prompt, navigate to the directory where the scan engine has been installed, and run the following command:

      ```
      java -jar xmlmodifier.jar -s /policies/Misc/HonorReadOnly/@value
      false policy.xml
      ```

   c. Restart the Scan Engine Service.

   If the above setting is not specified, Symantec Protection Engine cannot delete the infected files because CAVA will not accept any scan requests.
5. Click **LiveUpdate**. Click **LiveUpdate Now** to get any new definition files.

Setting exclusions

When using Symantec Protection Engine and Symantec Endpoint Protection on the same machine, the temporary scan directory of Symantec Protection Engine must be set in the Exclusions section of the File System Auto-Protect configuration menu in the Symantec Endpoint Protection main console. This is to ensure that the AV engine takes action on all infected files that the virus scan detects.

About this task

Steps

1. Navigate to the Symantec Protection Engine **Status** page. Click **Configuration** and **Resources**.
2. Specify a temporary directory for scanning.

   NOTE: Allow enough room for this directory to grow because it can become several GBs in size. If a local AV solution is used, ensure to also exclude this directory from scanning. A local AV solution on the AV machine must not be allowed to scan the temporary working directory in use by Symantec Protection Engine.

Setting container handling policies

The `RPCRequestTimeout` value set in the `viruschecker.conf` file (the default is 25000 milliseconds) should be set to greater than the Symantec Protection Engine Container File Processing Limit for the time to extract a file. Not doing so can cause the NAS server to repeat the scans for large files to other AV machines while the scan is still in progress by the AV machine.

This timeout should be set 30 to 60 seconds higher than the container file processing limit so that the NAS server has adequate time to receive the response. The Symantec timeout can be set lower depending on the security scanning requirements and processing load of the AV machine.

Modifying LimitChoiceStop settings

The `LimitChoiceStop` parameter controls container violations actions. If this is set to false, the scan engine allows access to a file that is violating some of the container policies (such as max extract time exceeded) and will only log this error. If this is set to true (the default setting), the scan engine blocks access to (deletes) the file on the container violations.

About this task

You need to set the `LimitChoiceStop` parameter to false. Failure to perform this step results in an `AV_INTERFACE` error and CAVA will not come online:

Steps

1. Edit the `filtering.xml` file that resides in the SAV install directory.
2. Set the **LimitChoiceStop** option to **`false`**.

Trend Micro ServerProtect

If you are installing Trend Micro ServerProtect, use the installation path shown in Installation procedure for Trend Micro.

Table 6. Installation procedure for Trend Micro

Step	Action	Procedure
1.	Create a domain user with the EMC virus-checking right.	Configuring the Domain User Account
2.	Configure virus-checking parameters on the NAS servers.	See the AV documentation for the Dell platform you are using.
3.	Install CAVA (as part of CEE) on the Windows AV machines.	Installing the Common Event Enabler
4.	Install the Trend AV engine.	Install Trend Micro ServerProtect
5.	Start the virus-checking client on the NAS servers.	See the AV documentation for the Dell platform you are using.
6.	Verify the CAVA installation.	Verify the CAVA installation

Install Trend Micro ServerProtect

Prerequisites

Trend Micro ServerProtect must be installed after installing CAVA. Installing the Common Event Enabler provides instructions on installing CAVA as part of CEE.

If CAVA is not installed on the ServerProtect target AV machine, you will receive this server error message:

```
Before installing ServerProtect, you must install the EMC
Common AntiVirus Agent (CAVA).
```

About this task

Trend Micro ServerProtect resides on an AV machine and interfaces with CAVA. To protect the storage system and the AV machine, the default setting for the ServerProtect Real-time Scan function is Incoming & Outgoing. It is strongly recommended not to change this setting.

NOTE: The Trend Micro documentation provides specific installation and configuration steps.

Steps

1. Start ServerProtect. The **Management Console** window appears. Trend Micro ServerProtect Real-time Scan options window shows the **ServerProtect Management Console** window.
2. Select **Enable real-time scanning**, and select the following:
   - Under **Scan file type**, select **Selected files**.
   - Under **Scan options**, select **Scan floppy boot area**, **MacroTrap**, and **Scan mapped network drive**.
     NOTE: Ensure that you have selected **Scan mapped network drive** for CAVA to function with Server Protect 5.58.
   - Under **Compressed files**, select **Scan compressed files**.

   Leave all other settings as they are.

   When you have completed the steps, the **Management Console** window should look like Trend Micro ServerProtect Real-time Scan options window.
3. Click **Apply** to save the changes. See the AV documentation for the Dell platform you are using for how to start the virus-checking client on NAS servers.

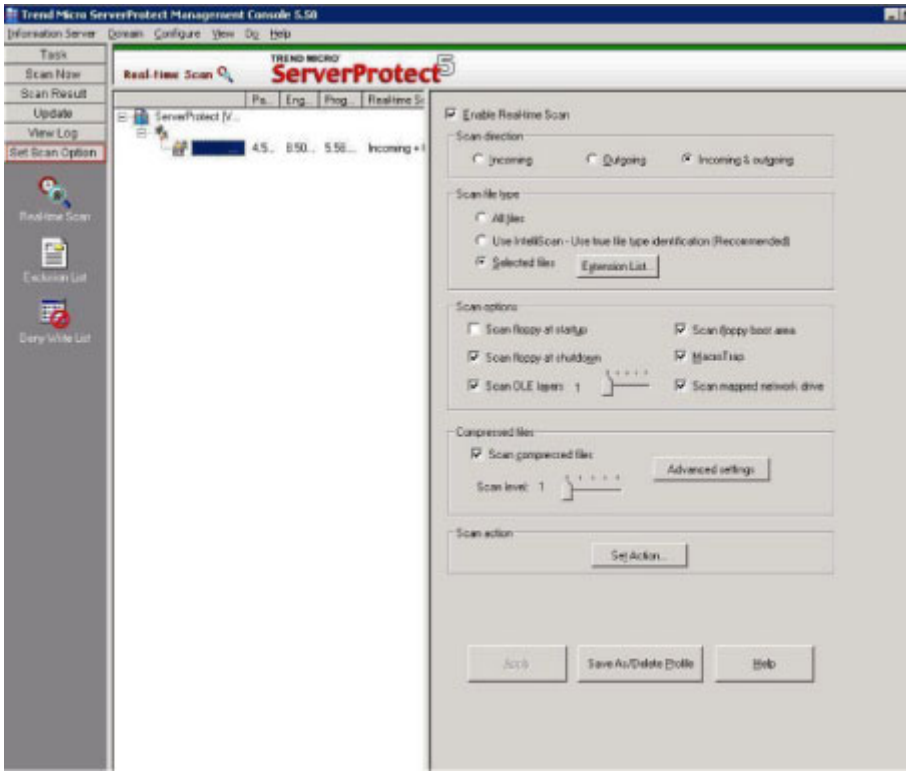


Figure 1. Trend Micro ServerProtect Real-time Scan options window

Verify the CAVA installation

Confirm that virus checking is operating properly.

