Dell EMC Unity™ Family

Version 4.5

Configuring Hosts to Access SMB File Systems

P/N 302-002-566 REV 04

DELL EMC

Published January 2019

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

CONTENTS

Additional resources

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

Where to get help
Support, product, and licensing information can be obtained as follows:

Product information
For product and feature documentation or release notes, go to Unity Technical Documentation at: www.emc.com/en-us/documentation/unity-family.htm.

Troubleshooting
For information about products, software updates, licensing, and service, go to Online Support (registration required) at: https://Support.EMC.com. After logging in, locate the appropriate **Support by Product** page.

Technical support
For technical support and service requests, go to Online Support at: https://Support.EMC.com. After logging in, locate **Create a service request**. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

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.

CHAPTER 1

Setting up a host for SMB storage

This chapter contains the following topics:

Requirements for setting up a host

These system and network requirements must be met before setting up a host to use Unity storage.

Before you can set up a host to use Unity storage, the following storage system and network requirements must be met.

Overview

This topic describes the purpose of this document, its intended audience, and provides a list of related documentation.

This document is part of the Unity documentation set. It describes how to set up the Windows hosts with clients that need to access Server Message Block (SMB) file system storage on a Unity system.

This document is intended for the person or persons who are responsible for setting up the hosts to access the Unity storage.

Readers of this document a should be familiar with Unity SMB file system storage and the Windows operating system running on hosts with clients that will access Unity SMB file system storage.

Other Unity documents include:

- *Installation Guide*
- *Hardware Information Guide*
- *Configuring Hosts to Access NFS File Systems*
- *Configuring Hosts to Access Fibre Channel (FC) or iSCSI LUNs*
- *Configuring Hosts to Access VMware NFS or VMware VMFS Datastores*
- *EMC Storage Integrator for Windows Suite*
- *Unisphere CLI User Guide*

Unisphere help provides specific information about the Unity storage, features, and functionality.

System requirements

Before configuring hosts to access the storage system, ensure that these requirements are met.

Complete the following tasks before connecting hosts to the storage system:

- Install and configure the system using the **Initial Configuration** wizard.
- Use Unisphere or the CLI to configure NAS servers or interfaces, or iSCSI or Fibre Channel (FC) LUNs, on the storage system.

Network requirements

This topic lists the network requirements for a host attaching to the storage system.

Ensure that you observe these network requirements:

- The host (client) must be in a LAN environment with the NAS server.

- The NAS server can be either a member of a Windows Active Directory domain or operate independently of any Windows domain as a stand-alone SMB server.
- For SMB shares that are in a Windows Active Directory domain, you must also configure DNS and NTP.
- If the NAS server is enabled for multiprotocol (SMB and NFS), configure a Unix Directory Services (UDS) using the NIS or LDAP protocol, local files, or local files and a UDS.
- Unisphere online help describes how to configure Unix Directory Service (either NIS or LDAP) on the Unity.

SMB NAS server in a Windows domain

This topic describes an SMB NAS server in a Windows Active Directory domain.

An SMB NAS server with Active Directory enabled:

- Uses domain-based Kerberos authentication
- Maintains its own identity (computer account) in the domain
- Leverages domain site information to locate services, such as domain controllers.

Associating an SMB NAS server with a Windows domain allows any users in the domain to connect to the SMB server. In addition, authentication and authorization settings maintained on the Active Directory server apply to the files and folders on the SMB file system.

An SMB NAS server with Active Directory enabled requires a Windows domain with an Active Directory (AD) server and a DNS server. You must also configure NTP.

Stand-alone SMB NAS server

This topic describes a stand-alone SMB NAS server.

A stand-alone SMB NAS server does not have access to a Windows domain or its associates services. Only users with local user accounts created and managed on the stand-alone SMB NAS server can access the server, and the SMB server performs user authentication.

A stand-alone SMB NAS server requires a Windows workgroup.

Host software in an SMB environment

This topic provides an overview of the host software for a Unity system in an SMB environment.

