Dell EMC CEE

Version 8.6

Using the Common Event Enabler on Windows Platforms

P/N 302-002-456 REV. 04

EMC²

Copyright © 2011-2019 Dell Inc. or its subsidiaries. All rights reserved.

Published February 2019

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.“ DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

Preface

As part of an effort to improve and enhance the performance and capabilities of its product lines, revisions of product hardware and software are periodically released. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, please contact your Customer Support representative.

Special notice conventions used in this document

DANGER

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Addresses practices not related to personal injury.

Note

Presents information that is important, but not hazard-related.

Where to get help

Support, product, and licensing information can be obtained as follows:

Product information—For documentation, release notes, software updates, or for information about products, licensing, and service, go to Online Support (registration required) at http://Support.EMC.com.

Troubleshooting—Go to Online Support. After logging in, locate the applicable Support by Product page.

Technical support—For technical support and service requests, go to Customer Service on Online Support. After logging in, locate the applicable Support by Product page, and choose either **Live Chat** or **Create a service request**. To open a service request through Online Support, you must have a valid support agreement. Contact your product's sales representative for details about obtaining a valid support agreement or with questions about your account.

Note

Do not request a specific support representative unless one has already been assigned to your particular system problem.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications.

Please send your opinion of this document to:

```
techpubcomments@EMC.com
```

CONTENTS

CHAPTER 1

Introduction

This section discusses Dell EMC Common Event Enabler (CEE).

Topics included are:

About CEE

The Dell EMC 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 auditing, content/quota management (CQM), and Common Asynchronous Publishing Service (VCAPS)

CAVA provides an antivirus solution for Dell EMC systems (for example, the VNX® series). It uses an industry-standard Common Internet File System (CIFS) 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.

Note

VNXe® customers should refer to *Using a VNXe System with CIFS Shared Folders* on Online Support for specific CAVA information.

CEPA is a mechanism whereby applications can register to receive event notification and context from sources such as VNX or Dell EMC Unity. 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.
- 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.
- VCAPS—A mechanism for delivering post-events in asynchronous mode. The delivery cadence is based on 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

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 VNX and Dell EMC Unity™ customers who want to use consumer applications (such as for quotas or content type) to manage content stored on file systems.

System requirements

Table 1 on page 11 describes the Dell EMC software, hardware, network, and storage configurations.

Table 1 System 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 EMC E-Lab™ Interoperability Navigator for consumer applications supported when using CEE, CAVA, and CEPA.
Hardware	No specific hardware requirements.
Network	The Windows network must contain a domain controller with Active Directory and DNS enabled. VNX and Dell EMC Unity systems must be configured with the SMB/CIFS protocol. You cannot use a Virtual Data Mover (VDM) for the SMB/CIFS protocol. *Configuring and Managing CIFS on VNX* provides more information on configuring the CIFS protocol on a VNX. *Using a VNXe System with CIFS Shared Folders* provides more information on configuring the CIFS protocol on a VNXe. *Configuring Hosts to Access SMB File Systems* provides more information on configuring the SMB protocol on a Unity system.
Storage	No specific storage requirements.

For the latest system requirements of CAVA, consult the website or documentation of the particular third-party AntiVirus (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.

.NET Framework system requirements for Windows 8 and Windows Server 2012

Windows 8 and Windows Server 2012 install and enable by default the .NET Framework 4.5. However, the CEE Framework, "cava.exe", is a .NET Framework 3.5

service. You must enable .NET Framework 3.5. The Microsoft website contains instructions on enabling the .NET Framework 3.5 on Windows 8 and Windows 2012 at:

http://msdn.microsoft.com/ens/library/hh506443.aspx

Restrictions

The following are known limitations at the time of publication.

AV engines
Currently, no known limitations exist for the number of AV engines configured in the viruschecker.conf file. All AV engines are surveyed every 10 seconds (by default) 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 VNX Data Mover or Dell EMC Unity NAS server should have a CAVA pool consisting of a minimum of two CAVA servers. This is specified in the Data Mover's or NAS server's viruschecker.conf file. Configuring viruschecker.conf on page 55 provides more information.

For Dell EMC Unity systems, use Unisphere to create and manage Events Publishing details for a NAS server.

CEPA pools
In VNX and Dell EMC Unity systems:

- For post-events and post-error events, you can define up to three CEPA pools.
- For pre-events, you can define only one CEPA pool.

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.

File-level retention
It is strongly recommended that the AV administrator update the virus definition files on all resident AV engines in the CAVA pools, and periodically run a full file system scan of the file system to detect infected file-level retention (FLR) files. *Using VNX File-Level Retention* provides detailed information about FLR files.

For VNX systems, to run a full file scan from the Control Station, use the `server_viruschk -fsscan` command. For Dell EMC Unity systems, to run a full file scan, use the `svc_cava` command. When an infected FLR file is discovered, the resident AV engine records the presence of the infection and its location in the log file of the resident scan engine. Although an administrator cannot fix or remove the infected file, the file's read access can be restricted to make the file unavailable. The infected file can only be deleted after its retention date has passed.

The scan-on-first-read functionality of CAVA does not detect a virus in an FLR file.

Non-SMB/CIFS protocols
The Dell EMC antivirus solution is only for the clients running the SMB/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) to be in the local administrators group of a VNX for File SMB/CIFS server or a Dell EMC Unity NAS server. If the SMB/CIFS server or NAS server has Restricted Group GPO enforced and the AV user account is removed from the local administrators group, after the next CAVA restart the status will change from ONLINE to AV_NOT_FOUND. To ensure that the CAVA status remains ONLINE, you must either include the corresponding AV user account in the Restricted Group, or remove the Restricted Group.

Configuration file
For VNX systems, you must manually create the cepp.conf file before using CEPA. Create the cepp.conf file on page 64 provides details.

For Dell EMC Unity systems, use Unisphere to create and manage Events Publishing details for a NAS server.

FTP protocol
CEPA is only for the clients that run either the SMB/CIFS or NFS protocol. If the FTP protocol is used to move or modify files, no events are processed or published for the files.

CAVA and CEPA servers
Each VNX Data Mover or Dell EMC Unity NAS Server should specify:

- A CAVA pool consisting of a minimum of two CAVA servers, or
- A CEPA pool consisting of a minimum of two CEPA servers.

User interface choices

The system offers flexibility in managing networked storage based on the support environment and interface preferences. This guide describes how to configure CAVA and CEPA on a VNX by using the command line interface (CLI).

You can also perform some of these tasks by using the following management applications:

- Dell EMC Unisphere® software
- Dell EMC Unity/VNX/VNXe NAS Management snap-in
- Microsoft Management Console (MMC) snap-ins
- Active Directory Users and Computers (ADUC) extensions

Installing Management Applications on VNX for File includes instructions on launching Dell EMC Unisphere software, and on installing the MMC snap-ins and the ADUC extensions.

For VNX and Dell EMC Unity systems, this document also describes how to manually create a configuration file, assign the EMC Event Notification Bypass privilege to suppress third-party application events, and issue commands by using the CLI. The *EMC VNX Command Line Interface Reference for File* provides full descriptions of the commands.

Related information

Specific information related to the features and functionality described in this guide is included in:

- *Parameters Guide for VNX for File*
- *Managing a Multiprotocol Environment on VNX*
- *Configuring and Managing CIFS on VNX*
- *EMC VNX Command Line Interface Reference for File*
- VNX for File man pages
- 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
- McAfee VirusScan documentation
- McAfee Endpoint Security Threat Prevention documentation
- Microsoft Forefront Endpoint Protection 2010 documentation
- Microsoft System Center 2012 Endpoint Protection documentation
- Sophos Anti-Virus documentation
- Symantec Endpoint Protection documentation
- Trend Micro ServerProtect for EMC documentation

EMC VNX documentation on Online Support

The complete set of EMC VNX series customer publications is available on Online Support. To search for technical documentation, go to http://Support.EMC.com. After logging in to the website, click **Support by Product** and type **VNX series** in the Find a Product text box. Then search for the specific feature required.

Use of the term Windows Server

The term Windows Server is used in the document to depict both Windows Server 2012 and Windows Server 2008 operating systems.

CHAPTER 2

Concepts

Topics included are:

CAVA and CEPA concepts

CAVA overview

VNX and Unity are resistant to the invasion of viruses because of their architecture. Each VNX Data Mover or Unity NAS server runs data access in realtime software, which is an embedded operating system. Resistance to viruses occurs because third parties are unable to run programs containing viruses on a Data Mover or NAS server.

Although the Data Mover or NAS server is resistant to viruses, Windows clients also require virus protection. Virus protection on the client reduces the chance that the client will store an infected file on the server, and protects the client if it opens an infected file.

VNX and Unity antivirus solutions use a combination of a VNX Data Mover or Unity NAS server; a CAVA agent; and a third-party antivirus engine. The CAVA software and a third-party AV engine must be installed on a Windows machine in the domain.

CEPA overview

VNX and Unity are responsible for:

- Creating event notifications (event and its associated context)
- Sending the event package into the CEPA pool

The CEPA pool is responsible for:

- Maintaining a topology and state mapping of all consumer applications
- Delivering event type and associated event metadata through the CEPA API

AntiVirus partners

Dell EMC 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
- McAfee VirusScan
- McAfee Endpoint Security Threat Prevention
- Microsoft Forefront Endpoint Protection 2010
- Microsoft System Center 2012 Endpoint Protection
- Sophos Anti-Virus
- Symantec Endpoint Protection
- Symantec Protection Engine
- Trend Micro ServerProtect for EMC

This list was correct at the time of publication. The Dell EMC 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 on page 25 contains further information about supported third-party antivirus software.

CAVA and Data Mover or NAS server

On Unity, you can configure a NAS server.

On VNX, you can configure a CIFS server on a physical Data Mover or on a VDM. The CIFS servers are typically configured on a VDM (one or more VDMs on a physical Data Mover). However, for CAVA to work, you must have a CIFS server configured on the physical Data Mover against which the virus checking will be done, and the user rights or permissions must be assigned against this CIFS server. This is the global CIFS server or the default CIFS server on the physical Data Mover.

Note

For VNX, all file systems or shares can be mounted on a VDM. However, CAVA will scan all the file systems on the physical Data Mover covering all VDMs and all CIFS servers.

CAVA features

When CAVA is used with one of the supported third-party antivirus applications listed in AntiVirus partners on page 16, the following features are available:

- Load balancing and fault tolerance on page 17
- Scan-on-first-read on page 18
- Updating virus definition files on page 18
- Scan on write on page 18
- CAVA sizing tool on page 18
- CAVA Calculator on page 19
- Virus-checking continuation on page 19
- Scanning after definition file update (manual process) on page 20

Load balancing and fault tolerance

You can use the CAVA Calculator and the CAVA sizing tool to determine the number of AV machines that the system requires. The CAVA Calculator can help you prior to installation, and you can use it to run what-if scenarios after installation. The CAVA sizing tool collects information from a running environment to give you a recommendation on the number of AV machines needed. If fault tolerance is a concern, you should configure a minimum of two AV machines in the network. If one of the AV machines goes offline or cannot be reached by the VNX or Unity, having two AV machines ensures that the file scanning capability is maintained.

If you have more than one AV machine on the network, the VNX or Unity balances workloads among the AV machines by distributing the scanning jobs in a round-robin fashion. For example, if one AV machine goes offline, the VNX or Unity distributes the scanning load among the other available AV machines.

Note

Each file is scanned by one AV machine. You cannot configure CAVA so that a file is simultaneously scanned by multiple AV machines by running different AV software.

Scan-on-first-read

CAVA uses the access time of a file to determine if a file should be scanned. The access time is compared with a time reference stored in the EMC CAVA service. If the file's access time is earlier than the reference time, the file is scanned on read before it is opened by the SMB/CIFS client.

For VNX systems, set the access time by using the `server_viruschk` command. The *EMC VNX Command Line Interface Reference for File* provides more information about the `server_viruschk` command.

For Unity systems, set the access time by using the `svc_cava` command. *Unity Service Commands Technical Notes* provides more information about the `svc_cava` command.

CAVA updates the scan-on-first-read access time when it detects a virus definition file update on the AV engine.

Updating virus definition files

CAVA can automatically detect a new version of the virus definition file and update the access time. To use this feature you must have scan-on-first-read enabled. Currently, the latest versions of all supported third-party antivirus engines support automatic pattern updates. The *VNX Operating Environment for File Release Notes* and the Dell EMC E-Lab Interoperability Navigator provide the latest information on other antivirus products.

Scan on write

CAVA initiates a scan after a file is modified and closed. If a file is opened, but no modifications made to it, it is not scanned upon closing it.

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 VNX and Unity 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 on page 101 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

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 EMC systems (for example, the VNX series), whereas the sizing tool uses the actual workload. This utility is installed as part of CEE framework. System requirements on page 11 provides more information.

Virus-checking continuation

This feature stores the paths of all unscanned files whenever virus scanning is interrupted, such as in the following circumstances:

- Data Mover or NAS server restarts — The list of unscanned files is stored in a directory reserved by the panic handler software. When the Data Mover or NAS server restarts, the virus checker reads the list of unscanned files, and then scans the files.
- Virus checking is stopped or a file system is unmounted — The list of unscanned files is stored in a special file on the file system. When the virus checker is restarted or the file system is remounted, the virus checker reads the unscanned list and scans the files.

The list of unscanned files is stored in the /.etc/viruschecker.audit file on each Data Mover or NAS server.

On a VNX, use this command to manually update this file.

1. Store the list of unscanned files by using this command syntax:
   ```
   $ server_viruschk <movername> -audit
   ```
   where:

   <movername> = name of the Data Mover

For Unity systems, use Unisphere to manually update configuration information.

1. Under **Storage**, select **File** > **NAS Servers**.
2. Select the relevant NAS Server, and then select the **Edit** icon.
3. On the **Security** tab, select **Antivirus**.

4. Select **Retrieve Current Configuration**.
5. Edit the configuration file, and then save the changes.
6. Select **Upload new configuration** to upload the updated configuration file.

Scanning after definition file update (manual process)

To verify files after the third-party antivirus definition file is updated, you must run the `server_viruschk -set accesstime` command (VNX systems) or `svc_cava -set accesstime` *<time>* command (Unity systems). CAVA also supports scanning for compressed files (for example, files with the `.zip` extension), if the third-party antivirus software (AV engine) supports the scanning of compressed files.

Virus-checking client

The virus-checking (VC) client is the agent component of VNX software on the Data Mover, or Unity software on a NAS server. The VC client interacts with the AV engine, which processes requests from the VC client. Scanning is supported only for SMB/CIFS access. While the scan or other related actions are taking place, access to the file from any SMB/CIFS client is blocked.