Use a placebo virus to trigger the AV engine. A placebo, or benign virus, does not infect a Windows Server or NAS Server. To download the Eicar antivirus eicar.com.txt file, visit Eicar online at:

https://www.eicar.org/anti_virus_test_file.htm/

To verify that the infected file was found and deleted:

1. Check the resident AV log file.
2. Check the AV statistics file for the Dell platform you are using.

3

Installing the Common Event Enabler Framework

Topics:

Install CEE

Prerequisites

- Download the CEE framework software from Online Support:
  1. Open a browser window, and go to Online Support.
  2. Perform a search for **`Common Event Enabler`**.
  3. In the **Downloads** list, look for the **Common Event Enabler***<version number>***for Windows** program file.
  4. Click the program file name, and save the file.
  5. From the iso file, extract the 32-bit or 64-bit EMC_CEE_Pack executable file that you need.
- Installation prerequisites provides information that is needed before installing the CEE framework software. Specify the information pertinent to your company.

Table 7. Installation prerequisites

Prerequisite	Your company's data
User account with local administrator privileges to set up a CEPA account on domain server where CEE will be installed. This information is required when performing this installation procedure.	Account name: Account password:
Windows Server available where CEE will be installed. This information is required when performing this installation procedure.	IP address:
Windows domain server	Domain name: IP address:
CIFS server configured for use with the Windows domain server	IP address:
File systems	File system names:

About this task

Steps

1. Log in to the domain as an administrator.
2. If the Windows Server where you want to install the CEE software already has the CAVA software earlier than version 5.6 installed, you must uninstall it before installing the CEE software:
   a. From the Windows taskbar, click **Start** and select **Settings** > **Control Panel**.
   b. Double-click **Add or Remove Programs**.

c. Select **EMC CAVA** from the list.
d. Click **Change/Remove**. The anti-virus agent software will be removed from the Windows Server.

3. Run the **EMC_CEE_Pack** executable file for either the 32-bit (_Win32) or the 64-bit (_x64) version of the software. Click **OK** to start the InstallShield Wizard.

   The **Welcome to the InstallShield Wizard for EMC Common Event Enabler Framework Package** window appears:

   - If you have the most current version of InstallShield, the **License Agreement** window appears. Go to step 7.
   - If you do not have the most current version of InstallShield, you are prompted to install it. Go to step 4.

4. Click **Next**.
5. On the **Location to Save Files** window, click **Next**.

   NOTE: Do not change the location of the temporary directory.

   The Extracting Files process runs and returns to the **Welcome to the InstallShield Wizard** window.

6. Click **Next**.
7. On the **License Agreement** window, select **I accept the terms in the license agreement**, and click **Next**.
8. On the **Customer Information** window, type a username and organization, and click **Next**.
9. On the **Setup Type** window, select **Complete**, and click **Next**.
10. On the **Symantec** window, if you are using Symantec API-based anti-virus software, select **Work with Symantec SAV for NAS/Protection Engine** and the option for the Symantec anti-virus software version you are using. Otherwise, click **Next**.

    NOTE: This checkbox is used for the Symantec Protection Engine anti-virus agent. However, it is NOT used for the Symantec EndPoint Protection anti-virus agent.

11. On the **Ready to Install the Program** window, click **Install**. After the program is installed, the **InstallShield Wizard Completed** window appears.
12. Click **Finish**. The **EMC Common Event Enabler Installer Information** window appears and prompts you to restart the server.
13. Click **Yes** to restart the machine.

    NOTE: Clicking **No** cancels the restart.

14. Go to "Complete the CEE installation for Windows Server" to finish the CEE installation.

Verifying the CEE installation package

Starting with the CEE v8.9.4.x release, all CEE installers are signed with Microsoft Authenticode.

Instructions for verifying the CEE Installation package are found in the *Common Event Enabler Security Configuration Guide*.

Complete the CEE installation for Windows Server

About this task

Steps

1. From the Windows taskbar, click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **Services**.
2. Double-click **EMC CAVA** in the **Service** list.
3. On the **EMC CAVA Properties** window, click **Log On**.
4. Select **This account**, and click **Browse**.
5. On the **Select User** window, navigate to the domain where the account for the administrative user who has the rights to set up CAVA and CEPA server accounts exists, select the domain location, and click **OK**. The **Select User** window now contains the location.
6. Click **Advanced**.
7. Click **Find Now**.
8. Select the user account that was created to manage CAVA and CEPA services from the list, and click **OK**.

9. For this user account, type the account password in both the **Password** and **Confirm password** fields.
10. Click **OK**. The following message appears:

```
The new logon name will not take effect until you stop and
restart the service.
```

11. Click **OK**.
12. Restart the computer.
13. If you are using the CEPA facility, go to Third-Party Consumer Applications that explains how to set up the CEE framework for remote access to a third-party consumer application.
14. If you are using CAVA, stop and restart the CAVA service. Start, stop, and restart CAVA provides instructions on using the EMC CAVA services.

Uninstall CEE

About this task

To remove the CEE software and perform a clean uninstall:

Steps

1. From the Windows taskbar, click **Start** and select **Settings** > **Control Panel** > **Add or Remove Programs**.
2. Select **Common Event Enabler Framework**.
3. Click **Remove**.
4. Close the **Add or Remove Programs** window.
5. Close the **Control Panel** window.

4

Configuring the Event Publishing Agent

Topics:

Configuring CEPA

You configure CEPA by using the management software for your product. Refer to the product online help for instructions on editing Events Publishing configuration information.