This section describes the host software that is available for a Unity system in an SMB environment and describes how to install this software on a host that will use Unity SMB file system storage.

Common AntiVirus Agent

This topic describes the antivirus solution for SMB clients using Unity systems.

The Common AntiVirus Agent (CAVA) provides an antivirus solution for SMB clients using Unity systems. It uses third-party antivirus software to identify and eliminate known viruses before they infect files on the system. CAVA is part of the Common Event Enabler (CEE) software package. For information about the third-party antivirus software that CAVA supports, refer to the Unity Support Matrix on the

support website. For information about installing the enabler, see *Using the Common Event Enabler on Windows Platforms* on the support website.

Management snap-ins

This topic lists the management snap-ins that a Unity NAS server supports.

A NAS server supports the Unity NAS Management snap-in, which consist of the following Microsoft Management Console (MMC) snap-ins that you can use to manage home directories, security settings, and virus-checking on a NAS server from a Windows computer:

- Home Directory Management snap-in
- NAS Server Management snap-in
- AntiVirus Management snap-in

Home Directory Management snap-in

This topic describes how the home directory feature simplifies administration of personal shares.

You can use the Home Directory Management snap-in to associate a username with a directory; that directory then acts as the user's home directory. The home directory feature simplifies the administration of personal shares and the process of connecting to them because it lets you use a single share name, called HOME, to which all users can connect.

NAS Server Management snap-in

This topic describes how to use the audit policy and user rights assignment nodes of the NAS Server Management snap-in.

Audit Policy node

You can use the Audit Policy node under NAS Server Security Settings to determine which NAS server security events are logged in the security log. You can then view the security log by using the Windows Event Viewer. You can log successful attempts, failed attempts, both, or neither. The audit policies that appear in the Audit Policy node are a subset of the policies available as group policy objects (GPOs) in Active Domain Users and Computers. Audit policies are local policies and apply to the selected NAS server. You cannot use the Audit Policy node to manage GPO audit policies.

User Rights Assignment node

You can use the User Rights Assignment node to manage which users and groups have login and task privileges to a NAS server. The user rights assignments that appear in the User Rights Assignment node are a subset of the user rights assignments available as GPOs in Active Domain Users and Computers. User rights assignments are local policies and apply to the selected NAS server. You cannot use the User Rights Assignment node to manage GPO policies.

Common AntiVirus Management snap-in

You can use the Common AntiVirus Management snap-in to manage the virus-checking parameters (viruschecker.conf file) used with Common AntiVirus Agent (CAVA) and third-party antivirus programs.

Installing host software for SMB

This topic provides a list of the host software that you can install for Unity SMB environments, the purpose of each software package, the systems on which you can install the packages, and the installation steps.

Table 1 Host software for Unity SMB environments

Software	Install software if you want to	Install on
Home Directory Management snap-in	Manage user home directories.	The Windows system from which you will manage the Unity NAS servers in the domain.
NAS Server Management snap-in	Audit NAS server security events in the security log and manage user and group access and task privileges for a NAS server.	The Windows system from which you will manage the Unity NAS servers in the domain.
CEE AntiVirus Management snap-in	Manage virus checking parameters used in conjunction with CAVA and third-party antivirus programs.	The Windows system that uses Unity storage. Requires one or more Windows hosts that are AntiVirus (AV) servers. These AV servers can also be hosts that use Unity storage.