The VC client does the following:

- Queues and communicates filenames to the antivirus agent for scanning.
- Provides and acknowledges event triggers for scans. Possible event triggers include:
  - A file is renamed on VNX or Unity
  - A file is copied or saved to VNX or Unity
  - A file is modified and closed on VNX or Unity

  Note

  Table 2 on page 21 provides a detailed list of scanning triggers.
- Requests a virus check by sending the universal naming convention (UNC) pathname to the antivirus agent.
- Allows the AV engine to perform the correct user-defined action on the file when the file is discovered to contain a virus. User-defined actions include:
  - Curing or repairing the file
  - Renaming the file
  - Changing the file extension
  - Moving the file to a quarantined area
  - Deleting or purging the file

  Note

  The AV engine maintains full access to the file being scanned while performing the user-defined action on the file. After completion, the AV engine returns control of the file to the VC client.
- If the antivirus agent reports that the file was successfully scanned, VNX or Unity allows the file to be available to the client.
- If multiple instances of the antivirus agent have been installed, the VC client sends scanning requests to the AV machines in a round-robin method.

Basic VC client configuration

The VC client can be configured by using the `server_viruschk` command and the `viruschecker.conf` file. An alternative method uses the EMC Unity/VNX/VNXe AntiVirus snap-in, which is part of the Unity/VNX/VNXe NAS Management snap-in. (Optional) Install EMC Unity/VNX/VNXe NAS Management snap-in on page 76 provides more information.

Full file system scan

An administrator can perform a full scan of a file system by using the `server_viruschk -fsscan` command (VNX systems) or `svc_cava -fsscan` command (Unity systems). To use this feature, CAVA must be enabled and running. The administrator can query the state of the scan while it is running, and can stop the scan if necessary. For VNX systems, a file system cannot be scanned if the file system is mounted with the option `noscan`. As the scan proceeds through the file system, it touches each file and triggers a scan request for each file.

Scanning quick glance chart

Table 2 on page 21 explains when virus scanning occurs.

Table 2 Scanning quick glance chart

On the Data Mover/NAS server	Does scanning occur
Read a file (scan-on-first-read)	Yes
Move or copy a file	Yes
Create and save a file	Yes
Modify and close a file	Yes
Restore from a backup, only if it needs to restore a file (write)	Yes
Rename: New name (extension is not in `masks=` and is in `excl=`) [a]	No
Rename: Original filename (extension is not in `masks=` and is not in `excl=`), new name (extension is not in `masks=` and is not in `excl=`) has same extension[a]	No
Rename: Original filename (extension is not in `masks=` and is not in `excl=`), new name (extension is in `masks=` and is not in `excl=`) has different extension[a]	Yes
Rename: Original filename (extension is in `masks=` and is not in `excl=`), new name (extension is in `masks=` and is not in `excl=`)[a]	No

Note

`masks=` and `excl=` are defined in the `viruschecker.conf` file. The `masks=` is set to `*.*` and the antivirus engine is configured to scan all files.

a. If masks=*.*, renames will not trigger scanning. If the masks option does not equal *.* (that is, *.exe, *.bat), then a trigger will occur.

Note

When virus checking is enabled, two clients cannot concurrently write to the same file. The first client that requests the file opens the file for write access. The second client must wait until the file is closed by the first client, and, if the first client modified the file, until the file is checked by the AV machines.

The cepp.conf file

Note

The `cepp.conf` file is used for VNX systems only. For Unity systems, the configuration details are created when setting up Events Publishing for each NAS server in Unisphere (**Storage** > **File** > **NAS Servers** > **Properties** > **Protection & Events** > **Events Publishing**).

The `cepp.conf` file contains information that is necessary to connect one or more VNX Data Movers to the Windows machines that are running the CEE software. The administrator must create a configuration file that contains at least one event, one pool, and one server. All other parameters are optional. The `cepp.conf` file resides on the VNX Data Mover.

To use CEPA, each VNX Data Mover that runs the EMC CAVA service must have a valid `cepp.conf` file on it or the EMC CAVA service will not start.

Examples of cepp.conf

Example 1 on page 22 shows a `cepp.conf` file that uses one continuous line for most of the options except for the global options, each of which is on its own line. Depending on the text editor being used, the information can wrap to additional lines, but will be treated by the system as one continuous line. Example 2 on page 23 shows the same `cepp.conf` file with separate lines for all options. Example 3 on page 23 shows a `cepp.conf` file that specifies multiple pools for post events.

Note

`httpport`, `cifsserver`, `surveytime`, `ft`, and `msrpcuser` are global options that are always written on separate lines. Do not add "\" at the end of the lines that contain `httpport`, `cifsserver`, `surveytime`, `ft`, and `msrpcuser`.

Example 1

```
httpport=12228
cifsserver=dbms
surveytime=90
ft level=1 location=/fs1 size=5
msrpcuser=user1
pool name=pool1 servers=128.221.252.1:[2510:0:175:111:0:4:aab:ad2]
preevents=* postevents=* posterrevents=* option=ignore
reqtimeout=500
retrytimeout=50
```

Note

IPv6 addresses should be enclosed in square brackets to separate them from the colon delimiter that is used between multiple addresses.

Example 2

```
httpport=12228
cifsserver=dbms
surveytime=90
ft level=1 location=/fs1 size=5
msrpcuser=user1
pool name=pool1 \
servers=128.221.252.1:[2510:0:175:111:0:4:aab:ad2] \
preevents=* \
postevents=* \
posterrevents=* \
option=ignore \
reqtimeout=500 \
retrytimeout=50
```

Note

Table 9 on page 66 contains the list of valid pre-event, post-event, and post error event values.

Note

You must include a space before a "\" used at the end of a line. The "\" is not used on the last line or on lines that contain any of the five global options.

Example 3

```
httpport=12228
cifsserver=dbms
surveytime=90
ft level=1 location=/fs1 size=5
msrpcuser=user1
pool name=pool1 servers=omega43.w2k8r2.cee.com postevents=*
pool name=pool2 servers=omega45.w2k8r2.cee.com postevents=*
```

Assign rights

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 MMC 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 VNX Data Mover or Unity NAS Server. *Installing Management Applications on VNX for File* contains installation instructions for the MMC snap-in.

Note

You cannot use Microsoft Windows Local Policy Setting tools to manage user rights assignments on a VNX Data Mover or Unity NAS Server because the tools do not allow you to remotely manage user rights assignments.

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 system. The consumer applications require event notifications, from the VNX Data Mover or Unity NAS server, to organize the access of information that is stored on the file system. 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 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.

CHAPTER 3

Installing Third-Party Application Antivirus Engines

Topics included are:

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 on page 43 contains instructions on installing CEE.

NOTICE

All packages except Trend Micro ServerProtect must be installed prior to installing CAVA (as part of CEE). Install Trend Micro ServerProtect on page 41 provides more information.

If you are installing one of the following third-party antivirus software applications, use the installation path shown in Table 3 on page 26.

- Computer Associates *e*Trust
- F-Secure AntiVirus
- Kaspersky Anti-Virus for Windows Servers Enterprise Edition
- McAfee VirusScan
- Microsoft Forefront Endpoint Protection 2010
- Microsoft System Center 2012 Endpoint Protection
- 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 on page 47
2.	Configure virus-checking parameters on VNX Data Movers or Unity NAS servers.	Configuring viruschecker.conf on page 55
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 on page 43
5.	Start the virus-checking client on VNX Data Movers or Unity NAS servers.	Managing the VC Client on page 69
6.	Verify the CAVA installation.	Verify the installation on page 72

If you are installing McAfee Endpoint Security (ENS) Threat Prevention, use the installation path shown in Table 4 on page 27.

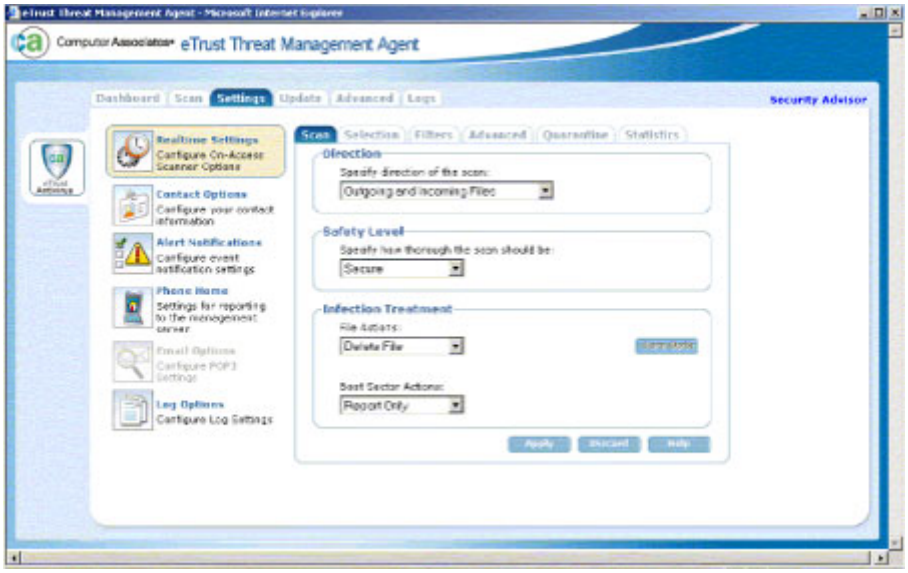
Table 4 McAfee Endpoint Security Threat Prevention installation procedure

Step	Action	Procedure
1.	Install the McAfee ENS AV engine on the Windows AV machine.	McAfee Endpoint Security Threat Prevention on page 35
2.	Install CAVA (as part of CEE) on the Windows AV machines.	Installing the Common Event Enabler on page 43
3.	Start the virus-checking client on VNX Data Movers or Unity NAS servers.	Managing the VC Client on page 69
4.	Verify the CAVA installation.	Verify the installation on page 72

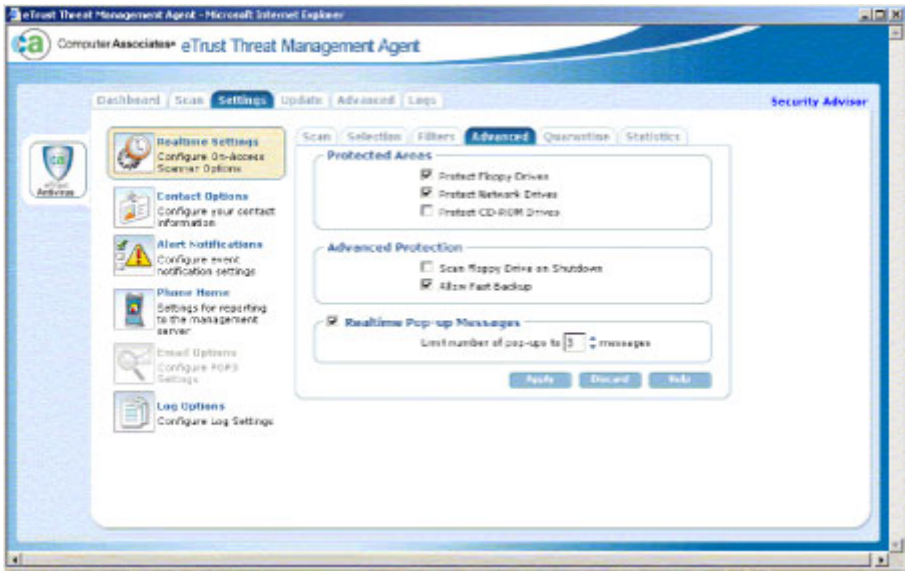
Computer Associates *e*Trust

Procedure

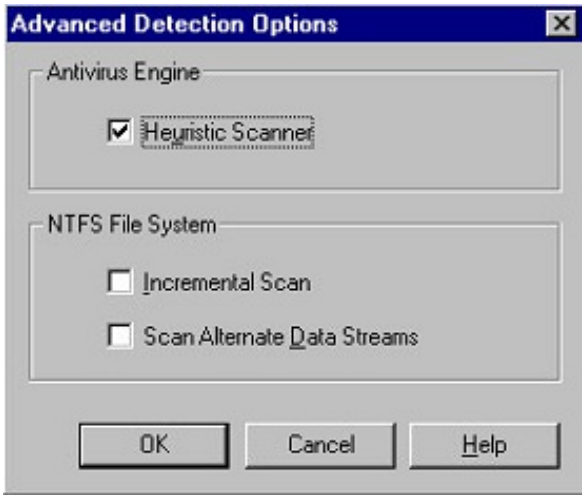
1. Install the *e*Trust application on an AV machine to interface with CAVA. Computer Associates documentation provides specific installation steps.
2. Start the application, and navigate to the **eTrust Threat Management Agent** window.
3. On the **eTrust Threat Management Agent** window, click the **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 on page 43 (to install CAVA as part of CEE).

F-Secure AntiVirus

Procedure

1. Install one of the following on a machine where you will install CEE/CAVA (v6.0.0 or later). The F-Secure documentation provides specific installation steps:
   - F-Secure E-mail and Server Security 9.20 with F-Secure hotfix FSESS920-900, or
   - F-Secure Server Security 9.20 with F-Secure hotfix FSSS920-900
2. Install CEE/CAVA (v6.0.0 or later). Go to Installing the Common Event Enabler on page 43.

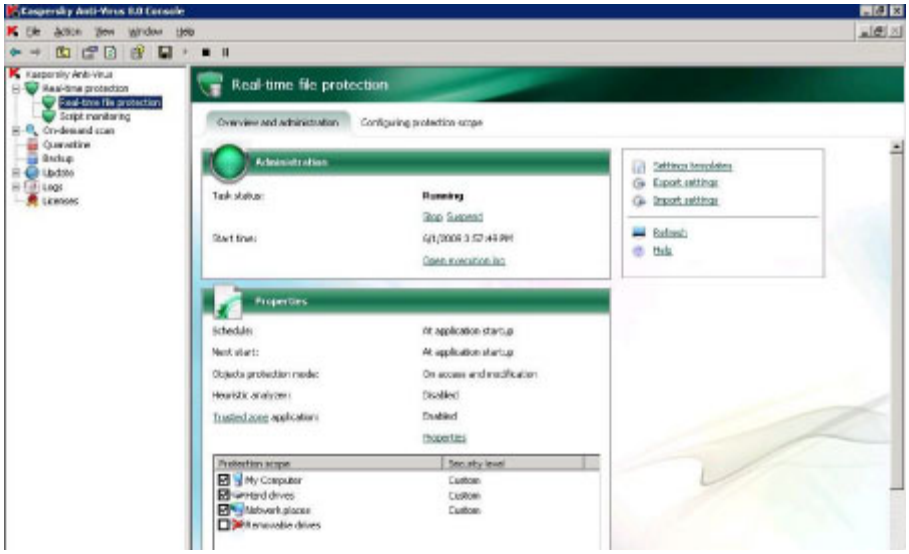
Results

The installation of the F-Secure hotfix pre-configures the F-Secure AV engine for use with CEE/CAVA.