5

Configuring the Domain User Account

This chapter describes how to configure the AV user (domain user) account with the EMC virus-checking right. Having this account allows the NAS Server to distinguish CAVA requests from all other requests.

Topics:

Domain user account overview

The antivirus agent installation requires a Windows user account that is recognized by the NAS Servers as having the EMC virus-checking privilege. This user account enables the NAS Server to distinguish CAVA requests from all other client requests. To accomplish this, you should create a new domain user, assign to this user the EMC virus-checking right locally on the NAS Server, and run the EMC CAVA service in this user context.

Overview of configuring the AV user provides an overview of configuring the AV user (domain user) with the EMC virus-checking right. The user account that you create in the following procedures is the preferred user account that should be configured with EMC virus-checking access.

You can also configure a local user account with access rights even if it is on a standalone server. See the Configuring SMB or CIFS documentation provided with your storage system for more information about configuring a domain user account.

Table 8. Overview of configuring the AV user

Task	Action	Procedure
1.	Create a domain user account (AV user).	Create a domain user account
2.	Create a local group on each NAS Server in the domain and add the AV user to the group.	Create a local group on each NAS Server
3.	Assign the EMC virus-checking right to the local group.	Assign the EMC virus-checking right to the group
4.	Assign local administrative rights to the local group on each AV machine.	Assign local administrative rights to the AV user

Optional method

For a Windows Server, you can accomplish Tasks 2 through 5 by using the Dell NAS Management snap-in.

Create a domain user account

You must create a domain user account on the Windows domain controller. The EMC CAVA service is running in the context of this user.

Use one of the following sections to create the domain user account:

- Create with Active Directory on a Windows Server
- Create from User Manager for Domains

Create with Active Directory on a Windows Server

Steps

1. Log in to a Windows Server as the Domain Administrator.
2. From the Windows taskbar, click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the console tree, right-click **Users**, and select **New** > **User** from the shortcut menu. The **New Object - User** dialog box appears.
4. In the **New Object - User** dialog box, perform the following:
   a. Specify the **First name**, **Last name**, and **User logon** name. For the logon name, use something that refers to virus checking, for example, virususer.

      NOTE: You can give the domain user any name that you want, although it should have a context-appropriate name. The name virususer is used as an example in this guide.

   b. Click **Next**. The **Password** dialog box appears.
5. In the **Password** dialog box, perform the following:
   a. Type a password and confirm the password in the appropriate fields.
   b. Select **Password never expires**.
   c. Click **Next**. A confirmation screen appears.
   d. Click **Finish**. The **New Object - User** dialog box closes.
6. Go to Create a local group on each NAS Server.

Create from User Manager for Domains

About this task

You can create a domain user account from User Manager for Domains on a Windows Server without Active Directory:

Steps

1. Start User Manager for a Windows Server without Active Directory. Click **Start** on the Windows taskbar, and select **Settings** > **Control Panel** > **Administrative Tools** > **Computer Management**. Select **Local Users and Groups**.
2. Right-click the **Users** folder and select **New User**. The **New User** dialog box appears.
3. In the **New User** dialog box, perform the following:
   a. In the **Username** box, type a name. For example, virususer.

      NOTE: You can give the domain user any name that you want, although it should have a context-appropriate name. The name virususer is used in this guide.

   b. Type a password and confirm the password in the appropriate fields.
   c. Clear **User Must Change Password at Next Logon**.
   d. Click **Add** to save the new virususer account.
   e. Click the **Groups** button. The **Group Memberships** dialog box appears.
4. In the **Group Memberships** dialog box, perform the following:
   a. Select **Administrators** from the **Not a Member Of** list.
   b. Click **Add**. The Administrator group is added to the **Member Of** list. The virususer account should be a member of the Domain Users group and the Administrators group.
   c. Click **OK**. The **Group Memberships** dialog box closes.
   d. Click **OK**. The **New User** dialog box closes.
5. Go to Create a local group on each NAS Server.

Create a local group on each NAS server

About this task

To assign the EMC virus-checking right to the domain user you just created, you must first create a local group on the NAS server and assign the user to this group. Then assign the EMC virus-checking right to the group. Use this procedure to create a local group in a Windows Server:

Steps

1. For systems with Active Directory, navigate to **Active Directory Users and Computers**, double-click **EMC NAS servers** and click **Computers**.
2. In the **Computer** pane, right-click the SMB/CIFS server that you want to manage and select **Manage** from the shortcut menu. The **Computer Management** window appears.
3. Under **System Tools**, double-click **Local Users and Groups**.
4. Right-click **Groups** and select **New Group**. The **New Group** dialog box appears.
5. In **Group name**, type a group name (for example, viruscheckers) and in **Description**, type a description.
6. Click **Add**. The **Select Users, Computers, or Groups** dialog box appears.
7. In the **Select Users, Computers, or Groups** dialog box, perform the following:
   a. Type the name of the AV user account that you created in Create a domain user account.
   b. Click **Check Names**.
   c. Click **OK** to close the **Select Users, Computers, or Groups** dialog box.
   d. Click **OK**. You return to the **New Group** dialog box.
8. Click **Create**, and click **Close**. The group is created and added to the Groups list. Go to Assign the EMC virus-checking right to the group.

Assign the EMC virus-checking right to the group

About this task

Now that you have created the domain user, you must distinguish this user from all other domain users by assigning the EMC virus-checking right. This right is not a domain privilege, but rather it exists locally in the NAS Server and is added to the local group that you created in Create a local group on each NAS Server.

NOTE: When using CEE/CAVA with PowerScale systems, the user in which the `cava.exe` service is running must have access to the CHECK$ share on the PowerScale NAS Server. Refer to the appropriate PowerScale OneFS documentation for details on configuring CEE/CAVA.

NOTE: You cannot use Microsoft's Windows Local Policy Setting tools to manage user rights assignments on a NAS Server because the Windows Local Policy Setting tools do not allow you to remotely manage user rights assignments.

Use this procedure to assign the EMC virus-checking right to the group in a Windows Server:

Steps

1. Click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **Dell NAS Management**.
2. Perform one of the following:
   - If a NAS Server is already selected (name appears after NAS Server Management), go to step 4.
   - If a NAS Server is not selected:
     - Right-click **NAS Server Management** and select **Connect to NAS Server**.
     - Select a NAS Server by using ONE of the following methods:
       - In the **Look in:** list box, select the domain in which the NAS Server that you want to manage is located, and select it from the list.