To install the host software for an SMB environment on a Unity host:

Procedure

1. Log in to the host through an account with administrator privileges.
2. Download the software package that you want to install as follows:
   a. Navigate to the software download section for the host software on the online support website.
   b. Choose the software package that you want to install, and select the option to save the software to the host.
3. In the directory where you saved the software, double-click the executable file to start the installation wizard.
4. On the **Product Installation** page, select the software package that you want to install on the host.
5. Either accept the default location for the program files by clicking **Next**, or specify a different location by typing the path to the folder or by clicking **Change** to browse for the folder and clicking **Next** when you are finished.
6. On the **Welcome** page, click **Next.**
7. On the **License Agreement** page, click **Yes.**
8. On the **Select Installation Folder** page, verify that the displayed folder name is where you want to install the program files, and click **Next.**

   To select a different folder, click **Browse**, locate the folder, and click **Next.**

9. On the **Select Components** page, select the software package (component) that you want to install, clear the components you do not want to install, and click **Next.**
10. On the **Start Copying Files** page, click **Next.**
11. On the **InstallShield Wizard Complete** page, click **Finish.**
12. When the installation is complete, restart the host.

Using Windows Continuous Availability

Since Windows 8, Windows environments provide the ability to add high-availability functionality to SMB resources. Windows CA allows applications running on hosts connected to shares with this property to support transparent server failover for implementations where the failover time is no longer than the application timeout. In these implementations, hosts can continue to access an SMB resource without the loss of an SMB session state, following a failover event.

Other features such as larger I/O size, offload copy, parallel I/O on same session, and directory leasing provide improvements to performance and user experience.

When Windows CA is enabled on a share, all I/O writes to the share are treated as synchronous write-through operations.

Using network high availability

This topic describes how to use link aggregation for high availability configurations.

The Unity system supports link aggregations that allow up to four Ethernet ports connected to the same physical or logical switch to be combined into a single logical link. To configure link aggregation on the system, each storage processor (SP) must have the same type and number of Ethernet ports as link aggregation actually creates two link aggregations — one on each SP. This provides high availability. If one of the ports in the link aggregation fails, the system directs the network traffic to one of the other ports in the aggregation. If you add an Ethernet I/O module to each SP in the system, you can create one additional link aggregation group (LAG) on the set of ports in the I/O module.

Link aggregations

This topic describes the advantages and function of link aggregations.

Link aggregations use the Link Aggregation Control Protocol (LACP) IEEE 802.3ad standard.

Note

Link Aggregation does not apply to iSCSI interfaces.

A link aggregation appears as a single Ethernet link with these advantages:

- High availability of network paths to and from the Unity system — If one physical port in a link aggregation fails, the system does not lose connectivity.
- Possible increased overall throughput — Because multiple physical ports are bonded into one logical port with network traffic distributed between the multiple physical ports.

Although link aggregations can provide more overall bandwidth than a single port, the connection to any single client runs through one physical port and is therefore limited

by the port's bandwidth. If the connection to one port fails, the switch automatically switches traffic to the remaining ports in the group. When the connection is restored, the switch automatically resumes using the port as part of the group.

On the Unity system, you can configure up to four ports in a link aggregation. When you configure a link aggregation, you are configuring two link aggregations — one on each SP. If one of the ports in an aggregation fails, the system directs network traffic to one of the other ports in the group.

Switch requirements

This topic describes switch requirements when using link aggregation.

If the Unity ports are connected to different network switches, you should configure all switch ports connected to these ports to immediately switch from blocking mode to forwarding mode and not pass through spanning tree states of listening and learning when an interface comes up. On Cisco switches, this means that you must enable the portfast capability for each switch port connected to a Unity port to guarantee that the switch forwards the Ethernet frame that the storage system generates when a physical link is enabled. You enable the portfast capability on a port-to-port basis. When enabled, the portfast variable causes the port to immediately switch from blocking to forwarding mode. Do not use portfast on switch-to-switch connections.

For link aggregation, network switches must have IEEE 802.3ad protocol support and guarantee that packets from a single TCP connection always go through the same link in a single direction.

Configuring a link aggregation

This topic describes link aggregation configuration and lists the required configuration tasks.

For link aggregation, you have at least one 802.3ad-compliant switch, each with an available port for each switch port you want to connect to a Unity port in the aggregation.

The term NIC teaming refers to all NIC redundancy schemes, including link aggregation with 802.3ad.