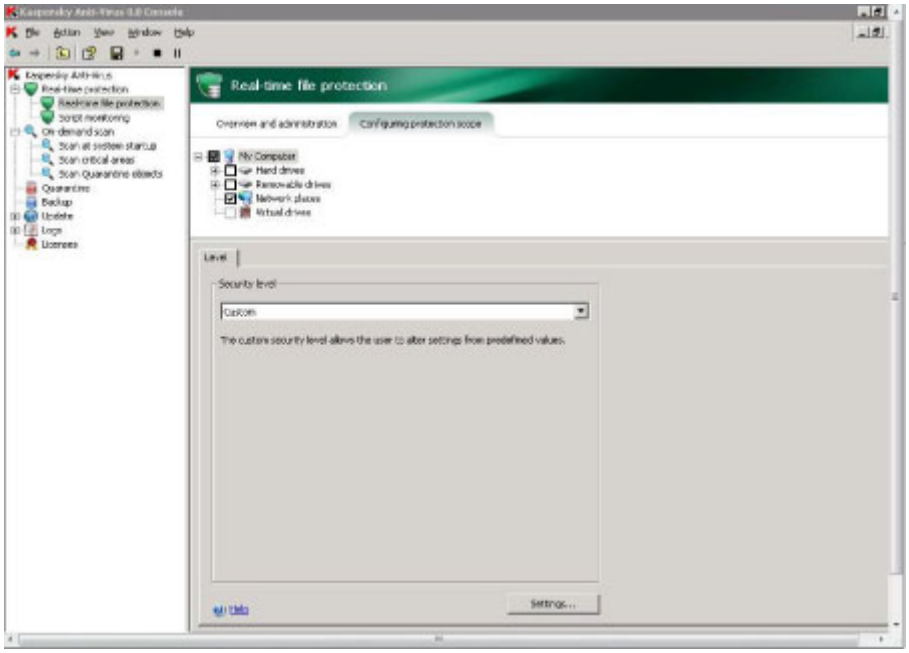
Kaspersky Anti-Virus

Procedure

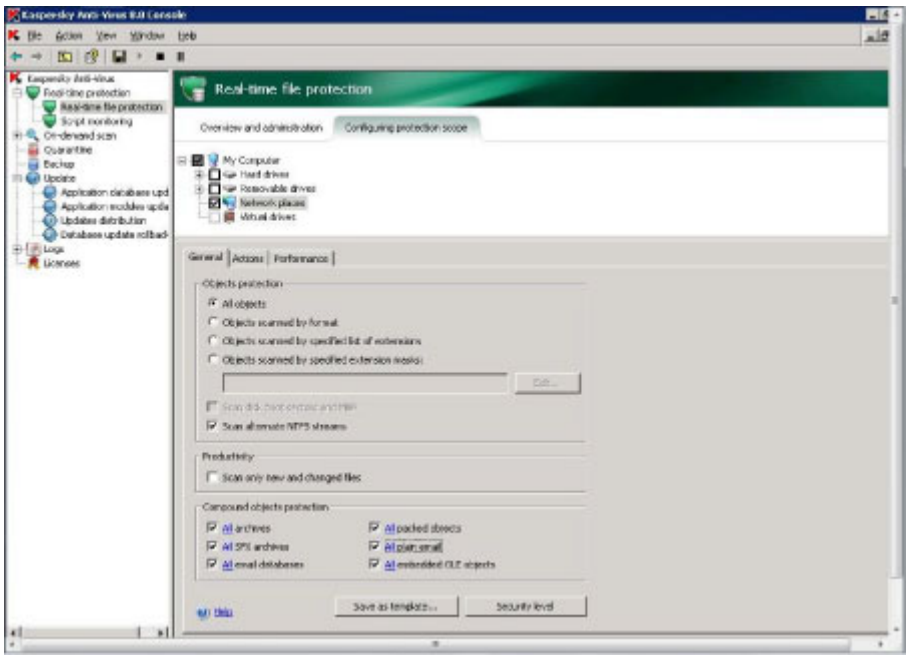
1. Install Kaspersky Anti-Virus for Windows Servers Enterprise Edition on a server that will interface with the AV machine. Kaspersky documentation provides specific installation steps.
2. Open the **Kaspersky Anti-Virus MMC Console**.
3. In the left pane, select **Real-time protection** and then **Real-time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

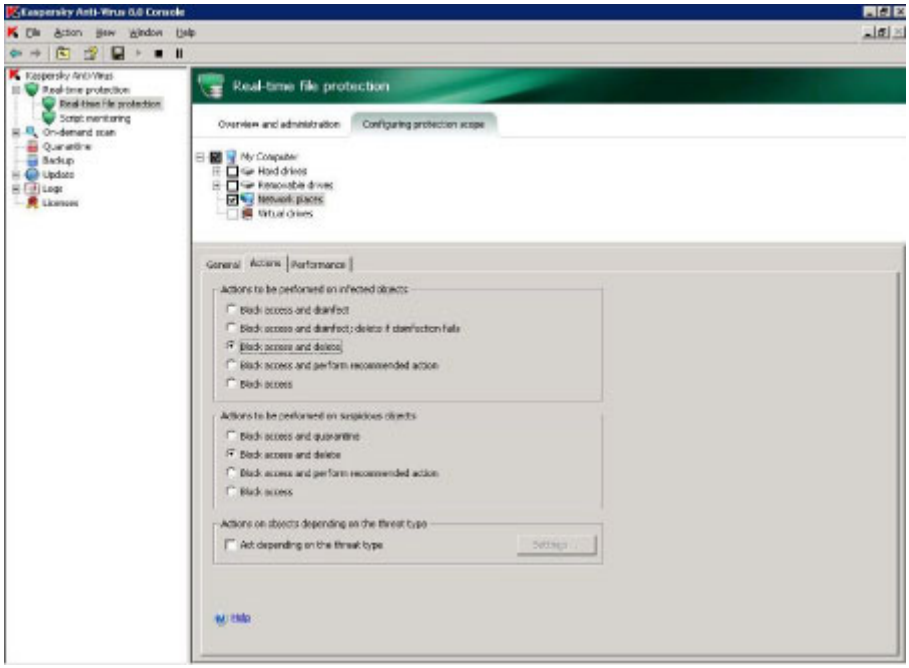
- Block access and delete
- Block access and perform recommended action

Note

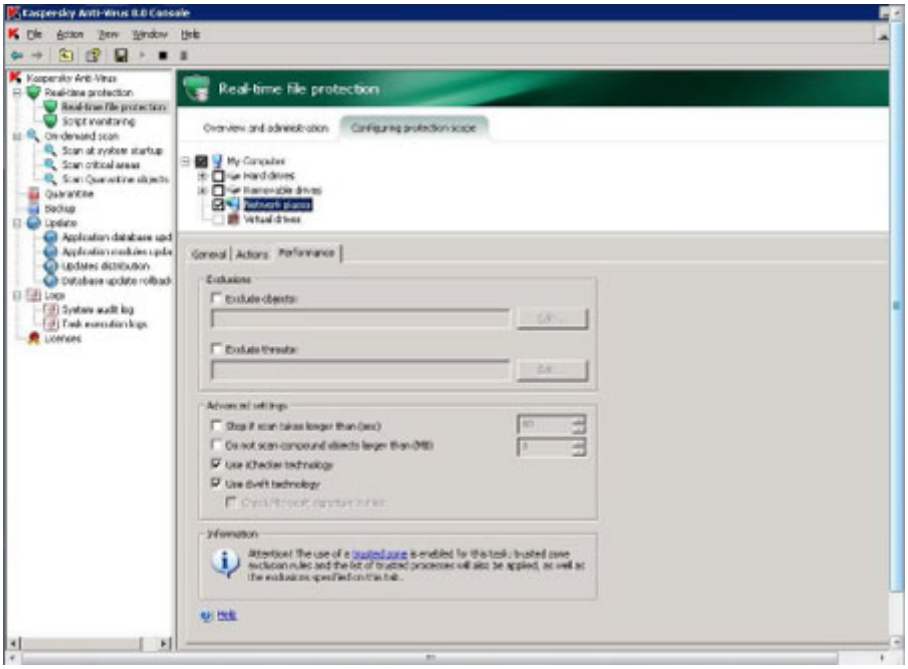
Block access does not work with CAVA.

In **Actions to be performed on suspicious objects**, select one of the following options:

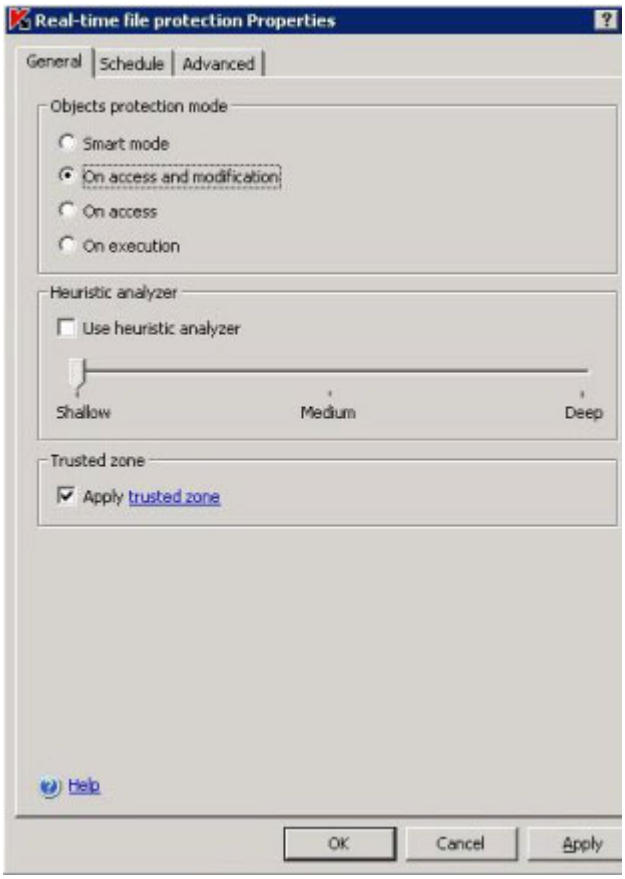
- Block access and quarantine
- Block access and delete
- Block access and perform recommended action



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 on page 43 (to install CAVA as part of CEE).

McAfee VirusScan

A default setting for a file scanning cache option that is used by VirusScan has been changed. With this change, network files may not be scanned after being cached. This issue occurs when the same file is sent multiple times to an Dell EMC VNX or Unity device. If you are using McAfee VirusScan version 8.8 or later, read McAfee's KnowledgeBase article for instructions on how to prevent this condition.

Procedure

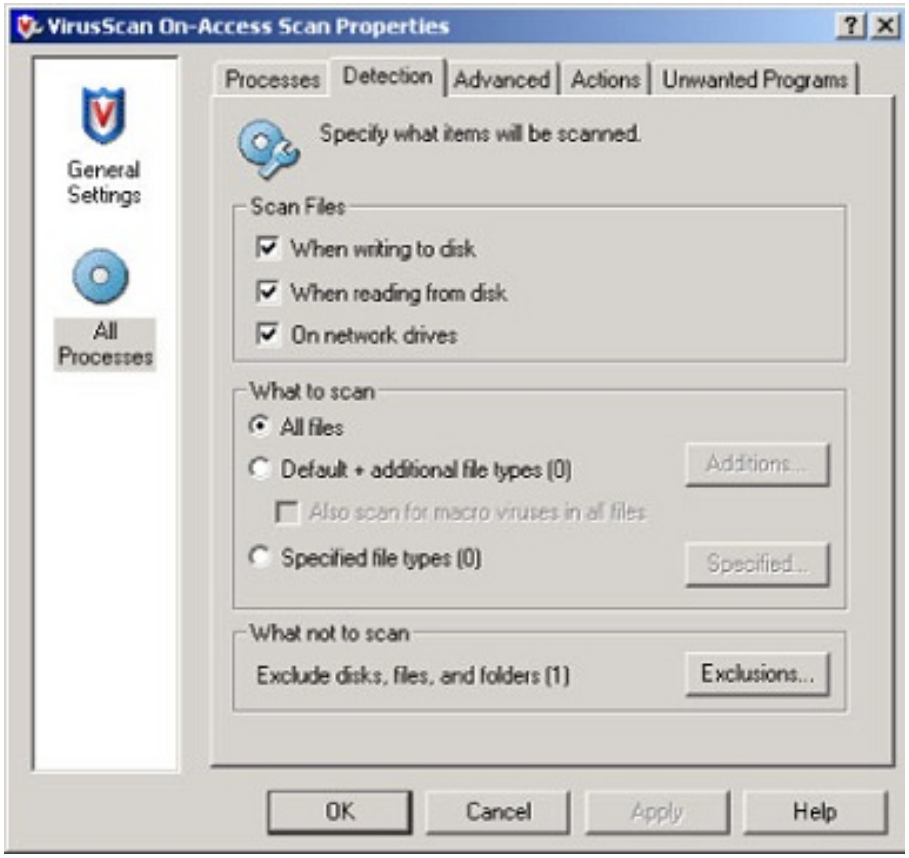
1. Create a temporary directory on the hard drive of an AV machine to interface with CAVA, and extract the VirusScan release files into that directory. McAfee documentation provides specific installation steps.
2. Install and start the application.

Note

If you are upgrading VirusScan, create a backup copy of the MCSHIELD.EXE file. Copy this file to a different directory or rename the file with a different extension.

---

3. Open the **VirusScan On-Access Monitor**, and click **Properties**. The **VirusScan Properties** dialog box appears.
4. On the **VirusScan Properties** window, click **Detection**. The **Detection** tab appears.