         OR

       - In the **Name** box, type the computer name, IP address, or the NetBIOS name of the NAS Server.
3. Double-click **NAS Server Management**, and double-click **NAS Server Security Settings**.
4. Click **User Rights Assignment**. The assignable rights appear in the right pane.

5. Double-click **EMC Virus Checking**.
6. In the **Security Policy Setting** dialog box, click **Add**.
7. In the **Select Users or Groups** window perform the following:
   a. Select the NAS server from the **Look in:** list box.
   b. Select the antivirus group that you created in Create a local group on each NAS Server.
   c. Click **Add**. The group name appears in the lower window.
   d. Click **OK**. You return to the **Security Policy Setting** dialog box.
8. Click **OK**. The EMC Virus Checking policy now shows the NAS Server local group. Go to Assign local administrative rights to the AV user to continue.

Assign local administrative rights to the AV user

About this task

You must assign local administrative rights to the AV user on each AV machine. You must repeat this procedure for each AV machine.

NOTE: If the AV machine is a domain controller, the virus-checking user account should join the Domain Administrator group instead of the local administrator group. This is because the local administrator group is not managed on a domain controller.

Use this procedure to assign local administrative rights to the group in a Windows Server:

Steps

1. Click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **Computer Management**. The **Computer Management** window appears.
2. From the **Action** menu, select **Connect to Another Computer**. The **Select Computer** window appears.
3. In the **Select Computer** window:
   a. Select the virus-checker server.
   b. Click **OK** to close the **Select Computer** window.
4. In the **Computer Management** window:
   a. Expand **System Tools**.
   b. Expand **Local Users and Groups**.
   c. Click **Groups**. The group names appear in the right pane.
5. Double-click the **Administrators** group. The **Administrators Properties** dialog box appears.
6. Click **Add**. The **Select Users or Groups** window appears.
7. In the **Select Users or Groups** window:
   a. Select the domain from the **Look in:** list box.
   b. Select the AV user account that you created in Create from User Manager for Domains.
   c. Click **Add**.
   d. Click **OK** to close the **Select Users or Groups** window.
8. Click **OK** to close the **Administrators Properties** dialog box.
9. Repeat steps 1–8 for each AV machine in the network. On completion of the steps, see the AV documentation for the Dell platform you are using for configuring virus-checking parameters on NAS servers.

6

Managing CAVA

Topics:

(Optional) Install Dell NAS Management snap-in

In a Windows Server environment, use the Dell NAS Management snap-in to modify the antivirus agent parameters on the NAS Server. You can download the snap-in from Online Support.

Open the Dell NAS Management snap-in

To open the Dell NAS Management snap-in, click **Start** on the Windows taskbar, and select **Settings** > **Control Panel** > **Administrative Tools** > **Dell NAS Management**.

For assistance in using the Dell NAS Management snap-in, click **Help** in the toolbar.

NOTE: The SMB/CIFS services must be configured and started on the NAS server before you can change the virus-checking configuration parameters.

Assign rights in Windows Server

About this task

There are two rights that can be assigned to the user contexts:

- EMC Event Notification Bypass right—to suppress generation of CEPA events by the users who are assigned this right
- EMC Virus Checking right—to distinguish the CAVA user from all other domain users

Steps

1. Click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **Dell NAS Management**.
2. Perform one of the following:
   - If a NAS Server is already selected (name appears after NAS Server Management), go to step 4.
   - If a NAS Server is not selected:
     - Right-click **NAS Server Management** and select **Connect to NAS Server**.
     - Select a NAS Server by using ONE of the following methods:
       - In the **Look in:** list box, select the domain in which the NAS Server that you want to manage is located, and select it from the list.

         OR

       - In the **Name** box, type the computer name, IP address, or the NetBIOS name of the NAS Server.
3. Double-click **NAS Server Management**, and double-click **NAS Server Management Security Settings**.
4. Click **User Rights Assignment**. The assignable rights appear in the right pane.
5. When you want to exclude domain users from generating CEPA events, double-click **EMC Event Notification Bypass**. Otherwise, this right does not need to be assigned.
   a. In the **Security Policy Setting** dialog box, click **Add**.

b. If necessary, in the **Select Users or Groups** dialog box, choose the NAS Server from the **Look in** drop-down list. Select the user from the list box.
c. Click **Add**, and then click **OK** to close the **Select Users or Groups** dialog box.
d. Click **OK** to close the **Security Policy Setting** dialog box.

6. To distinguish a CAVA user from all other domain users, in the **User Rights Assignment** list, double-click **EMC Virus Checking**.
   a. In the **Security Policy Setting** dialog box, click **Add**.
   b. If necessary, in the **Select Users or Groups** window, choose the NAS Server from the **Look in** drop-down list. Select the user from the list box.
   c. Click **Add**, and then click **OK** to close the **Select Users or Groups** dialog box.
   d. Click **OK** to close the **Security Policy Setting** dialog box.
7. Close the **Dell NAS Management** window.

Assign rights for third-party applications

If events need to be suppressed, third-party applications use the EMC Event Notification Bypass privilege to identify their I/O requests to the CEPA facility. This facility then suppresses any event/context packets from I/O requests.

You also need to distinguish the CEPA user from all other domain users by assigning the EMC virus-checking right.

Use the Dell NAS Management snap-in to assign the EMC Event Notification Bypass right to domain users for the third-party application and the EMC virus-checking right to the CEPA user. The EMC Event Notification Bypass right is not a domain privilege, but rather exists locally in the NAS Server.

NOTE: You cannot use Microsoft Windows Local Policy Setting tools to manage user rights assignments on a NAS Server because the tools do not allow you to remotely manage user rights assignments.

Start, stop, and restart CAVA

About this task

Use the EMC CAVA service to start, stop, pause, or resume services on the AV machine. Through the Services window, you can manage the EMC CAVA service if it fails to start on restart.

You can access the EMC CAVA service from a Windows Server by using this procedure:

Steps

1. From the Windows taskbar, click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **Services**.
2. Scroll to **EMC CAVA**.
3. Right-click **EMC CAVA** and click **Start**, and select either **Stop**, **Pause**, **Resume**, or **Restart** (whichever is appropriate) from the shortcut menu.