For link aggregation, you need to perform two sets of configuration tasks:

- Configure a link aggregation from the switch to the Unity system
- Configure a link aggregation from the host to the switch

Configuring link aggregation from the switch to the Unity system

Learn how to configure the switch ports and join them into a link aggregation.

Procedure

1. Configure the switch ports, which are connected to the Unity system, for LACP in active mode. Refer to the documentation provided with your switch for details.
2. Join the ports into a link aggregation using Unisphere. To do this:
   a. Select the **Settings** icon, then select **Access** > **Ethernet**.
   b. Select an Ethernet port, then select **Link Aggregation** > **Create Link Aggregation**.
   c. Select the ports for the link aggregation, then select **Create**.

Results

Two link aggregations are created with the same ports — one aggregation on each SP.

Configuring link aggregation from host to switch

This topic describes how to configure link aggregation from host to switch. Steps involve configuring switch ports for link aggregation and NIC teaming on the host. These steps are for an Intel network interface driver.

Procedure

1. Configure the switch ports, which are connected to the host, for link aggregation.
2. Configure NIC teaming on a Windows Server version 2008 SP2 through 2016, or Windows 8 host.

   Note

   Windows Server 2008 through 2016 and Windows 8 hosts refer to link aggregation as NIC teaming. Windows Server 2012 R2, 2016, and Windows 8 automatically detect NIC teaming on Unity, and configure the host to use the same interfaces as Unity. Manual configuration is not necessary.

   a. In the **Control Panel**, select **Network and Internet** > **Network Connections**.

   b. In the **Network Connections** dialog box, right-click one NIC you want in the team and click **Properties.**

   c. Click **Configure.**

   d. In the **Properties** dialog box, select the **Teaming** tab.
3. In the **Teaming** tab:

   a. Select **Team this adapter with other adapters**.

   b. Click **New Team**.

   The **New Team Wizard** opens.
4. In the **New Team Wizard**:

   a. Specify the name for the team and click **Next.**

   b. Select the other NICs that you want in the team and click **Next.**

   c. Select the team type and click **Next**. For information on a type, select the type and read the information below the selection box.

   d. Click **Finish.**
5. If you selected **Adaptive Load Balancing** as the team type and you want to use the new NIC team for Hyper-V virtual machines, disable **Receive Load Balancing**:

   a. Click the **Advanced** tab.

   b. Under Settings, select **Receive Load Balancing**.

   c. Under Values, select **Disabled.**

   d. Click **OK.**

The new team shows in the **Network Connections** dialog box as a Local Area Network Connection.

6. To use the new NIC team for a virtual machine:
   a. In the Hyper-V Manager, under Virtual Machines, select the virtual machine.
   b. Under Actions, select **Virtual Network Manager**.
   c. In the Virtual Network Manager, under Virtual Networks, select **VM NIC - Virtual Machine Network**.
   d. Under Connection type, select the network type and the NIC team.
   e. Click **Apply.**
   f. When the changes have been appled, click **OK.**

Configuring Windows Server 2012 R2 and Windows Server 2016

Procedure

1. Open the Server Manager Console.
2. Click **Local Server** on the left side and locate the Properties box (the top box on this screen).
3. Locate **NIC Teaming** and click **Disabled**.
4. In the Adapters and Interfaces section, press and hold the **Ctrl** key on the keyboard, and then click the adapters you want to add to a team.
5. Click **TASKS** on the top right of the Adapters and Interfaces section, and then select **Add to New Team**.
6. In the NIC Teaming window, add a name for the team you are creating and select any adapters that you may have missed.

Note

If you are configuring the server remotely, you might lose connectivity to the server after the team is created. This happens if you are connected through an adapter that is being added to the team. Once the team is created, a teamed adapter is given an address through DHCP and will need to be reconfigured with a static IP address, if you had one assigned to it.

If you open the Network Connections window, you should see your teamed network adapter. You can configure it with an IP address, if needed.

Using SMB encryption

Windows 8 and Windows 12 SMB3 environments provide the ability to encrypt data stored on Unity SMB file systems as that data moves between Unity and the Windows host.