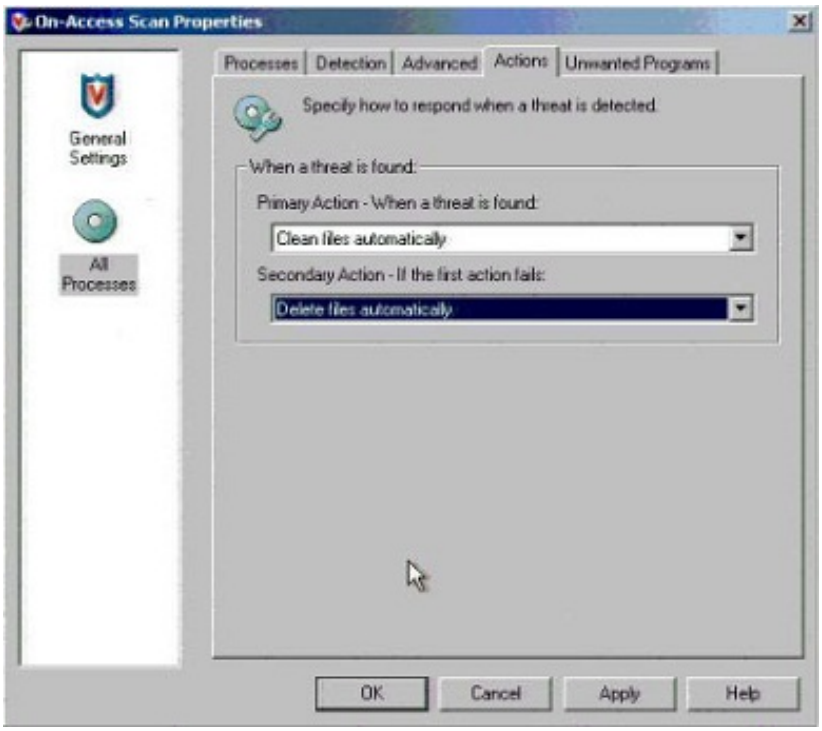


5. From the **Detection** tab, select the following:
   a. In **Scan Files**, select:
      - When writing to disk
      - When reading from disk
      - On network drives
   b. In **What to scan**, select **All files**.

   Note

   If you are running McAfee version 7.1 or later, it is critical to have **When reading from disk** selected.

6. Click **Apply**.
7. On the **VirusScan Properties** window, click **Actions**. The **Actions** tab appears.



8. From the **Actions** tab, perform the following:
   a. From the **When a threat is found** list, select one of the following options:
      - **Clean files automatically**: This automatically cleans the infection (if it can be cleaned). If the infection cannot be cleaned, the file is left in place and the extension VIR is appended to the filename.
      - **Delete files automatically**: This automatically deletes infected files.
   b. Click **Apply**.

   Note

   Optionally, you can configure the **Response to user** options.

9. Close the **VirusScan Properties** window. Go to Installing the Common Event Enabler on page 43.

McAfee Endpoint Security Threat Prevention

The necessary configuration options for using Endpoint Security (ENS) Threat Prevention with CAVA are incorporated into the ENS installation. Refer to the appropriate McAfee documentation and Knowledgebase articles for additional information.

After installing McAfee Endpoint Security Threat Prevention, go to Installing the Common Event Enabler on page 43.

Microsoft Forefront Endpoint Protection 2010

Procedure

1. On a machine where you will install CEE/CAVA (v6.0.0 or later), install Microsoft Forefront Endpoint Protection 2010 with hotfix KB2758685 or later. The Microsoft Forefront Endpoint Protection 2010 documentation provides specific installation steps. Updates to Microsoft Forefront Endpoint Protection 2010 are available by using Microsoft's Windows Update.
2. After installation, verify that Microsoft Antimalware Client Version 1.522.0 or later is running. If it is not running, contact Microsoft Support.
3. Install CEE/CAVA (v6.0.0 or later). Go to Installing the Common Event Enabler on page 43.

Microsoft System Center 2012 Endpoint Protection

Procedure

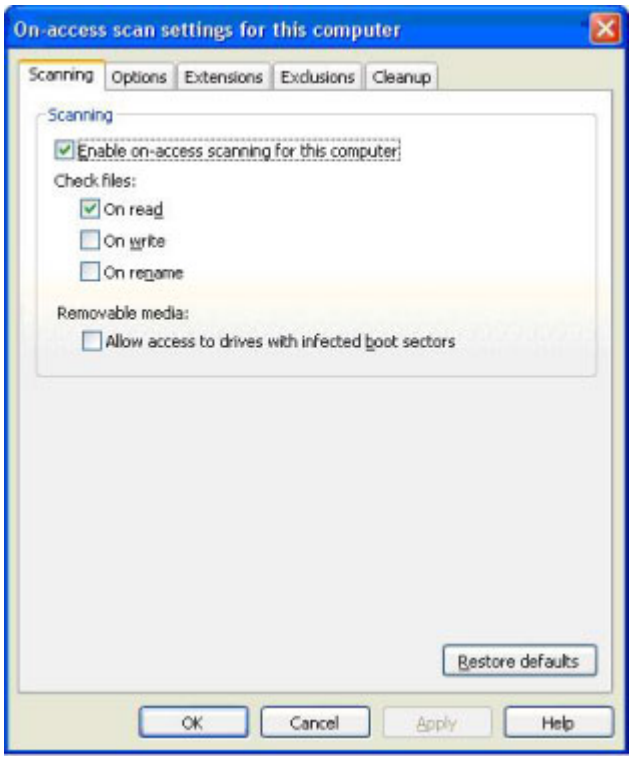
1. On a machine where you will install CEE/CAVA (v6.0.0 or later), install Microsoft System Center 2012 Endpoint Protection. The Microsoft System Center 2012 Endpoint Protection documentation provides specific installation steps. Updates to Microsoft System Center 2012 Endpoint Protection are available by using Microsoft's Windows Update.
2. After installation, verify that Microsoft Antimalware Client Version 1.522.0 or later is running. If it is not running, contact Microsoft Support.
3. Install CEE/CAVA (v6.0.0 or later). Go to Installing the Common Event Enabler on page 43.

Sophos Anti-Virus

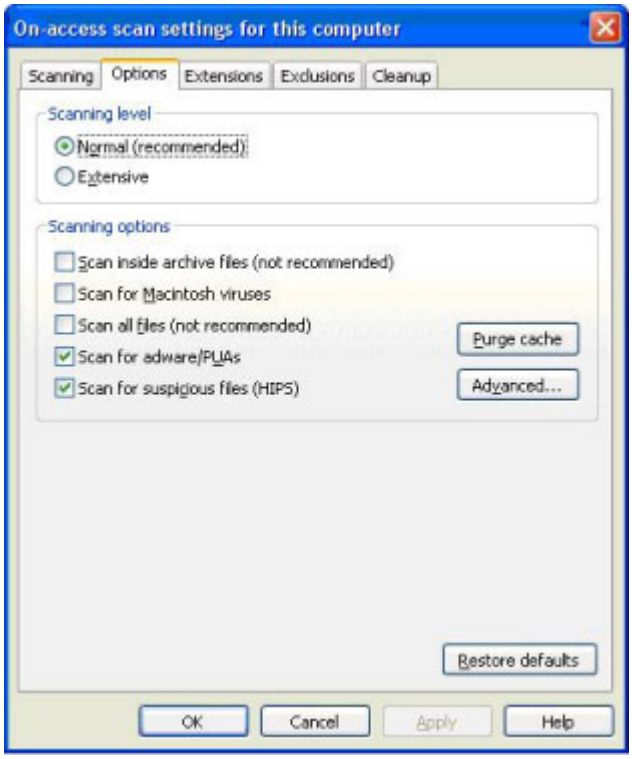
Procedure

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.

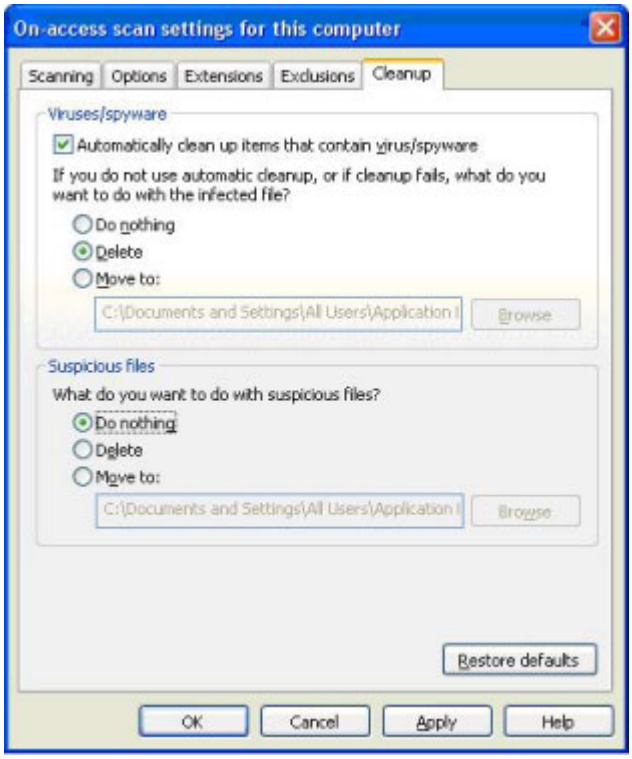
5. On the **Scanning** tab, ensure that **Enable on-access scanning for this computer** is selected and select **On read**.



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 on page 43.

Symantec Endpoint Protection

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:

Procedure

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

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

Procedure

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

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

Procedure

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.

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 on page 48 provides more information about configuring the domain user and assigning access rights.

Procedure

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 work with VNX or Unity, 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.

Procedure

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 VNX Data Mover or Unity 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 VNX Data Mover or Unity 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.

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:

Procedure

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 Table 5 on page 40.

Table 5 Installation procedure for Trend Micro

Step	Action	Procedure
1.	Create a domain user with the EMC virus-checking right.	Configuring the Domain User Account on page 47
2.	Configure virus-checking parameters on the VNX Data Movers or Unity NAS servers.	Configuring viruschecker.conf on page 55

Table 5 Installation procedure for Trend Micro (continued)

Step	Action	Procedure
3.	Install CAVA (as part of CEE) on the Windows AV machines.	Installing the Common Event Enabler on page 43
4.	Install the Trend AV engine.	Install Trend Micro ServerProtect on page 41
5.	Start the virus-checking client on the VNX Data Movers or Unity NAS servers.	Managing the VC Client on page 69
6.	Verify the CAVA installation.	Verify the installation on page 72

Install Trend Micro ServerProtect

Before you begin

Trend Micro ServerProtect must be installed after installing CAVA. Installing the Common Event Enabler on page 43 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).
```

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.

Procedure

1. Start ServerProtect. The **Management Console** window appears. Figure 1 on page 42 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

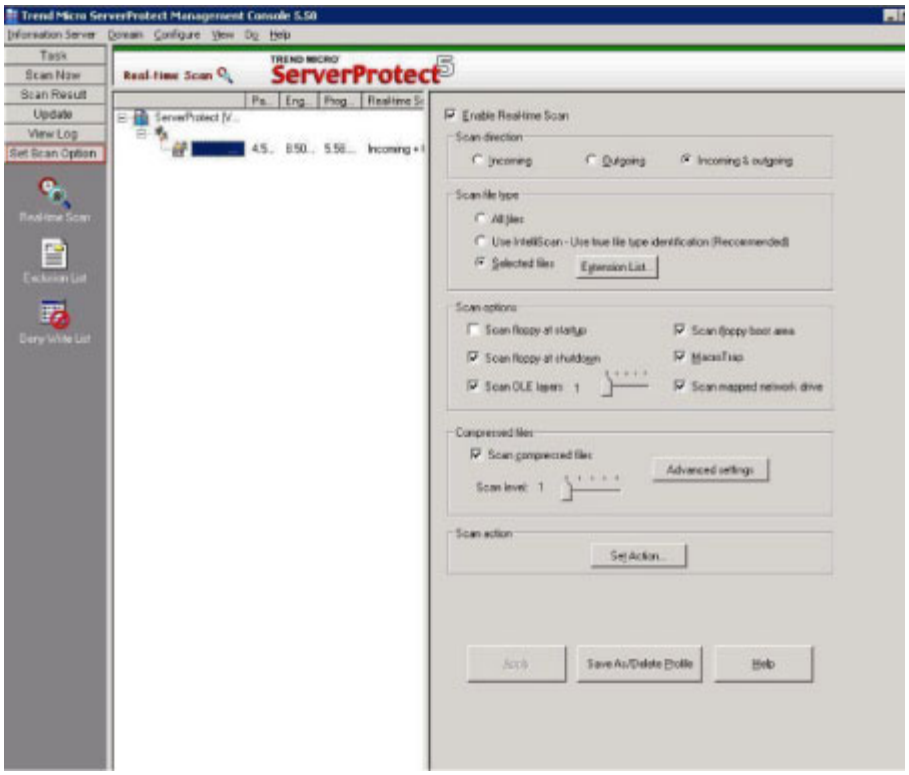
     Ensure that you have selected **Scan mapped network drive** for CAVA to function with Server Protect 5.58.
   - Under **Compressed files**, select **Scan compressed files**.

   Leave all other settings as they are.

   When you have completed the steps, the **Management Console** window should look like Figure 1 on page 42.

3. Click **Apply** to save the changes. Go to Managing the VC Client on page 69.

Figure 1 Trend Micro ServerProtect Real-time Scan options window



CHAPTER 4

Installing the Common Event Enabler

Topics to install the CEE framework include:

Install CEE

Before you begin

- Download the CEE framework software from Online Support:
  1. Open a browser window, and navigate to https://Support.EMC.com.
  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.
- For VNX systems, synchronize date/time stamps on file systems and domain servers by running the following command:
  `server_date server_# -timesvc start ntp <domain controller ip>`
- Table 6 on page 44 provides information that is needed before installing the CEE framework software. Fill in the information pertinent to your company.

Table 6 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:

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 antivirus 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. Skip 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 antivirus software, select **Work with Symantec SAV for NAS/Protection Engine** and the option for the Symantec antivirus software version you are using. Otherwise, click **Next**.
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.

Complete the CEE installation for Windows Server

Procedure

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 on page 105 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 on page 77 provides instructions on using the EMC CAVA services.

Uninstall CEE

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.

CHAPTER 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 VNX Data Mover or Unity NAS Server to distinguish CAVA requests from all other requests.

Note

For CAVA information on VNXe systems, refer to *Using a VNXe System with CIFS Shared Folders* on Online Support.

Topics included are:

Domain user account overview

The antivirus agent installation requires a Windows user account that is recognized by the VNX Data Movers or Unity NAS Servers as having the EMC virus-checking privilege. This user account enables the Data Mover or 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 Data Mover or NAS Server, and run the EMC CAVA service in this user context.

Table 7 on page 48 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. *Configuring and Managing CIFS on VNX* provides more information on local users for VNX systems. *Configuring Hosts to Access SMB File Systems* provides more information on configuring the domain user account on a Unity system.

Table 7 Overview of configuring the AV user

Task	Action	Procedure
1.	Determine which VNX Data Mover or Unity NAS Server interface to use when creating the local group.	Determine the interface name on the Data Mover on page 48
2.	Create a domain user account (AV user).	Create a domain user account on page 50
3.	Create a local group on each VNX Data Mover or Unity NAS Server in the domain and add the AV user to the group.	Create a local group on each Data Mover or NAS server on page 51
4.	Assign the EMC virus-checking right to the local group.	Assign the EMC virus-checking right to the group on page 52
5.	Assign local administrative rights to the local group on each AV machine.	Assign local administrative rights to the AV user on page 53

Optional method

For a Windows Server, you can accomplish Tasks 2 through 5 by using the EMC Unity/VNX/VNXe NAS Management snap-in. *Installing Management Applications on VNX for File* provides installation instructions.

Determine the interface name on the Data Mover

This procedure is valid for VNX systems only.

You must identify the CIFS interface for the Data Mover before you create a local group on a Data Mover. Frequently, a Data Mover is configured with more than one CIFS interface. If this is the case, choose one CIFS interface for each Data Mover and use the same CIFS interface throughout the CAVA configuration.

To obtain the interface name, run the following `server_cifs` command from the Control Station.

If you do not want to use the default CIFS interface for virus checking, you must specify another CIFS interface by setting the `CIFSserver=` parameter in the `viruschecker.conf` file. (Optional) Define VC scanning criteria on page 57 provides more information.

Procedure

1. Display all CIFS interfaces configured on a Data Mover by using this command syntax:

   `$ server_cifs <movername>`
   where:

   <movername> = name of the Data Mover

   Example:

   To display the CIFS interfaces configured on server_3, type:

   `$ server_cifs server_3`
   Output:

```
server_3 :
256 Cifs threads started
Security mode = NT
Max protocol = SMB2
I18N mode = UNICODE
Home Directory Shares DISABLED
Usermapper auto broadcast enabled

Usermapper[0] = [128.221.252.2] state:active (auto discovered)
Usermapper[1] = [128.221.253.2] state:active (auto discovered)

Enabled interfaces: (All interfaces are enabled)

Disabled interfaces: (No interface disabled)

Unused Interface(s):
if=10-1-3-1 l=10.1.3.1 b=10.1.3.255 mac=0:60:48:1d:7e:e4
if=10-1-3-2 l=10.1.3.2 b=10.1.3.255 mac=0:60:48:1d:7e:e4
if=10-1-3-3 l=10.1.3.3 b=10.1.3.255 mac=0:60:48:1d:7e:e4
if=10-1-3-4 l=10.1.3.4 b=10.1.3.255 mac=0:60:48:1d:7e:e4
if=10-1-3-5 l=10.1.3.5 b=10.1.3.255 mac=0:60:48:1d:7e:e5
if=10-1-3-6 l=10.1.3.6 b=10.1.3.255 mac=0:60:48:1d:7e:e5
if=10-1-3-7 l=10.1.3.7 b=10.1.3.255 mac=0:60:48:1d:7e:e5
if=10-1-3-8 l=10.1.3.8 b=10.1.3.255 mac=0:60:48:1d:7e:e5
if=10-1-3-9 l=10.1.3.9 b=10.1.3.255 mac=0:60:48:1d:7e:e5
if=ip6-10-1-3-200 l=2620:0:170:1d48::af5:48db mac=0:60:48:1d:7e:ea
if=ip6-10-1-3-201 l=2620:0:170:1d48::af5:48da mac=0:60:48:1d:7e:ea
if=ip6-10-1-3-202 l=2620:0:170:1d48::af5:48d9 mac=0:60:48:1d:7e:ea
if=ip6-10-1-3-203 l=2620:0:170:1d48::af5:48d8 mac=0:60:48:1d:7e:ea
if=ip6-10-1-3-204 l=2620:0:170:1d48::af5:48d7 mac=0:60:48:1d:7e:ea
if=ip6-10-1-3-205 l=2620:0:170:1d48::af5:48d0 mac=0:60:48:1d:7e:eb
if=ip6-10-1-3-206 l=2620:0:170:1d48::af5:48df mac=0:60:48:1d:7e:eb
if=ip6-10-1-3-207 l=2620:0:170:1d48::af5:48de mac=0:60:48:1d:7e:eb
if=ip6-10-1-3-208 l=2620:0:170:1d48::af5:48dd mac=0:60:48:1d:7e:eb
if=ip6-10-1-3-209 l=2620:0:170:1d48::af5:48dc mac=0:60:48:1d:7e:eb

DOMAIN CIFS FQDN=cifs.lab.com SITE=Default-First-Site-Name RC=3
SID=S-1-5-15-912f739d-ff96d019-69c4989d-ffffffff
>DC=ENG554104(10.1.3.100) ref=5 time=1 ms (Closest Site)

CIFS Server ALPHA43[cifs] RC=3
Full computer name=alpha43.cifs.lab.com realm=CIFS.LAB.COM
Comment='SNAS:T7.1.56.75120059'
if=10-1-3-200 l=10.1.3.200 b=10.1.3.255 mac=0:60:48:1d:7e:e4
   FQDN=alpha43.cifs.lab.com (Updated to DNS)
```

```
Password change interval: 0 minutes
Last password change: Fri May 3 17:11:37 2013 GMT
Password versions: 2
```

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 on page 50
- Create from User Manager for Domains on page 50

Create with Active Directory on a Windows Server

Procedure

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 Data Mover or NAS server on page 51.

Create from User Manager for Domains

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

Procedure

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 Data Mover or NAS server on page 51.

Create a local group on each Data Mover or NAS server

To assign the EMC virus-checking right to the domain user you just created, you must first create a local group on the VNX Data Mover or Unity 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:

Procedure

1. For systems with Active Directory:
   - VNX systems: in **Active Directory Users and Computers**, double-click **EMC Celerra** and click **Computers**.
   - Unity systems: in **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 on page 50.

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 on page 52.

Assign the EMC virus-checking right to the group

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 Data Mover/NAS Server and is added to the local group that you created in Create a local group on each Data Mover or NAS server on page 51.

Note

You cannot use Microsoft's Windows Local Policy Setting tools to manage user rights assignments on a Data Mover/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:

Procedure

1. Click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **EMC Unity VNX VNXe NAS Management**.

   Note

   Installing Management Applications on VNX for File provides information on installing MMC snap-ins and ADUC extensions.

2. Perform one of the following:
   - If a Data Mover/NAS Server is already selected (name appears after Data Mover/NAS Server Management), go to step 4.
   - If a Data Mover/NAS Server is not selected:
     - Right-click **Data Mover/NAS Server Management** and select **Connect to Data Mover/NAS Server**.
     - Select a Data Mover/NAS Server by using one of the following methods:
       - In the **Look in:** list box, select the domain in which the Data Mover/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 Data Mover/NAS Server.

3. Double-click **Data Mover/NAS Server Management**, and double-click **Data Mover/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 CIFS server from the **Look in:** list box.
   b. Select the antivirus group that you created in Create a local group on each Data Mover or NAS server on page 51.
   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 Data Mover/NAS Server local group. Go to Assign local administrative rights to the AV user on page 53 to continue.

Assign local administrative rights to the AV user

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:

Procedure

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 on page 50.

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, go to Configuring viruschecker.conf on page 55.

CHAPTER 6

Configuring viruschecker.conf

The `viruschecker.conf` file defines virus-checking parameters for each VNX Data Mover or Unity NAS server in the domain. For CAVA to work properly, some parameters, such as the `addr` parameter, must be configured. Other parameters are optional and you can configure them if you want to control the scope and style of the virus scanning.

This guide describes only the command-line procedures. In a Windows Server environment, you can also use the EMC Unity/VNX/VNXe NAS Management snap-in to modify the antivirus agent parameters on the Data Mover or NAS Server. EMC Unity/VNX/VNXe NAS Management is installed as an MMC snap-in to Unisphere. *Installing Management Applications on VNX for File* provides instructions on installing the snap-in.

Topics included are:

Create and edit viruschecker.conf

For Unity systems, you can either retrieve the configuration file in Unisphere and edit it, or you can upload a configuration file that you create offline. The antivirus configuration is found in Unisphere at **Storage** > **File** > **NAS Servers** > **Properties** > **Security** > **Antivirus**.

For VNX systems, ensure that the `viruschecker.conf` file resides in the `/.etc` directory on the Data Mover before editing. You can either create a new `viruschecker.conf` file or retrieve the existing `viruschecker.conf` file and edit the contents:

- If the `viruschecker.conf` file exists in the `/.etc` directory, type the following command to retrieve this file for editing:
  `$ server_file <movername> -get viruschecker.conf viruschecker.conf`
- If the `viruschecker.conf` file does not exist in the `/.etc` directory, copy the template `viruschecker.conf` file from the `/nas/sys` directory on the Control Station to another directory, such as `/nas/site` for editing with a text editor.

Define AV machine IP addresses in viruschecker.conf

Procedure

1. Open the viruschecker.conf file using an editor.
2. Locate the addr entry.
3. Add the IP addresses of all Windows Servers running the CAVA software. Use colons to separate multiple Windows Server IP addresses.

   Example:

   The first entry below identifies a single Windows Server, the second entry identifies multiple Windows Servers, while the third entry identifies a fully qualified domain name (FQDN):

   ```
   addr=192.16.20.29

   addr=192.16.20.15:[2510:0:175:111:0:4:aab:ad2]:
   [2510:0:175:111:0:4:aab:a6f]:192.16.20.16:192.16.20.17