View the application log file from a Windows Server

Steps

1. From the Windows taskbar, click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **Computer Management**.

   NOTE: Another way to open Event Viewer is to click **Start** on the Windows taskbar, and select **Settings** > **Control Panel** > **Administrative Tools** > **Event Viewer**.

2. Under **System Tools**, double-click **Event Viewer**, and click **Application Log**.
3. In the right-hand pane, locate the entries for **EMC Checker Server**.

Enable automatic virus detection notification

About this task

When CAVA detects an infected file, it can automatically send notification to the client through Windows pop-up messages when the Windows Messenger service is enabled. For administrators, events are logged in the system log.

Use this procedure to enable messaging on a Windows Server:

Steps

1. Click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **Services**.
2. In the **Services** window, right-click the **Messenger** service entry and select **Properties**. The **Messenger Properties** dialog box appears.
3. Select **Automatic** from the **Startup type** list. Click **Apply**.
4. Click **OK** to exit.

Customize virus-checking notification

About this task

Each third-party antivirus vendor varies slightly on which type of remediation works with CAVA. Types of remediation lists the types of remediation supported by the third-party vendors. Third-party vendor documentation provides more information.

Table 9. Types of remediation

Vendor	Supported remediations
Computer Associates	Delete; Rename; Move; Quarantine
F-Secure	Decide action automatically/Quarantine automatically
McAfee	Clean; Delete
Microsoft Forefront Endpoint Protection	Remove; Quarantine
Sophos	Delete; Move to
Symantec Endpoint Protection 2012	Delete; Quarantine
Symantec Protection Engine	Delete; Quarantine
Trend Micro	Clean; Delete; Quarantine

7

Managing the Registry and AV Drivers

CAVA provides Windows parameters that you can set to modify the behavior of CAVA. You edit the parameters through the Windows Registry Editor. For information about editing the Registry, view the Changing Keys and Values online help topic in the Registry Editor (regedit.exe).

NOTE: Editing the Windows Server Registry can cause serious problems that require a reinstallation of the operating system. It is advisable to create a backup copy of the Registry files before editing them. You should edit the following parameters only if you have an in-depth knowledge of CAVA and the Microsoft Registry.

Topics:

EMC CAVA configuration Registry entries

Two user-configurable Registry entries are available for CAVA configuration:

- AgentType — Currently, the only supported AgentType is driver. This option allows for future support of other possible interfaces as they become available.
- NumberOfThreads — Determines the number of threads which the CEE framework uses to process incoming requests from the system:
  - Minimum value = 1
  - Default value = 20 (decimal)

To access the AgentType entry from the Registry Editor, use this directory path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CAVA\Configuration
```

To access the NumberOfThreads entry from the Registry Editor, use this directory path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\Configuration
```

EMC AV driver Registry entry

Use this directory path to access the Windows Registry to ensure that the EMC AV driver is properly configured:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EMCVirCk
```

The correct settings for the EMC AV driver are:

- ErrorControl = 1
- Start = 2
- Type = 1

If the settings are different from those indicated, modify them.

Manage the EMC AV driver

About this task

The EMC AV driver (EMCVirCk) is a Windows Server driver. Use this procedure to manage the AV driver:

Steps

1. From the Windows taskbar, click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **Event Viewer**.
2. From the **Event Viewer** window, select **System Log**.
3. In the right pane, double-click **EMCVirCk** in the Event Viewer's System Log list. The **Event Properties** window appears.
4. Ensure that a loaded successfully message appears in the Description field. If the driver was not loaded successfully, restart the AV machine.
5. Click **OK** to close the **Event Properties** window.

Restricting CEE platform HTTP connections

About this task

When enabled and configured, AccessList allows HTTP connections only from IP addresses which are listed in the AccessList section of the CEE configuration.

NOTE: Any time you modify the CEE section of the Registry, except for Verbose and Debug, you must restart the EMC CAVA service.

Steps

1. Open a command window on the machine where CEE is installed and type **`regedit`**.
2. On the Windows Registry Editor window, navigate to:

   HKEY_LOCAL_MACHINE > **SOFTWARE** > **EMC** > **CEE** > **Configuration** > **Security** > **Access**

3. Set the **AccessListEnabled** DWORD option to **1** (enabled).

   NOTE: Setting this option to **0** disables it.

4. Set the **AccessList** REG_SZ option to the list of IP addresses from which CEE will accept messages. You can designate multiple IP addresses by separating them with semicolons (;).
5. Restart the EMC CAVA service by using the Windows Service Control Manager.

8

Managing CARA

Common Anti-Ransomware Agent (CARA) is a mechanism for delivering post-events in asynchronous mode. The delivery cadence is based on a time period or a number of events.

Topics:

Set up access for Windows platforms

About this task

You must add one CARA entry to the Microsoft Windows Registry.

NOTE: Any time you modify the CEE section of the Registry, except for Verbose and Debug, you need to restart the EMC CAVA service.

Steps

1. Open a command window on the machine where CEE and CARA are installed and type **regedit**.
2. On the Windows Registry Editor window, navigate to:

   HKEY_LOCAL_MACHINE > **SOFTWARE** > **EMC** > **CEE** > **CEPP** > **CARA** > **Configuration**

3. Double-click **Endpoint** and specify the IP address and port of the computer where the consumer application is installed, in the following format:

   <carapartner>@<IP address>:<port>

   When setting multiple computers, you must use a ; (semicolon) to separate the IP addresses.

4. Restart the EMC CAVA service by using the Windows Service Control Manager.

Results

The FeedInterval and MaxEventsPerFeed delivery cadences are used simultaneously.

CARA sends a list of modified events to the consumer application, not the actual content.

9

Managing VCAPS

Common Asynchronous Publishing Service (VCAPS) is a mechanism for delivering post-events in asynchronous mode. The delivery cadence is based on a time period or a number of events.

Topics:

Set up access

About this task

You must add four VCAPS entries to the Microsoft Windows Registry.

NOTE: Any time you modify the CEE section of the Registry, except for Verbose and Debug, you need to restart the EMC CAVA service.

Steps

1. Open a command window on the machine where CEE and VCAPS are installed and type **`regedit`**.
2. On the Windows Registry Editor window, navigate to:

   HKEY_LOCAL_MACHINE > **SOFTWARE** > **EMC** > **CEE** > **CEPP** > **VCAPS** > **Configuration**

3. Double-click Endpoint and specify the IP addresses of the computers where the consumer application is installed, in the following format:

   <vendorname>@<IP address>

   When setting multiple computers, you must use a ; (semicolon) to separate the IP addresses.

4. Double-click **Enabled**. Specify **`1`** to enable VCAPS, or **`0`** to disable it.
5. Double-click **FeedInterval** and specify how often, in seconds, information is sent from VCAPS to the consumer application. The default is 60 seconds. The range is from 60 seconds to 600 seconds.
6. Double-click **MaxEventsPerFeed** and specify how many modification events must occur before information is sent from VCAPS to the consumer application. The default is 100 events. The range is from 10 events to 10,000 events.
7. Restart the EMC CAVA service by using the Windows Service Control Manager.

Results

The FeedInterval and MaxEventsPerFeed delivery cadences are used simultaneously.

VCAPS sends a list of modified events to the consumer application, not the actual content.

10

Managing CEE for RabbitMQ

NOTE: RabbitMQ is supported only for Dell Unity and VNX systems running CEE version 8.8.2.1 and earlier.

CEE Messaging with RabbitMQ is a mechanism for delivering events in asynchronous mode into a RabbitMQ exchange.

When consuming events by using RabbitMQ, a consumer application must set up and maintain its queue. Ensure that the application's queue is emptied periodically to prevent accumulated events in the queue from using all of RabbitMQ's available storage. It is also recommended to use RabbitMQ's inherent policy parameter which imposes a "queue length limit" as described in the RabbitMQ documentation.

NOTE: CEE supports RabbitMQ version 3.8.9, and ERLANG version 23.0.

Topics:

Set up CEE for RabbitMQ

About this task

NOTE: RabbitMQ is supported only for Dell Unity and VNX systems running CEE version 8.8.2.1 and earlier.

You must configure CEE to send events to the RabbitMQ server.

Steps

1. In the CEE installation area (the default directory is \Program Files\EMC\CEE), find and edit the MsgSys.xml file:
   a. Set **Host name** to the IP address of the RabbitMQ server.
   b. Keep the **port** set to the default of 5672, which is the port used for communication between CEE and the RabbitMQ server.
   c. Set **username** and **password** to the username and password for a RabbitMQ user who has an "administrator" tag in the RabbitMQ virtual host in which the CEE_Events exchange resides.
   d. Set **vhost** to the RabbitMQ virtual host in which the CEE_Events exchange resides.

   Example:

```
<?xml version="1.0" encoding="utf-8"?>
<MsgSys>
  <MsgBus enabled="1">
    <Host name="10.1.4.50" port="5672" username="ceetester"
     password="EMCnew1">
      <Exchange name="CEE_Events" vhost="CEE" type="topic">
        <Message persistent="1" />
      </Exchange>
    </Host>
  </MsgBus>
</MsgSys>
```

2. Save the MsgSys.xml file.
3. Restart the CEE service.

11

Managing Indexing

The Index sub-facility of CEPA is a mechanism for delivering bulk events in asynchronous mode to partner applications. The delivery cadence is based on either a time period or a number of events. You can use this Index facility to deliver bulk events to Splunk Enterprise or Splunk Cloud. CEE uses the Splunk HTTP Event Collector (HEC) to send events to a Splunk deployment over the Secure HTTP (HTTPS) protocol. The index used in Splunk Enterprise or Splunk Cloud to receive the CEE events must be configured in Splunk for structured messaging in the JSON format.

Topics:

Set up access for Splunk

About this task

Use the Index facility to deliver events to Splunk Enterprise or Splunk Cloud by performing the following steps.

You must add Index entries to the Microsoft Windows Registry.

NOTE: Any time you modify the CEE section of the Registry, except for Verbose and Debug, you need to restart the EMC CAVA service.

Steps

1. Open a command window on the machine where CEE and the Index application are installed and type **regedit**.
2. On the Windows Registry Editor window, navigate to:
   HKEY_LOCAL_MACHINE > **SOFTWARE** > **EMC** > **CEE** > **CEPP** > **Index** > **Configuration**
   a. Double-click **Enabled**. Specify **1** to enable Index, or **0** to disable it.
   b. Double-click **Endpoint** and specify the host and port, or hosts and ports, of the instances where the Splunk consumer application is installed, in the following format:

      `SplunkHEC@https://<host>:<port>`

      where `<host>` is the URI, IP address, or FQDN of Splunk Enterprise or Splunk Cloud. For example, `SplunkHEC@https://10.1.2.1:8088`.

      When setting multiple entries, you must use a ; (semicolon) to separate the individual entries. For example, `SplunkHEC@https://10.3.4.20:8088;SplunkHEC@https://10.3.4.40:8088`.

   c. (Optional) **FeedInterval** specifies how often, in seconds, information is sent from the Index application to the Splunk consumer application. The default is 60 seconds. The range is from 60 seconds to 600 seconds. Update this value only if necessary.
   d. (Optional) **MaxEventsPerFeed** specifies how many events are accumulated before information is sent from the Index application to the Splunk consumer application. The default is 100 events. The range is from 10 events to 10,000 events. Update this value only if necessary.
3. Navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **EMC** > **CEE** > **CEPP** > **Index** > **Configuration** > **SplunkHEC**.
   a. Add a value for **Index**, which is a user-defined name for the index being used on Splunk Enterprise or Splunk Cloud. Only one index value is allowed.
   b. Under **SplunkHEC**, create a key for the **Host server** using the URI, FQDN, or IP address of the instance (used as `<host>` in the EndPoint above) where the Splunk consumer application is installed.
   c. Under that key, create a REG_SZ value called **Token**. Copy the token value that is defined in the HTTP Event Collector in Splunk Enterprise or Splunk Cloud to here.

   NOTE: To use multiple instances of the Splunk consumer application, you must create multiple sub keys under SplunkHEC in the registry - one for each location - and specify a token for each instance.

4. Restart the EMC CAVA service by using the Windows Service Control Manager.

Results

The **FeedInterval** and **MaxEventsPerFeed** delivery cadences are used simultaneously.

The Index application sends a list of events to the Splunk consumer application, not the actual content of files.

12

Monitoring and Sizing the Antivirus Agent

You can use the CAVA Calculator to estimate the number of AV machines that are required before installing the antivirus agent. You can also use the CAVA sizing tool to monitor the antivirus agent usage on the network and determine the optimal number of AV machines, based on the system usage.

Topics:

CAVA Calculator

CAVA Calculator is a utility that assists you in determining the number of AV machines for the environment prior to installation. The CAVA Calculator can be installed and run independent of CAVA and Dell systems, whereas the sizing tool uses the actual workload. This utility is installed as part of CEE framework. System requirements provides more information.

Install the CAVA Calculator

Prerequisites

You must have the Microsoft .NET Framework 1.1 or later installed on the system. The .NET Framework software is included with Windows Server installations, and is available on the antivirus agent software installation media. You can also download the .NET Framework from the Microsoft website.

The CAVA Calculator installation requires a restart at the end of the installation process.

About this task

The CAVA Calculator is automatically installed as part of a complete CEE software installation. You only need to perform this procedure if you performed a Custom installation and did not install the CAVA Calculator:

Steps

1. Run the **EMC_CEE_Pack** executable file for either the 32-bit (_Win32) or the 64-bit (_x64) version of the software. Click **OK** to start the InstallShield Wizard.

   The **Welcome to the InstallShield Wizard for EMC Common Event Enabler Framework Package** window appears.

   - If you have the most current version of InstallShield, the License Agreement window appears. Skip to step 5.
   - If you do not have the most current version of InstallShield, you are prompted to install it. Go to step 2.
2. Click **Next**. The **Location to Save Files** window appears.
3. Click **Next**.

   NOTE: Do not change the location of the temporary directory.

   The Extracting Files process runs and returns to the **Welcome to the InstallShield Wizard** window.
4. Click **Next**.
5. In the **License Agreement** window, click **I accept the terms in the license agreement**, and click **Next**.
6. In the **Customer Information** window, type a username and organization, and click **Next**.
7. In the **Setup Type** window, select **Custom**, and click **Next**.
8. In the **Custom Setup** window, select **Tools** and click **Next**.

NOTE: To install only the CAVA Tools, click the down arrow beside each feature you do not want to install and select **This feature will not be available**.

9. Click **Install**.
10. Click **Finish**.
11. The **EMC CAVA Installer Information** window appears.

    You need to restart the system to complete the installation. Click **Yes** to restart immediately or **No** to restart at a later time.

Start the CAVA Calculator

About this task

The CAVA Calculator's online help provides more information about using CAVA Calculator.

Steps

1. Click the **EMC CAVA Tools** icon. The **CAVA Tools** window appears.
2. Select **File** > **New** if the CAVA Calculator is not in the CAVA Tools workspace.

Uninstall the CAVA Calculator

About this task

The CAVA Calculator is automatically uninstalled when the CEE software is uninstalled, and cannot be uninstalled by itself. Only use this procedure if you want to uninstall the CEE:

Steps

1. From the Windows taskbar, click **Start** and select **Settings** > **Control Panel** > **Add or Remove Programs**.
2. Select **Common Event Enabler Framework**.
3. Click **Remove**.
4. Close the **Add or Remove Programs** window.
5. Close the **Control Panel** window.

CAVA sizing tool

The CAVA sizing tool runs on Windows-based systems. The tool assists the system administrator in determining how many AV engines are necessary to provide adequate AV scanning across Dell systems.

The tool gathers information based on the specified AV machines queried, and returns statistics on each AV machine.

When you install CAVA on the AV machines, the CAVA sizing tool, cavamon.exe, is also installed. In addition, you can use the VB script, cavamon.vbs, to monitor the AV machines. However, cavamon.vbs does not perform sizing.

The heuristic in the sizing tool is set to size the CAVA environment for an average 60 percent saturation level (or workload level) in all AV machines in the environment. Users wanting to use their own heuristic for sizing can use the cavamon.vbs script for gathering CAVA statistics. These statistics can then be used as input to custom algorithms.

Configure the sizing tool describes configuration procedures.

CAVA sizing tool configuration overview

Configure one or more AV machines in the network as the monitoring CAVA sizing tool server—this is the server that you use can to monitor and size all other AV machines. The monitoring system, and all AV machines that you want to monitor, must be running the WMI subsystem. WMI is built into Windows systems.

NOTE: The CAVA sizing tool must run on an AV machine—you cannot run the sizing tool from any Windows machine in the domain.

The CAVA sizing tool must be enabled on the AV machines that you monitor. However, you do not have to configure the sizing tool on these machines. If you want the ability to monitor CAVA from multiple machines in the network, you can enable and configure the CAVA sizing tool on multiple machines.

The monitoring sizing tool server:

- Monitors all other Windows Servers running CAVA
- Monitors and gathers statistics on the AV engines
- Gathers and lists workload information for each individual AV engine
- Provides recommendations on how many AV engines are required to provide optimal antivirus protection

Configure the sizing tool

Prerequisites

The user account on the primary sizing tool server must have local administrative privileges.

About this task

Actions for configuring the sizing tool lists the actions you must perform to configure the sizing tool.

Table 10. Actions for configuring the sizing tool

Task	Action	Procedure
1.	Enable the sizing tool on the monitoring sizing tool server and on all AV machines that you want to monitor.	Enable the sizing tool
2.	Create the cavamon.dat file on the monitoring server. **NOTE:** Only needed if you use cavamon.exe to run the sizing tool.	Create the cavamon.dat file
3.	Start the sizing tool on the monitoring server.	Start the sizing tool
4.	Size the anivirus agent.	Size the antivirus agent
5.	Optionally run **cavamon.vbs**.	(Optional) Gather AV statistics with cavamon.vbs

Enable the sizing tool

About this task

Enable the sizing tool on the primary sizing tool server and on all AV machines that you want to monitor:

NOTE: If you enable the CAVA sizing tool and you want to enable local file system scanning on the AV machine, you should exclude the `%SYSTEMROOT%\system32\wbem\` directory from directories to be scanned.

Steps

1. Open the Windows Registry Editor by running **regedit.exe**.
2. Locate the **Sizing** entry in the left pane of the Registry Editor in the `HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CAVA\Sizing` directory.
3. Double-click the **Sizing** entry located in the right pane. The **Edit DWORD Value** dialog box for Sizing appears.
4. In the **Value data** field, type **1**. Click **OK**.
5. (Optional) To control how often CAVA sends information to the sizing tool, double-click the **SampleIntervalSecs** entry. The **Edit DWORD Value** dialog box for SampleIntervalSecs appears.
6. (Optional) In the **Value data** field, type a number, in seconds, from 1 to 60. The default value is 10 seconds. Click **OK**.

   NOTE: Do not type any decimal value greater than 60. Any number greater than 60 is not supported in Visual Basic.
7. Close the **Registry Editor**.
8. Restart CAVA, as described in Start, stop, and restart CAVA.

Manually compile the cee.mof file

About this task

If the cavamon.exe utility does not start, you must manually compile the Managed Object Format (MOF) file used by CEE CAVA.

Steps

1. Locate the **cee.mof** file (found in the `wbem` directory of the local Windows installation).
2. From a command prompt, change (cd) to the directory above and run the **`mofcomp cee.mof`** command.

Create the cavamon.dat file

About this task

If you run the sizing tool by running `cavamon.exe` (instead of using the script `cavamon.vbs`), you must create a `cavamon.dat` file. The `cavamon.dat` file contains the name or IP address of each AV machine that the sizing tool monitors.

NOTE: The `cavamon.vbs` script takes its input from the CLI when the script is run.

To create the `cavamon.dat` file:

Steps

1. Create a text file, named `cavamon.dat`, in the `Program Files\EMC\CEE` directory.
2. Add a line for each AV machine that you want to monitor. The file must contain either the IP address or machine name of each AV machine. Monitoring operates properly with both types of entries in the file.

   To find the name for a Windows Server, click **Start** in the taskbar, and select **Control Panel** > **Settings** > **System**. On a Windows Server, click the **Computer Name** tab.

   NOTE: You must enable the CAVA sizing tool for each AV machine that is listed in the `cavamon.dat` file.

3. Save and close the file.

Start the sizing tool

About this task

Steps

1. Restart the EMC CAVA service.
2. From the `Program Files\EMC\CEE` directory, run `cavamon.exe`.
3. Click **Get Stats** to start the monitoring process. The output is automatically updated every interval with the CAVA population statistics.

   NOTE: An interval, set in the sizing tool Registry entry, has a default of 10 seconds. Every interval, the sizing tool captures information about the AV machines defined in the `cavamon.dat` file.

4. Click **Stop Stats** to stop the monitoring process.

Size the antivirus agent

To start an analysis, click **Size** in the **CAVA Monitor** dialog box. The sizing tool collects data for 10 successive intervals, and then feeds this data into its heuristic algorithms. After the tool completes its session, the **Size** box shown at the bottom of the CAVA Monitor window displays the recommended numbers of AV machines.

(Optional) Gather AV statistics with cavamon.vbs

About this task

Steps

From a command window on the sizing tool system, run the following command. Use as many AV machine names as necessary:

`cscript cavamon.vbs <machine_name_1> <machine_name_2> <machine_name_3>`

where:

<machine_name_n> = machine name or IP address of the AV machine that you want to monitor

Example:

To get AV statistics, type:

`cscript cavamon.vbs \\WIN910108`

Output:

```
Server:\\WIN910108
AV Engine State:Up
AV Engine Type:TM ServerProtect
Files Scanned:127899
Health:Good
Msec Per Scan:19.85
Saturation %:3.45
Scans Per Second:0
CAVA State:NORMAL
CAVA Version:2.2.1
```

NOTE:

- The CAVA sizing tool must be enabled on all AV machines that you want to monitor.
- If you have any problems while running the script, download and install the Windows Script Host (available at https://www.microsoft.com).

13

Third-Party Consumer Applications

This chapter discusses setting up access to a third-party vendor application, which is used for managing the content stored on the file systems, and how to allow communication with CEE.

Topics:

Overview

A third-party consumer application can reside either on the same local Windows computer where the CEE is installed, or on another remote computer that is in the same domain as the Windows computer where the CEE is installed. The Windows computers that have the CEE installed but do not have the consumer applications installed will route events to the appropriate computer where the registered consumer application resides.

When both the consumer application and the CEE are installed on the local computer, communication between the applications occurs through local RPC (LRPC). When the consumer application is installed on a remote computer in the same domain, communication between the applications occurs through Microsoft RPC.

The consumer application registers through the publishing agent API on the CEE computer and specifies which events it will receive.

You determine the events for which you want to be notified, based on the consumer application used. See the AV documentation for the Dell platform you are using for a list of supported events.

The NAS server generates events for selected file system activity and sends them to a defined Windows Server that has the CEE installed, which then communicates with the consumer application, requesting a response. Depending on the type of consumer application used, policies can be checked and the appropriate response sent to the event publishing agent. If necessary, the appropriate response is sent to the user who performed the action.

Set up consumer application access

Steps

1. Open a command window on the Windows Server where the consumer application is installed and type **`regedit`**.

   The **Windows Registry Editor** window appears.

2. Navigate to:

   HKEY_LOCAL_MACHINE > **Software** > **EMC** > **CEE** > **CEPP** > ***<application>*** > **Configuration**

   where:

   <application> = type of consumer application being used.

3. Double-click **EndPoint**.
   - If the consumer application is installed on the local computer, type *<local vendor>*

     where:

     <local vendor> = name of the vendor on the local computer.
   - If the consumer application is installed on a remote computer, type *<vendor>*@*<IPaddr>*; *<vendor>*@*<IPaddr>*...

     where:

     <vendor> = name of the vendor.

<IPaddr> = IP addresses of the remote computers where the consumer application is installed. When setting multiple remote computers, you must use a ; (semicolon) to separate the IP addresses.

CEE monitors the state of the first audit partner defined in the list to determine whether to publish events. If the first partner in the list is not available, events are also not published to subsequent partners in the list. The availability of the first partner also determines whether the event is re-sent at a later time.

4. Double-click **Enable**.
   - Type either **0** to disable or **1** to enable the CEPA functionality that supports the consumer application being used.
5. Restart the computer.

Results

NOTE: Any time you modify the CEE section of the Registry, except for Verbose and Debug, you need to restart the EMC CAVA service.

Index

S

T

V

W