Note

In Unisphere, this type of encryption is called Protocol Encryption.

SMB encryption at the share level is enabled on a specific share and is enforced when that share is accessed. To configure SMB encryption for a share, see the Unisphere online help.

Optionally, encryption can be enforced at the system level (where encryption is set in the registry of the NAS server), and all share access would require encryption. Client-level configuration is not needed.

Configuring SMB file system storage

Procedure

1. Use Unisphere or the Unity CLI to create Unity SMB file system storage for the host (client).
2. For information on performing these tasks, refer to the Unisphere online help.

Configuring user access to the SMB share

This task describes how to configure user access to the SMB share from the host. You will need the name or IP address of the Unity NAS server.

User access to the share is configured per file using the Active Directory:

Procedure

1. Log in to the Windows host with the Active Directory from a domain administrator account.

   Note

   The Windows host must have access to the domain with the NAS server for the SMB share.

2. Open the Computer Management window:
   a. For all Windows OSs, open the Computer Management MMC snap-in.
   b. For a Windows Server version 2008 SP2 through 2016 or Windows 8 host, click **Start** and select **Control Panel** > **Administrative Tools** > **Computer Management**.
3. In the **Computer Management** tree, right-click **Computer Management (local)**.
4. Select **Connect to another computer**.

   The **Select Computer** dialog opens.
5. In the **Select Computer** dialog box, enter the name or IP address of the NAS server to provide the client SMB shares.
6. In the Computer Management tree, select **System Tools** > **File Systems** > **Shares**.

   The available shares appear on the right. If the Unity shares do not appear, make sure that you are logged in to the correct domain.
7. Right-click the share whose permissions you want to change and select **Properties.**
8. Click the **Share Permissions** tab.
9. Select the user or group and the permissions for the selected user or group.
10. Click **OK.**

Mapping the SMB share

This task directs you to connect the host to the SMB share. It also describes how to get the export path for the share.

You will need the export path for the share (`\\NASServer\share`), which you can find in Unisphere, as described below.

Procedure

1. On the Windows host, use the Windows Map Network Drive function to connect the host to the SMB share and optionally to reconnect to the share whenever you log in to the host.
2. If you need the export path for the share, follow these steps:
   a. Access Unisphere.
   b. Under **Storage**, select **File** > **SMB Shares**.
   c. Add the **Export Path** column to the view.
   d. Locate the SMB share on the screen.

   If you have read/write access to the share, you can create directories on the share and store files in the directories (after the share is mapped).

CHAPTER 2

Migrating SMB Data to a Unity storage system

You can migrate SMB data to a Unity storage system using a manual copy. A manual copy operation disrupts access to the data and may not preserve the ACLs and permissions within the file structure.

This chapter contains the following topics:

Migration environment and limitations

This topic describes requirements and limitations for data migration.

You can migrate data to the Unity system with either a manual copy or an application-specific tool, if one is available.

If the SMB configuration that you want to migrate has any of the following, contact your Unity service provider:

- More shares than you want to migrate.
- Permissions that you do not want to manually reassign to the Unity shares.
- Any share that you want to divide between Unity shares.
- Any share that you want to combine with other shares on the same Unity share.

Table 2 on page 20 outlines the environment required for data migration. Table 3 on page 20 lists the characteristics of a manual copy migration.

Table 2 Environment for data migration

Component	Requirement
Unity storage	File system with share sized to accommodate the data in the share that you want to migrate and to allow for data growth
Host	Host with read access to the share containing the data to be migrated and with write access to the Unity share for the migrated data
Share	Share that you migrate in its entirety to the Unity share

Table 3 Characteristics of manual copy migration

Component	Characteristic
Permissions	May not be preserved
Downtime	Downtime is relative to the time required for: • Copying the share contents to the Unity share • Reconfiguring the hosts to connect to the Unity share

For both a manual copy migration and a migration with an application, the downtime is relative to the time required for:

- Copying the share contents to the Unity share
- Reconfiguring the hosts to connect to the Unity share

Migrating data

This topic lists the tasks for migrating data to a Unity share.