   addr=wichita.nasdocs.emc.com
   ```

   Note

   IPv6 addresses should be enclosed in square brackets to separate them from the colon delimiter that is used between multiple addresses.

   The addresses entered represent the Windows Servers that the VNX Data Mover or Unity NAS Server will send the UNC path of the files to scan. For multiple server installations, the UNCs are sent in a round-robin fashion to all Windows Servers configured with the CAVA software and the AV engine.
4. Save and close the viruschecker.conf file.

Send viruschecker.conf to the Data Mover

This procedure is used for VNX systems. For Unity systems, upload the CAVA configuration by using either the Unity CLI or Unisphere software. Refer to the *Unity Unisphere Command Line Interface User Guide* for CLI commands. Instructions for retrieving the configuration file on Unity systems are described in Virus-checking continuation on page 19.

You must put a copy of the `viruschecker.conf` file on each Data Mover in the domain.

Note

If you customize a Data Mover's `viruschecker.conf` file by configuring the `CIFSserver=` parameter, ensure that you put the customized `viruschecker.conf` file on the correct Data Mover.

Procedure

1. Copy the `viruschecker.conf` file from the Control Station to the `/.etc` directory on the Data Mover by using this command syntax:

   ```
   $ server_file <movername> -put viruschecker.conf
   viruschecker.conf
   ```

   where:

   <movername> = name of the Data Mover

   Output:

   ```
   server_2:done
   ```

   Note

   - Repeat this command for each Data Mover within the domain.
   - If the `viruschecker.conf` file is missing from the `/.etc` directory, the VC client will not start.

   The following documents provide more information:

   - *EMC VNX Command Line Interface Reference for File* provides detailed information on the `server_file` command.
   - *Managing a Multiprotocol Environment on VNX* provides details on mounting a file system.

(Optional) Define VC scanning criteria

You can configure the `masks=` parameter in the `viruschecker.conf` file to scan files with a specific extension, for example, the extension .doc or .docx for Microsoft Word documents. If you have multiple SMB/CIFS interfaces on a VNX Data Mover or Unity NAS server, you can set the `CIFSserver=` parameter to specify which interface the VNX Data Mover or Unity NAS server uses to communicate with the AV machines.

viruschecker.conf parameters on page 58 provides a complete list of `viruschecker.conf` parameters, including `mask`:

Procedure

1. Open the `viruschecker.conf` file using an editor.

   Instructions for retrieving the configuration file on Unity systems are described in Virus-checking continuation on page 19.

2. Locate the `masks=` entry.
3. Type the entry for the list of files to be scanned.

   Examples:

   In the following example, all files are scanned:

   `masks=*.*`
   In the following example, only .exe, .com, .doc, .docx, and .ppt files are scanned:

   `masks=*.exe:*.com:*.doc:*.docx:*.ppt`

4. Type the NetBIOS name of the VNX Data Mover or Unity NAS server:

   `CIFSserver=<netbios_name or IP address>`
   Determine the interface name on the Data Mover on page 48 provides more information.

   Example:

   `CIFSserver=dm53-ana0`

   Note

   If this parameter is not set, the default NetBIOS name on that VNX Data Mover or Unity NAS server is used. If you set this parameter, ensure that you use the same interface that you used in Create a domain user account on page 50.

5. Save and close the `viruschecker.conf` file.

viruschecker.conf parameters

Table 8 on page 59 provides additional parameters that can be configured within the `viruschecker.conf` file, or for use with the EMC Unity/VNX/VNXe NAS Management snap-in.

Note

For Unity systems, you can either create a configuration file in Unisphere, or you can upload a configuration file that you create offline. In Unisphere, the antivirus configuration is found at **Storage** > **File** > **Properties** > **NAS Servers** > **Security** > **Antivirus**.

The `masks=` parameter can greatly affect virus-checking performance. It is recommended that you do not use `masks=*.*` because this setting scans all files. Many files cannot harbor viruses, therefore, `masks=*.*` is not an efficient setting. Most AV engines do not scan all files. The `masks=` and `excl=` parameters in the `viruschecker.conf` file should be equal to or a superset of the `masks=` and `excl=` settings used by the AV engine.

Table 8 Parameters in the viruschecker.conf file

Parameter	Description	Example
`httpport=`	HTTP port number on the CEE machine that the storage system will use. **Note** If you set the `httpport=` parameter, you must also specify the same port number in the HttpPort entry of the Windows Registry at: `HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\Configuration`	`httpport=12228`

`masks=`	Configures file extensions that will be scanned.	`masks=*.exe`
		In the following example, only .exe, .com, .doc, .docx, and .ppt files are scanned:
		`masks=*.exe:*.com:*.doc:*.docx:*.ppt`

`excl=`	Defines files or file extensions to exclude during scanning.	`excl=pagefile.sys:*.tmp`
`addr=`	Sets the IP addresses for the AV machines, or an FQDN. **Note** The use of link-local network addresses for defining AV machines is not supported.	Single IP address: `addr=192.16.20.29` Multiple IP addresses: `addr=192.16.20.15:192.16.20.16:[2510:0:175:111:0:4:aab:ad2]:[2510:0:175:111:0:4:aab:a6f]:192.16.20.17` **Note** IPv6 addresses should be enclosed in square brackets to separate them from the colon delimiter that is used between multiple addresses. FQDN: `addr=wichita.nasdocs.emc.com` **Note** If an AV machine is going to be temporarily or permanently removed, delete its IP address from this file before shutting down the EMC CAVA service.
`CIFSserver=<CIFS_server_name>` (optional)	Identifies the interface on the VNX Data Mover or Unity NAS server used by the CAVA Client `<CIFS_server_name>` (NetBIOS name, compname, or the IP address) of the SMB/CIFS server on the Data Mover or NAS server. If the parameter is not given, the Data Mover	`CIFSserver=CIFS_Host2`

Table 8 Parameters in the viruschecker.conf file (continued)

Parameter	Description	Example
	or NAS server uses the first SMB/CIFS server that it finds. **Note** The use of link-local network addresses for defining AV machines is not supported.	
`maxsize=<n>` (optional)	Sets the maximum file size for files that will be checked. Files that exceed this size are not checked. Type a hexadecimal number with a prefix of 0x. The maxsize must be less than or equal to 0xFFFFFFFF. If the parameter is not given or is equal to 0, it means no file size limitation is set. The file size is in bytes with a 4 GB maximum.	`maxsize=0xFFFFFFFF`
`highWaterMark=<n>` (optional)	Edits the `highWaterMark` parameter. When the number of requests in progress becomes greater than the High Water Mark value, a log event is sent to the storage system. The default value is 200. The maximum is 0xFFFFFFFF.	`highWaterMark=200`
`lowWaterMark=<n>` (optional)	Edits the `lowWaterMark` parameter. When the number of requests in progress becomes lower than Low Water Mark value, a log event is sent to VNX or Unity. The default value is 50.	`lowWaterMark=50`
`waitTimeout=<n>` (optional)	Sets the maximum time allowed in milliseconds for a client to be blocked while the client tries to access a file which is being scanned. The default value is 0 milliseconds, indicating that client access is blocked until the file has been scanned. Setting this parameter does not affect the actual scanning of the file.	`waitTimeout=0 milliseconds`
`RPCRetryTimeout=<n>` (optional)	Sets the timeout of the RPC retry. The timeout is set in milliseconds. The default value is 5000 milliseconds. The maximum is 0xFFFFFFFF.	`RPCRetryTimeout=4000 milliseconds`

Table 8 Parameters in the viruschecker.conf file (continued)

Parameter	Description	Example
`RPCRequestTimeout=<n>` (optional)	Sets the timeout of the RPC request (in milliseconds). Works with `RPCRetryTimeout`. When an RPC is sent to the AV machine, if the server answers after the `RPCRetryTimeout`, the Data Mover or NAS server retries until `RPCRequestTimeout` is reached. If `RPCRequestTimeout` is reached, the Data Mover or NAS server goes to the next available AV machine. The default value is 25000 milliseconds. **Note** This value should be greater than the Symantec Protection Engine Container File Processing Limits value. Setting container handling policies on page 40 contains details.	`RPCRequestTimeout=20000 milliseconds`

`msrpcuser=` (optional)	Specifies the name assigned to either a simple user account or user account that is part of a domain that the EMC CAVA service is running under on the CEE machine.	User account:
		`msrpcuser=user1`
		Domain\user account:
		`msrpcuser=CEE1\user1`

`surveyTime=<n>` (optional)	Specifies the time interval used to scan all AV machines to see if they are online or offline. This parameter works with the `shutdown` parameter shown next. If no AV machine answers, the shutdown process begins using the configured shutdown parameter. This is the only parameter that triggers shutdown. The default value is 10 seconds. min=1, max=3600.	`surveyTime=60 seconds`
`shutdown=`	Specifies the shutdown action to take when no server is available. Works with the `surveyTime` parameter. Options include the following parameters: • `shutdown=cifs` — Stops SMB/CIFS if no AV machine is available. (No Windows clients can access any VNX or Unity share.) If strict data security is important in the environment, you should enable	`shutdown=cifs`

Table 8 Parameters in the viruschecker.conf file (continued)

Parameter	Description	Example
	this option to prevent access to the files if all AV machines are unavailable. If this option is not enabled, and all AV machines are unavailable, clients can modify files without any virus checking. **Note** `shutdown=CIFS` should be disabled if less than two AV machines are configured. • `shutdown=no` — Continues retrying list of AV machines if no AV machine is available. Two watermarks exist (low and high). When each is reached, an Event log is sent. Use the Event log to take corrective action on the Data Mover or NAS server to ensure that virus checking is functional. • `shutdown=viruschecking` — Stops the virus checking if no AV machine is available. (Windows clients can access VNX or Unity shares without virus checking.) The default is shutdown=no.	`shutdown=no` `shutdown=viruschecking`

CHAPTER 7

Configuring the Event Publishing Agent

The task to configure CEPA is:

Create the cepp.conf file

Note

- The following procedure is used for VNX systems only. For Unity systems, the configuration details are created when setting up Events Publishing for each NAS server in Unisphere (**Storage** > **File** > **NAS Servers** > **Properties** > **Protection & Events** > **Events Publishing**).
- For VNX systems, the `cepp.conf` file must be defined with the correct syntax to ensure that the EMC CEPA service starts on the Data Mover.

Procedure

1. Log in to the system with your administrative username and password:

   ```
   login:    <username>
   password: <password>
   ```

   where:

   <username> = username defined for the administrative account (default is nasadmin)

   <password> = password defined for the administrative account (default is nasadmin)

2. Use a text editor to create a new, blank file in the home directory.
3. Add the CEPA information that is necessary for your system. This information can be on one line, or on separate lines by using a space and a "\" at the end of each line except for the last line and the lines that contain global options (`httpport`, `cifsserver`, `surveytime`, `ft`, and `msrpcuser`). The cepp.conf file on page 22 contains sample `cepp.conf` files:

   ```
   httpport=<httpport>
   cifsserver=<cifsserver>
   surveytime=<surveytime>
   ft level=[0|1|2|3] {location=<location>} {size=<size>}
   msrpcuser=<msrpcuser>
   pool name=<poolname> \
   servers=<IP_addr1>|<IP_addr2>|... \
   preevents=<event1>|<event2>|... \
   postevents=<event3>|<event4>|... \
   posterrevents=<event5>|<event6>|... \
   option=ignore or denied \
   reqtimeout=<reqtimeout> \
   retrytimeout=<retrytimeout>
   ```

   where:

   <httpport> = HTTP port number on the CEE machine that VNX will use. If you set this `httpport=` parameter, you must also specify the same port number in the HttpPort entry of the Windows Registry at: `HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\Configuration`

   <cifsserver> = name of SMB/CIFS server used by the event publishing agent to access the files in the system. If you do not include this option, the Data Mover

uses the first SMB/CIFS server that it finds. If you include this option, the server specified must be a physical Data Mover, not a VDM, in order for the EMC CEPA service to start on the Data Mover.

Note

The use of link-local network addresses for defining CEPA servers is not supported.

<surveytime> = time to scan each CEPA server. The default is 10 seconds and the range is 1 through 3600 seconds.

The global `ft` option has three parts:

- *level* = fault tolerance level assigned. This option is required. Valid values are 0 through 3, where:
  - 0 = continue and tolerate lost events (default)
  - 1 = continue and use a persistence file as a circular event buffer for lost events
  - 2 = continue and use a persistence file as a circular event buffer for lost events until the buffer is filled and then stop CIFS/NFS
  - 3 = upon heartbeat loss of connectivity, stop CIFS/NFS
- *location* = directory where the persistence buffer file resides relative to the root of a file system. If a location is not specified, the default location is the root of the file system.

  Note

  The file system that contains the persistence buffer file must have an amount of free space available equal to the maximum size of the persistence buffer file. For example, if the persistence buffer file size is 100 MB, the file system must contain at least 100 MB of free space for the temporary file operations.

- *size* = maximum size in MB of the persistence buffer file. The default is 1 MB and the range is 1 MB to 100 MB.

<msrpcuser> = name assigned to the user account that the EMC CAVA service is running under on the CEE machine. For example, if the EMC CAVA service is running under a user called **user1**, the `cepp.conf` file entry would be **msrpcuser=user1**. If user1 is a member of a domain, the entry would be **msrpcuser=domain\user1**.

<poolname> = name assigned to the set of Windows Servers where the CEE software is installed. The specified Data Mover will use the set of servers to perform round-robin load sharing of events. One pool name must be specified. For <postevents> only, you can specify up to three pool names, each on a separate line with an IP address. Refer to The cepp.conf file on page 22 for an example.

<IP_addrx> = IP addresses of the Windows Servers where the CEE software is installed, or an FQDN.

Note

If you use an FQDN and the Data Mover cannot retrieve the IP address of it, add the FQDN to the /.etc/hosts list in the Data Mover.

At least one Windows Server must be specified. Use the vertical bar (|) or a colon (:) when listing multiple addresses.

NOTICE

IPv6 addresses should be enclosed in square brackets to separate them from the colon delimiter that is used between multiple addresses.

<eventx> = events to receive notification of. You must define at least one error option line (pre, post, or posterr) from the following options: * (all events), blank (no events), `OpenFileNoAccess`, `OpenFileRead`, `OpenFileReadOffline`, `OpenFileWrite`, `OpenFileWriteOffline`, `OpenDir`, `FileRead`, `FileWrite`, `CreateFile`, `CreateDir`, `DeleteFile`, `DeleteDir`, `CloseModified`, `CloseUnmodified`, `CloseDir`, `RenameFile`, `RenameDir`, `SetAclFile`, `SetAclDir`, `SetSecFile`, `SetSecDir`. Use the vertical bar (|) when listing multiple events. The following table provides descriptions for these event options.

ignore = if CEPA server is not available, ignore, and return no error to the caller.

denied = if CEPA server is not available, return access denied to the caller. The caller will lose read/write access to the CIFS share.

<reqtimeout> = timeout in millisecond (ms) to send a request that allows access to the CEPA server. Wait to receive the response from the CEPA server. The default is 1,000 ms and the range is 500 ms through 5,000 ms.

<retrytimeout> = timeout in ms to retry the access request sent to the CEPA server. This value must be less than or equal to the `reqtimeout` value. The default is 250 ms and the range is 50 ms through 5,000 ms.

Table 9 Event descriptions

Value	Definition	Protocol
`OpenFileNoAccess`	Sends a notification when a file is opened for a change other than read or write access (for example, read or write attributes on the file).	• SMB/CIFS • NFS (v4)
`OpenFileRead`	Sends a notification when a file is opened for read access.	• SMB/CIFS • NFS (v4)
`OpenFileReadOffline`	Sends a notification when an offline file is opened for read access.	• SMB/CIFS • NFS (v4)
`OpenFileWrite`	Sends a notification when a file is opened for write access.	• SMB/CIFS • NFS (v4)
`OpenFileWriteOffline`	Sends a notification when an offline file is opened for write access.	• SMB/CIFS • NFS (v4)
`OpenDir`	Sends a notification when a directory is opened.	SMB/CIFS
`FileRead`	Sends a notification when a file read is received over NFS.	NFS (v3/v4)
`FileWrite`	Sends a notification when a file write is received over NFS.	NFS (v3/v4)
`CreateFile`	Sends a notification when a file is created.	• SMB/CIFS

Table 9 Event descriptions (continued)

Value	Definition	Protocol
		• NFS (v3/v4)
`CreateDir`	Sends a notification when a directory is created.	• SMB/CIFS • NFS (v3/v4)
`DeleteFile`	Sends a notification when a file is deleted.	• SMB/CIFS • NFS (v3/v4)
`DeleteDir`	Sends a notification when a directory is deleted.	• SMB/CIFS • NFS (v3/v4)
`CloseModified`	Sends a notification when a file is changed before closing.	• SMB/CIFS • NFS (v4)
`CloseUnmodified`	Sends a notification when a file is not changed before closing.	• SMB/CIFS • NFS (v4)
`CloseDir`	Sends a notification when a directory is closed.	SMB/CIFS
`RenameFile`	Sends a notification when a file is renamed.	• SMB/CIFS • NFS (v3/v4)
`RenameDir`	Sends a notification when a directory is renamed.	• SMB/CIFS • NFS (v3/v4)
`SetAclFile`	Sends a notification when the security descriptor (ACL) on a file is changed.	SMB/CIFS
`SetAclDir`	Sends a notification when the security descriptor (ACL) on a directory is changed.	SMB/CIFS
`SetSecFile`	Sends a notification when a file security change is received over NFS.	NFS (v3/v4)
`SetSecDir`	Sends a notification when a directory security change is received over NFS.	NFS (v3/v4)

4. Save the file with the name **cepp.conf**, and then close the text editor.
5. Move the `cepp.conf` file to the Data Mover's root file system:

   `$ server_file <movername> -put cepp.conf cepp.conf`
   where:

   <movername> = name of the Data Mover

Note

Each Data Mover that runs CEPA must have a `cepp.conf` file, but each configuration file can specify different events.

---

6. Before starting CEPA for the first time, the administrator must issue the following command from the Control Station and follow the prompts for entering information:

   ```
   /nas/sbin/server_user server_2 -add -md5 -passwd
   <msrpcuser>
   ```

   where:

   <msrpcuser> = name assigned to either a simple user account or user account that is part of a domain that the EMC CAVA service is running under on the CEE machine, for example, user1 or CEE1\user1.

CHAPTER 8

Managing the VC Client

Before starting the VC client, you should have appropriately installed and configured the antivirus agent. After the virus checking service has been started, you should verify the installation.

Topics included are:

Start the VC client

Before you begin

- For VNX systems, if the user under which EMC CEPA service is running is in a different domain from the CIFS server, the following command needs to be run from the Control Station before starting the virus-checking service:

  ```
  /nas/sbin/server_user server_2 -add -md5 -passwd
  <user>.<domain>
  ```

  The administrator then must follow the prompts for entering information, where:

  <user> is the name assigned to a simple user account that the EMC CAVA service is running under on the CEE machine.

  <domain> is the name assigned to an msrpcuser account that is part of a domain that the EMC CAVA service is running under on the CEE machine.

  For example, if *<user>* equals **user1**, then run the following:

  ```
  /nas/sbin/server_user server_2 -add -md5 -passwd user1
  ```

  If *<user>.<domain>* equals **user1.domain1**, then run the following:

  ```
  /nas/sbin/server_user server_2 -add -md5 -passwd
  user1.domain1
  ```

  If the cepp.conf or viruschecker.conf files are updated manually:

  - the format for the domain user in these files should be:
    `msrpcuser=domain\user1`
  - the format for a local user in these files should be:
    `msrpcuser=user1`
- Ensure that the CIFS or NFS services are configured and started. *Managing a Multiprotocol Environment on VNX* provides details.
- Ensure that the CAVA is installed and running on all AV machines. Installing the Common Event Enabler on page 43 provides more information.

Procedure

1. To start the VC client on the Data Mover, use this command syntax:

   ```
   $ server_setup <movername> -Protocol viruschk -option
   start
   ```

   where:

   <movername> = name of the Data Mover

   Example:

   To start the VC client on server 2, type:

   ```
   $ server_setup server_2 -Protocol viruschk -option start
   ```

   Output:

   ```
   server_2 : done
   ```

Note

If CAVA is not running on a Windows Server in the domain, you will receive the following error message:

```
RPC Error from checker
xxx.xxx.xxx.xxx
```

Celerra Network Server Error Messages Guide provides more information.

After you finish

For VNX systems, you must start the VC client on the Data Mover by using the server_setup command or by using the EMC Unity/VNX/VNXe AntiVirus snap-in, which is part of the EMC Unity/VNX/VNXe NAS Management snap-in. The VC client communicates with CAVA on the AV machines. For Unity systems, you must enable the antivirus service in Unisphere (**Storage** > **File** > **NAS Server** > **Security** > **Antivirus**).

Stop the VC client

Procedure

1. To stop the VC client, use this command syntax:

   `$ server_setup <movername> -P viruschk -o stop`
   where:

   <movername> = name of the Data Mover

   Example:

   To stop the VC client on server_2, type:

   `$ server_setup server_2 -P viruschk -o stop`
   Output:

   `server_2 : done`

Update the viruschecker.conf file

On a VNX system, when making subsequent changes to the `viruschecker.conf` file, use the `server_viruschk` command with the `-update` parameter to load the file into memory. This updates the `viruschecker.conf` file without stopping the virus-checking services.

For Unity systems, instructions for retrieving the configuration file to manually update configuration information on a NAS server are described in Virus-checking continuation on page 19 and in the Unity Unisphere online help.

Note

The EMC Unity/VNX/VNXe AntiVirus snap-in, which is part of the EMC Unity/VNX/VNXe NAS Management snap-in, provides an alternative method to update the `viruschecker.conf` file. (Optional) Install EMC Unity/VNX/VNXe NAS Management snap-in on page 76 provides instructions on using the snap-in.

For VNX systems, use this procedure while the VC client is running:

Procedure

1. From the Control Station, use this command syntax to copy the `viruschecker.conf` file from the Data Mover:

   ```
   $ server_file <movername> -get viruschecker.conf
   viruschecker.conf
   ```

2. Edit the copied `viruschecker.conf` file with a text editor.
3. Use this command syntax to copy the modified `viruschecker.conf` file to the corresponding Data Mover:

   ```
   $ server_file <movername> -put viruschecker.conf
   viruschecker.conf
   ```

   where:

   <movername> = name of the Data Mover

4. Update the `viruschecker.conf` file on the Data Mover by using this command syntax:

   ```
   $ server_viruschk <movername> -update
   ```

   where:

   <movername> = name of the Data Mover

   Example:

   To update the file on server 2, type:

   ```
   $ server_viruschk server_2 -update
   ```

   Output:

   ```
   server_2 : done
   ```

Verify the installation

Confirm that the virus checking is operating properly by using one of the following methods:

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

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

  You can use the following step to verify if the infected file is deleted.

  1. To ensure that the infected file was found and deleted, use this command syntax:

     ```
     $ server_viruschk <mover_name> -audit
     ```

     where:

     <mover_name> = name of the Data Mover

     Example:

     To verify if the infected file is found and deleted, type:

     ```
     $ server_viruschk server_2 -audit
     ```

     Output:

     ```
     Total Infected Files          : 1
     Deleted Infected Files        : 1
     ```

```
Renamed Infected Files        : 0
Modified Infected Files       : 0
```

These fields display only if the infected files are found. They remain visible until the Data Mover is rebooted or the EMC CAVA service has been restarted.

- Mimic the client access to files on the Data Mover for various levels of access. For example, perform a write from one client followed by multiple reads from other clients, or copy a number of files from one directory to another on the Data Mover.

CHAPTER 9

Managing CAVA

Topics included are:

(Optional) Install EMC Unity/VNX/VNXe NAS Management snap-in

In a Windows Server environment, use the EMC Unity/VNX/VNXe NAS Management snap-in to modify the antivirus agent parameters on the Data Mover or NAS Server. *Installing Management Applications on VNX for File* provides instructions on installing the snap-in.

Open the EMC Unity/VNX/VNXe NAS Management snap-in

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

For assistance in using the EMC Unity/VNX/VNXe NAS Management snap-in, click **Help** in the toolbar.

Note

The SMB/CIFS services must be configured and started on the VNX Data Mover or Unity NAS server before you can change the virus-checking configuration parameters.

Display virus-checking information

For Unity systems, use the `svc_cava` command to modify virus checker information. *Unity Service Commands Technical Notes* provides more information on the `svc_cava` command.

Procedure

1. For VNX systems, to display the virus checker information, use this command syntax:

   ```
   $ server_viruschk {<movername>|ALL}
   ```

   Example:

   To display the virus checker information on server 2, type:

   `$ server_viruschk server_2`

   Output:

   ```
   server_2 :
   10 threads started
   1 Checker IP Address(es):
   172.24.101.217 ONLINE at Tue Jan 25 23:29:04 2005
   (GMT-00:00)
   RPC program version: 3
   CAVA release: 3.3.5, AV Engine: Network Associates
   Last time signature updated: Tue Jan 25 23:28:14
   2005 (GMT-00:00)
   1 File Mask(s):
   *.*
   No File excluded
   Share \\127_SVR2SH1\CHECK$
   RPC request timeout=25000 milliseconds
   RPC retry timeout=5000 milliseconds
   High water mark=200
   Low water mark=50
   Scan all virus checkers every 60 seconds
   ```

```
When all virus checkers are offline:
Continue to work with Virus Checking and CIFS
Scan on read if access Time less than Tue Jan 25
23:28:14 2005 (GMT-00:00)
Panic handler registered for 65 chunks
```

Note

- No arguments–Displays the virus checker configuration.
- `ALL`–Executes the command for all Data Movers.

Audit virus-checking information

Procedure

1. Audit the virus checker information by using this command syntax:

   `$ server_viruschk {<movername>|ALL} -audit`

   Example:

   To audit the virus checker information on server 2, type:

   `$ server_viruschk server_2 -audit`
   Output:

```
server_2 :
Total Requests : 244
Requests in progress:1

NO ANSWER from Virus Checker Servers: 0
ERROR_SETUP:0
FAIL: 0
TIMEOUT: 0
min=1837 uS, max=183991 uS average=30511 uS

0 File(s) in the collector queue
1 File(s) processed by the AV threads
Read file '/.etc/viruschecker.audit' to
display the list of pending requests
```

Note

- No arguments–Displays the virus checker configuration.
- `ALL`–Executes the command for all Data Movers.
- `-audit`–Displays the status of the virus checker, such as how many files have been checked and the progress of those that are being checked.

Start, stop, and restart CAVA

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:

Procedure

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.

Perform a full file system scan

For VNX systems, an administrator can perform a full scan of a file system by using the `server_viruschk -fsscan` command from the Control Station. To use this feature, the antivirus agent must be enabled and running. The administrator can query the state of the scan while it is running, and can stop the scan if necessary. A file system cannot be scanned if it is mounted with the option `noscan`. As the scan proceeds through the file system, it checks each file and triggers a scan request for each file.

Note

If a file system is unmounted during a full file system scan with `-fsscan`, the scan stops, and there can be files that might not have been touched by the scan, which means there can still be infected files present. Upon remount, `-fsscan` must be restarted to scan any remaining files for infection.

Although a single file system can have only one scan running on it at a time, you can scan multiple file systems simultaneously. However, scanning multiple file systems can cause the `lowWaterMark` and `highWaterMark` parameters to be reached, and an event log to be sent. In this case, you need to increase the `lowWaterMark` and `highWaterMark` parameter values. viruschecker.conf parameters on page 58 provides more information about parameters.

For VNX systems, use this command syntax to perform a full file system scan.

Procedure

1. To start a scan on a file system, use this command syntax:

   `$ server_viruschk <movername> -fsscan <fsname> -create`

   where:

   <movername> = name of the Data Mover

   <fsname> = name of the file system

   Example:

   To start a scan on ufs1, type:

   `$ server_viruschk server_2 -fsscan ufs1 -create`

   Output:

   `server_2 : done`

Verify the status of a file system scan

Procedure

1. To verify the status of a scan on a file system, use this command syntax:

   ```
   $ server_viruschk <movername> –fsscan <fsname> -list
   ```
   where:

   <movername> = name of the Data Mover

   <fsname> = name of the file system

   Example:

   To verify the scan of a file system (in this example, ufs1), type:

   $ server_viruschk server_2 -fsscan ufs1 -list

   Output:

   ```
   server_2 :
   FileSystem 24 mounted on /ufs1:
     8 dirs scanned and 22 files submitted to the scan engine
     firstFNN=0x0, lastFNN=0xe0f34b70, queueCount=0, burst=10
   ```

Stop a file system scan

Procedure

1. To stop a scan on a file system, use this command syntax:

   ```
   $ server_viruschk <movername> –fsscan <fsname> -delete
   ```
   where:

   <movername> = name of the Data Mover

   <fsname> = name of the file system

   Example:

   To stop a scan on ufs1, type:

   $ server_viruschk server_2 –fsscan ufs1 -delete

   Output:

   ```
   server_2 : done
   ```

Enable scan-on-first-read

For VNX systems, you can enable the antivirus agent scan-on-first-read functionality by using the `server_viruschk` command. The command sets the reference time on the virus-checker configuration file. The Data Mover uses the access time of a file during an open to see if the file must be scanned. This time is compared with the time reference that is in the virus checker configuration on the Data Mover. If the access time of the file is less than this reference, the file is scanned before it is opened by the CIFS client. The time reference is updated with a field of the response of the virus checker only if the time given in this field is greater than the time reference. The antivirus agent sets the access time when it detects a virus definition file update. The `accesstime=now` option sets the reference time to the current time. The `accesstime=none` option disables the time scan (scan-on-first-read) functionality. The reference time is stored in memory and in the viruschecker.dat file located in the /.etc directory. The time is persistent after a stop or start of the virus-checker service or after restarting the Data Mover.

For VNX systems, use this command to enable the scan-on-first-read functionality.

Procedure

1. To enable scan-on-first-read, use this command syntax:

   ```
   $ server_viruschk <movername> -set
   accesstime=0205231130.00
   ```
   where:

   <movername> = name of the Data Mover

   Example:

   To enable scan-on-first-read on file system server 2, type:

   ```
   $ server_viruschk server_2 -set accesstime=0205231130.00
   ```
   Output:

   ```
   server_2 : done
   ```

Update virus definition files

The antivirus agent can automatically detect a new version of the virus definition file and update the access time. When a CIFS user accesses a file, the file is scanned with the latest virus definitions, even if it has not been modified since the previous scan. Each time the antivirus agent receives an update, an entry in the Event Log is made. Updates are made through an antivirus agent heartbeat. To use this feature you must have scan-on-first-read enabled.

Note

Currently, McAfee version 8.0i supports automatic detection of virus definition updates. The *VNX Operating Environment for File Release Notes* and Dell EMC E-Lab Interoperability Navigator provide the latest information on other antivirus products.

Turn off the AV engine

Use this procedure to turn off the AV engine on an AV machine. If you do not, the virus-checking capability of the AV machine is compromised and the SMB/CIFS files stored on VNX or Unity might be susceptible to virus infection:

Procedure

1. Exclude the AV machines from the list of servers providing virus-checking capability to VNX or Unity. Define AV machine IP addresses in viruschecker.conf on page 56 provides more information.

   Instructions for retrieving the configuration file on Unity systems are described in Virus-checking continuation on page 19.

2. Stop the EMC CAVA service. Start, stop, and restart CAVA on page 77 provides more information.
3. Disable the third-party realtime scanning feature from the AV machine. The third-party application documentation provides more information.

Turn on the AV engine

If you turned off the AV engine on an AV machine, use this procedure to restore the virus checking to its fully operational configuration:

Procedure

1. Enable the third-party realtime scanning feature from the AV machine. The third-party application documentation provides more information.
2. Start the EMC CAVA service. Start, stop, and restart CAVA on page 77 provides more information.
3. Include the AV machines from the list of servers providing virus-checking capability to VNX or Unity. Define AV machine IP addresses in viruschecker.conf on page 56 provides more information.

   Instructions for retrieving the configuration file on Unity systems are described in Virus-checking continuation on page 19.

Manage CAVA thread usage

CAVA uses four types of threads to handle virus checking:

- Normal Data Mover or storage processor (SP) CIFS threads — Serve CIFS requests from any CIFS client.
- Reserved Data Mover or SP CIFS threads — Serve CIFS requests from the external AV machines only.
- Data Mover viruschk threads — (VNX systems only) Issue antivirus check requests to CAVA threads on the external AV machines.
- CAVA threads on each external antivirus (AV) machine — (VNX systems only) Service the requests issued by viruschk threads on the Data Movers.

By default, 20 threads run on each external AV machine. The default number of CIFS threads that run on a Data Mover or SP depends on Data Mover or SP memory. By default, three CIFS threads are reserved for AV activities (these are the reserved Data Mover or SP CIFS threads).

For VNX systems, each Data Mover runs 10 viruschk threads by default.

In general, you should set the number of reserved threads for the VC client equal to the number of AV checking machines. However, this number should not be set higher than half the number of CIFS threads.

- Adjust the maxVCThreads parameter on page 82 provides information on setting the `maxVCThreads` parameter for VNX systems. *Managing a Multiprotocol Environment on VNX* provides more information on setting the number of normal CIFS threads on a Data Mover.
- For Unity systems, use the `svc_nas` command to modify the `maxVCThreads` parameter, and then reboot the SPs. *Unity Service Commands Technical Notes* provides more information on the `svc_nas` command.

For VNX systems, you can set the number of viruschk threads by using the `server_setup` command. *VNX Command Line Interface Reference for File* describes how to set viruschk threads by using `server_setup`. Managing the Registry and AV Drivers on page 87 describes how to change the default number of CAVA threads.

If virus checking is enabled, a file usually must be scanned for viruses before the file can be accessed. Occasionally, if the VC client runs out of threads, file access

requests cannot progress because VC threads are not available for virus scanning. In effect, a deadlock occurs between file access requests and virus-checking requests.

For these situations, the VC client has special threads reserved for breaking deadlocks. The `maxVCThreads` parameter specifies the number of special threads reserved for the VC client. Generally, the default setting for `maxVCThreads` is appropriate for most networks. However, you can modify this value if necessary:

- For VNX systems, modify the `maxVCThreads` parameter in the `/nas/site/slot_param`, or the `/nas/server/slot_<x>/param` files.
- For Unity systems, use the `svc_nas` command to modify the `maxVCThreads` parameter, and then reboot the SPs.

Adjust the maxVCThreads parameter

Note

For Unity systems, use the `svc_nas` command to modify the `maxVCThreads` parameter, and then reboot the SPs. *Unity Service Commands Technical Notes* provides more information on the `svc_nas` command.

For VNX systems only, use the following procedure to adjust the maximum number of threads reserved for breaking deadlocks:

NOTICE

Do not change other lines in the parameter file without a thorough knowledge of the potential effects on the system. Contact Customer Support for more information.

Procedure

1. Log in to the Control Station.
2. Type the following:

   ```
   $ server_param {<movername>|ALL} -facility cifs -modify
   maxVCThreads -value <new_value>
   ```

   where:

   <movername> = name of the Data Mover

   <new value> = the maximum number of threads reserved for virus checking

3. Restart CAVA with the new parameter by typing:

   ```
   $ server_viruschk <movername> -update
   ```

   where:

   <movername> = name of the Data Mover

View the application log file from a Windows Server

Procedure

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

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:

Procedure

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

For VNX systems only, you can customize the type of virus-checking notification CAVA sends and who receives notification by modifying the `viruschk` parameter on the Data Mover. The default value for the `viruschk` parameter is 7. Table 10 on page 83 provides details on the parameter values.

Table 10 viruschk notify parameter values

Value	Comment/Description
0–3, 6, 7 (default) 4, 5 are not allowed	Setting this value determines the type of notification CAVA sends and upon which type of event it is sent: • 0= A log event is sent to the Control Station if a file is deleted or renamed. • 1= A log event is sent to the Control Station if a file is deleted, renamed, or modified. • 2= A Windows message and a log event are generated if a file is deleted or renamed. • 3= A Windows message is sent to the client if a file is deleted or renamed. A log event is generated if a file is deleted, renamed, or modified. • 6= A Windows message is sent to the client when a file is deleted, renamed, or modified. A log event is generated if a file is deleted or renamed. • 7= A Windows message and a log event are generated when a file is deleted, renamed, or modified. This is the default.

Each third-party antivirus vendor varies slightly on which type of remediation works with CAVA. Table 11 on page 84 lists the types of remediation supported by the third-party vendors. Third-party vendor documentation provides more information.

Table 11 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
Microsoft System Center 2012 Endpoint Protection	Remove; Quarantine
Sophos	Delete; Move to
Symantec Endpoint Protection 2012	Delete; Quarantine
Symantec Protection Engine	Delete; Quarantine
Trend Micro	Clean; Delete; Quarantine

Customize notification messages

For VNX systems only, use the following procedure to customize notification messages that are displayed when CAVA detects a virus:

Procedure

1. Log in to the Control Station as `root`.
2. Create and edit the `cifsmsg.txt` file in a text editor.
3. Use this syntax to customize a message:

Note

Use `#` at the beginning of a sentence if you want to add comments to this file.