To migrate data to a Unity share, set up access to the share. Then migrate the data.

Setting up access to a Unity share for the SMB host

This topic lists the steps to configure user access to the new share in the Active Directory and then map the share.

On the host that you want to use for the data migration:

Procedure

1. Configure user access to the new share in the Active Directory.

   For detailed steps, refer to Configuring user access to the SMB share on page 16.

2. Map the new share.

   For detailed steps, refer to Mapping the SMB share on page 17.

Migrating the data with a manual copy

This topic provides the steps to manually copy data one share at a time (instead of using an application-specific tool).

A manual copy minimizes the time during which a host cannot access a share being migrated.

Procedure

1. If any clients are actively using the share, disconnect these clients and any other clients that could access the data you are migrating.
2. Use the method that you think is best for copying data from the current storage location to the new Unity share.

   This method can be a cut-and-paste or drag-and-drop operation. Ensure that the method you choose preserves metadata such as file attributes, timestamps, and access rights that you need to preserve.

3. When the copy operation is complete, reconnect the clients to the new share exported by the Unity system and map a drive to this share as needed.

CHAPTER 3

Managing SMB File System Storage with Windows Tools

This chapter contains the following topics:

Opening Computer Management MMC

This topic describes how to open the Computer Management Microsoft Management Console (MMC) for a specific NAS server.

Procedure

1. Login to the Windows host that is part of the Active Directory with domain administrator account.

   The Windows host must have access to the domain with the Unity NAS server.
2. Open the Computer Management page:
   - For all Windows OSs, open the Computer Management MMC snap-in.
   - For a Windows Server versions 2008 SP2 through 2016 or Windows 8 host, click **Start** and select **Administrative Tools** > **Computer Management**.
3. Right-click **Computer Management**.
4. Select **Connect** to another computer.
5. Enter the name of the Unity NAS server, and click **OK**.

   Log in as the Administrator with Administrator rights to use the MMC snap-ins.

Creating shares and setting ACLs

It is recommended that you use Unisphere to create SMB shares, as described in Unisphere help, and then use the MMC to set access (ACLs) for the shares. As an alternative to using Unisphere, after you create an SMB file system on the Unity system, you can use the MMC to create shares within that folder.

To create a Windows share with the MMC, you must:

- Have mounted the Unity share of the root directory of the file system and created the directories you want to share in it
- Be a Unity administrator

Setting ACLs on an existing share

This topic describes how to set ACLs on an existing share by using the Computer Management MMC.

Procedure

1. Open the Computer Management MMC as described in Opening Computer Management MMC on page 24.
2. In the console tree, select **File Systems** > **Shares**.

   The current shares in use appear on the right.
3. Right-click the share whose permissions you want to change and select **Properties.**
4. Click the **Share Permissions** tab.
5. Select the user or group and the permissions for the selected user or group.
6. Click **OK.**

Creating a share and setting its ACLs

This topic provides the steps to create a share and set its ACLs by using the Computer Management MMC.

Procedure

1. Open the Computer Management MMC as described in Opening Computer Management MMC on page 24.
2. In the console tree, click **File Systems** > **Shares**.

   The current shares in use appear on the right.
3. Right-click **Shares**, and select **New File Share** from the shortcut menu.

   The **Share a Folder Wizard** appears.
4. Enter the name of the folder to share, share name for the folder, and share description. Then click **Next.**

   The wizard prompts you for share permissions.
5. Set permissions by choosing one of the options.

   With the **Customize Share and Folder Permissions** or **Customize Permissions** option, you can assign permissions to individual groups and users.
6. Click **Finish.**

Using the home directory feature

The home directory feature simplifies the administration of personal shares and the process of connecting to them by letting you associate a username with a directory that then acts as the user's home directory. The home directory is mapped in a user's profile so that upon login, the home directory is automatically connected to a network drive.