```
$error.FileDeletedByVC=
<message line 1>
<message line :>
<message line n>
.
$error.FileRenamedByVC=
<message line 1>
<message line :>
<message line n>
.
$warning.FileModifiedByVC=
<message line 1>
<message line :>
<message line n>
.
```

Note

The last line must be a period (.).

4. Save and close the file, then type:

   ```
   $ server_file <server_x> -put cifsmsg.txt cifsmsg.txt
   ```

   where:

   <server_x> = name of the Data Mover

5. To affect the changes you made to the `cifsmsg.txt` file, restart (stop and start) the CIFS service on the Data Mover by using this command syntax:

   ```
   $ server_setup <server_x> -P cifs -o stop
   $ server_setup <server_x> -P cifs -o start
   ```

   where:

   <server_x> = name of the Data Mover

   If you have also changed the parameter, as described in Customize virus-checking notification on page 83, restart the Data Mover (instead of restarting CIFS) to affect all changes at once.

CHAPTER 10

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).

NOTICE

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 included are:

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

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

Procedure

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.

CHAPTER 11

Managing the Event Publishing Agent

Note

Before issuing commands, you must be logged in as a domain user, not as a local user.

Topics included are:

Edit the cepp.conf file

This procedure is for VNX systems only. For Unity systems, refer to the Unisphere online help for instructions on editing Events Publishing configuration information.

Procedure

1. Copy the current configuration file from the Data Mover:

   ```
   $ server_file <movername> -get cepp.conf cepp.conf
   ```
   where:

   <movername> = name of the Data Mover where the configuration file resides

2. Edit the cepp.conf file as necessary.
3. Reload the file to the Data Mover:

   ```
   $ server_file <movername> -put cepp.conf cepp.conf
   ```
   where:

   <movername> = name of the Data Mover where the configuration file resides that needs to be replaced

Assign rights in Windows Server

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

Procedure

1. Click **Start** and select **Settings** > **Control Panel** > **Administrative Tools** > **EMC Unity VNX VNXe NAS Management**.

   Note

   Installing Management Applications on VNX for File provides information on installing the MMC snap-ins and ADUC extensions.

2. Perform one of the following:
   - If a Data Mover/NAS Server is already selected (name appears after Data Mover/NAS Server Management), go to step 4.
   - If a Data Mover/NAS Server is not selected:
     - Right-click **Data Mover/NAS Server Management** and select **Connect to Data Mover/NAS Server**.
     - Select a Data Mover/NAS Server by using one of the following methods:
       - In the **Look in:** list box, select the domain in which the Data Mover/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 Data Mover/NAS Server.

3. Double-click **Data Mover/NAS Server Management**, and double-click **Data Mover/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 Data Mover/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 Data Mover/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 **EMC Unity/VNX/VNXe NAS Management** window.

Start the CEPA facility

1. To start the CEPA facility, use this command syntax:
   `$ server_cepp <movername> -service -start`

   where:

   <movername> = name of the Data Mover

   Example:

   To start the CEPA facility on the Data Mover server_2, type:

   `$ server_cepp server_2 -service -start`
   Output:

   `server_2 : done`

Verify the CEPA status

Procedure

1. To verify the CEPA facility status, use this command syntax:

   `$ server_cepp <movername> -service -status`
   where:

<movername> = name of the Data Mover

Example:

To verify the CEPA facility status on the Data Mover server_2, type:

$ server_cepp server_2 -service -status
Output:

```
server_2 : CEPP Started
```

Stop the CEPA facility

1. To stop the CEPA facility, use this command syntax:

   ```
   $ server_cepp <movername> -service -stop
   ```

   where:

   <movername> = name of the Data Mover

   Example:

   To stop the CEPA facility on the Data Mover server_2, type:

   $ server_cepp server_2 -service -stop
   Output:

   ```
   server_2 : done
   ```

Display the CEPA facility properties

Procedure

1. To display information about the CEPA service, use this command syntax:

   ```
   $ server_cepp <movername> -service -info
   ```
   where:

   <movername> = name of the Data Mover

   Example:

   To display information about the CEPA service on the Data Mover server_2, type:

   $ server_cepp server_2 -service -info
   Output:

```
server_2 :
CIFS share name = \\DVBL\CHECK$
cifs_server = DVBL
heartbeat_interval = 15 seconds
pool_name server_required  access_checks_ignored req_timeout
retry_timeout
pool1     yes                   0
5000        25000
```

Display the CEPA facility statistics

Procedure

1. To display statistics about the CEPA pool, use this command syntax:

```
$ server_cepp <movername> -pool -stats -all
```
where:

<movername> = name of the Data Mover

Example:

To display statistics about the CEPA pool on the Data Mover server_2, type:

```
$ server_cepp server_2 -pool -stats
```
Output:

```
server_2 :
pool_name = pool1
Event Name         Requests   Min(us)    Max(us)   Average(us)
OpenFileWrite        2         659        758         709
CloseModified        2         604        635         620
Total Requests = 4
Min(us) = 604
Max(us) = 758
Average(us) = 664
```

Display detailed information for a CEPA pool

Procedure

1. To display configuration information for a CEPA pool, use this command syntax:

   ```
   $ server_cepp <movername> -pool -info
   ```
   where:

   <movername> = name of the Data Mover

   Example:

   To display configuration information for a CEPA pool on the Data Mover server_2, type:

   ```
   $ server_cepp server_2 -pool -info
   ```
   Output:

   ```
   server_2 :
   pool_name = pool1
   server_required = yes
   access_checks_ignored = 0
   req_timeout = 5000 ms
   retry_timeout = 25000 ms
   pre_events = OpenFileNoAccess,OpenFileRead
   post_events = CreateFile,DeleteFile
   post_err_events = CreateFile,DeleteFile
   CEPP Servers:
   IP = 128.221.252.100, state = ONLINE, vendor = Unknown
   ```

CHAPTER 12

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.

The task to manage VCAPS is:

Set up access

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.

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.

The FeedInterval and MaxEventsPerFeed delivery cadences are used simultaneously.

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

CHAPTER 13

Managing CEE for RabbitMQ

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. Dell EMC also recommends using RabbitMQ's inherent policy parameter which imposes a "queue length limit" as described in the RabbitMQ documentation.

The task to configure CEE Messaging for RabbitMQ is:

Set up CEE for RabbitMQ

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

Procedure

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.

CHAPTER 14

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 included are:

Install the CAVA Calculator

Before you begin

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.

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:

Procedure

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

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

Procedure

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

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:

Procedure

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.

Configure the sizing tool

Before you begin

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

Table 12 on page 101 lists the actions you must perform to configure the sizing tool.

Table 12 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 on page 102
2.	Manually compile the cava.mof file used by CEE CAVA.	Manually compile the cava.mof file on page 103
3.	Create the cavamon.dat file on the monitoring server.	Create the cavamon.dat file on page 103

Table 12 Actions for configuring the sizing tool (continued)

Task	Action	Procedure
	Note Only needed if you use cavamon.exe to run the sizing tool.	
4.	Start the sizing tool on the monitoring server.	Start the sizing tool on page 103
5.	Size the anivirus agent.	Size the antivirus agent on page 104
6.	Optionally run **cavamon.vbs**.	(Optional) Gather AV statistics with cavamon.vbs on page 104

Enable the sizing tool

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.

Procedure

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\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 between 1 and 60 (seconds). 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 on page 77.

Manually compile the cava.mof file

Before starting the cavamon.exe utility, you must manually compile the Managed Object Format (MOF) file used by CEE CAVA.

Procedure

1. Locate the **cava.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 cava.mof`** command.

Create the cavamon.dat file

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.

Use this procedure to create the cavamon.dat file:

Procedure

1. Create a text file, named cavamon.dat, in the Program Files\EMC\CAVA 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 will operate 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

   Each AV machine listed in the cavamon.dat file must have the CAVA sizing tool enabled.

3. Save and close the file.

Start the sizing tool

Procedure

1. Restart the EMC CAVA service.
2. From the `Program Files\EMC\CAVA` 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

Every interval (set in the sizing tool Registry entry with a default of 10 seconds), 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

Procedure

1. 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 http://www.microsoft.com).

CHAPTER 15

Third-Party Consumer Applications

Topics to set up access to a third-party vendor application, which is used for managing the content stored on the file systems, and topics to allow communication with the CEE include:

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.

Table 9 on page 66 lists the event types you can specify for a response from the consumer application. You determine the events for which you want to be notified, based on the consumer application used.

The Data Mover or 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

Procedure

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.

CHAPTER 16

Troubleshooting

As part of an effort to continuously improve and enhance the performance and capabilities of its product lines, new versions of product hardware and software are periodically released. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, contact your Customer Support representative.

Problem Resolution Roadmap for VNX contains additional information about using Online Support and resolving problems.

Topics included in this chapter are:

Dell EMC E-Lab Interoperability Navigator

The Dell EMC 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 https://Support.EMC.com. After logging in:

- Click **Diagnostics & Tools**.
- Under **Tools for Dell EMC Servers, Storage and Networking**, click **E-Lab Navigator**.

VNX user customized documentation

Dell EMC provides the ability to create step-by-step planning, installation, and maintenance instructions tailored to your environment. To create VNX user customized documentation, go to: https://mydocs.emc.com/VNX.

Error messages

All event, alert, and status messages provide detailed information and recommended actions to help you troubleshoot the situation.

To view message details, use any of these methods:

- Unisphere software:
  - Right-click an event, alert, or status message and select to view Event Details, Alert Details, or Status Details.
- CLI:
  - Type nas_message -info <MessageID>, where <MessageID> is the message identification number.
- *Celerra Error Messages Guide*:
  - Use this guide to locate information about messages that are in an earlier-release message format.
- Online Support:
  - Use the text from the error message's brief description or the message's ID to search the Knowledgebase on Online Support. After logging in to Online Support, locate the applicable **Support by Product** page, and search for the error message.

Known problems

Table 13 on page 110 describes the known problems that might occur and presents the workarounds.

Table 13 CEE known problems and workarounds

Known problem	Symptom	Workaround
AV Machine Failover	Upon failure of the AV machine, a VC client thread polls the AV	The `shutdown=` parameter in the `viruschecker.conf` file specifies the

Table 13 CEE known problems and workarounds (continued)

Known problem	Symptom	Workaround
If you have configured more than one server, and if one of the AV machines fails, file scanning is redirected to other available AV machines. If none of the AV machines are available, the VNX Data Mover or Unity NAS server CIFS service proceeds without any virus-checking capabilities.	machine in the background. This enables the VC client to reconnect to the failed AV machine when it is operational. **Note** All AV engines are polled every 60 seconds (by default) to determine which AV engines are online and available.	shutdown action to take when an AV machine is not available. CAVA can be configured to prevent all CIFS client access to any VNX or Unity share when AV machines are unavailable. The `shutdown=` parameter in Table 8 on page 59 provides details.
Using Microsoft SMB2 When using Microsoft SMB2 as the protocol between AV engines and VNX or Unity, the Microsoft Redirector uses a local cache for directory metadata on the machine where the AV engine resides. By default, this cache is invalidated every 10 seconds. As a consequence, the updates that are made to the server share during this period cannot be seen in the cache. It is possible under these conditions that AV engines will not scan the files requested by CAVA, as the Redirector intercepts the scan and returns a file not found error. This failure to scan occurs because the contents of the Redirector's cache and the actual directory structure on the server share do not match.	The Data Mover's or NAS server's `server_log` contains the following SMB2 error message: `file not found`	To avoid this condition, you must disable the directory cache on the machines on which CAVA and AV engines are running by using the following procedure: 1. Open the Windows **Registry Editor** and navigate to `HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters`. 2. Right-click **Parameters** and select **New > DWORD Value**. 3. For the new **REG_DWORD** entry, type a name of **DirectoryCacheLifetime**. 4. Set the value to `0` to disable **DirectoryCacheLifetime**. 5. Click **OK**. 6. Restart the machine.
Event publishing agent cannot communicate with the EMC CAVA service.	`OFFLINE` is displayed when running a CEPA command.	Open Windows Services and verify that the EMC CAVA service is started and running.

Training and Professional Services

Customer Education courses help you learn how the storage products you purchased work together within your environment to maximize your entire infrastructure investment. Customer Education features online and hands-on training in state-of-the-art labs conveniently located throughout the world. Customer training courses are developed and delivered by experts. Go to Online Support at https://Support.EMC.com for course and registration information.

Professional Services can help you implement your system efficiently. Consultants evaluate your business, IT processes, and technology, and recommend ways that you can leverage your information for the most benefit. From business plan to implementation, you get the experience and expertise that you need without straining your IT staff or hiring and training new personnel. Contact your Customer Support Representative for more information.

INDEX

U

V

W