The home directory feature is enabled, configured, and managed by the Home Directory Management snap-in. This feature lets you leverage the built-in Home Directory share using \HOME or \%username% when defining the user's logon profile. You do not have to create individual shares for each user.

The home directory feature is enabled by default.

To map and display the user's logon profile, do either of the following:

- Use \HOME as the built-in share and profile:

```
Z:  \\SMBServer1\HOME
```

- Use \%username% as the built-in share and profile:

```
Z:  \\SMBServer1\%username%
```

Home directory restrictions

A special share name, HOME, is reserved for the home directory. The following restrictions apply. If you have:

- Created a share called HOME, you cannot enable the home directory feature.

- Enabled the home directory feature, you cannot create a share called HOME.

A home directory is configured in a user's Windows user profile by using the Universal Naming Convention (UNC) path: `\\NAS_server\HOME` or `\\NAS_server\%username%`, where *NAS_server* is the IP address, computer name, or NetBIOS name of the NAS server.

HOME is a special share that is reserved for the home directory feature. When HOME is used in the path for a user's home directory and the user logs in, the user's home directory is automatically mapped to a network drive and the HOMEDRIVE, HOMEPATH, and HOMESHARE environment variables are automatically set.

Configuring the user profile in the Active Directory

Follow these steps to configure the user's logon profile in the Windows Active Directory. A Windows server and domain administrator account are required.

Procedure

1. Log in to the Windows server from a domain administrator account.
2. From the Control Panel, select **Administrative Tools** > **Active Directory Users and Computers**.
3. Click **Users** to display the users in the right pane.
4. Right-click a user and select **Properties.**

   The user's **User Properties** window appears.
5. Click the **Profile** tab and under Home folder:
   a. Select **Connect.**
   b. Select the drive letter you want to map to the home directory.
   c. In **To**, type: `\\NAS_server\HOME` or \\NAS_server\%username%, where *NAS_server* is the IP address, computer name, or NetBIOS name of the Unity NAS server.
6. Click **OK.**

Adding a home directory with expressions

This topic lists the steps for adding a home directory by using expressions. This procedure requires a domain administrator account.

Procedure

1. Log in to the Windows server from a domain administrator account.
2. From the Control Panel, select **Administrative Tools** > **EMC Unity VNX VNXe NAS Management**.
3. Right-click the **HomeDir** folder icon and select **New** > **home directory entry**.

   The home directory property page appears.
4. Enter the following information:
   a. In **Domain**, type the name of the user's domain using the NetBIOS name.

   NOTICE

   Do not use the fully qualified domain name.

For example, if the domain name is Company.local, you can type one of the following: `company`, `comp`, or `.*` (regular expressions must be true for this option to work).

b. In **User**, type the name of the user or the wildcard string.

For example, if the username is Tom, you can type one of the following: `T*` for usernames starting with T, `*` for any username, or `[r-v].*` for usernames starting with r, s, t, u, or v (regular expressions must be true for this option to work).

c. In the Path, type the pathname using one of the following methods:

Type the path of the folder, for example, `\HomeDirShare\dir1`.

Click **Browse** and either select the folder or create one.

If you want to automatically create the folder, select **Auto Create Directory**.

Examples of directories are:

- `\HomeDirShare\dir1\User1`
- `\HomeDirShare\<d>\<u>`, which creates a folder with the domain name `d` and a directory with the user name `u`.

5. Click **OK.**

Table 4 on page 27 provides examples of expression formats for adding a home directory.

Table 4 Examples of expression formats

Domain	User	Path	Options	Results
*	*	`\HomeDirShare\`	None	All the users have `\HomeDirShare` as their home directory.
*	*a	`\HomeDirShare\`	None	Users whose username starting with 'a' have `\HomeDirShare` as their home directory.
*	*	`\HomeDirShare \<d>\<u>\`	Auto Create Directory = True	All the users have their own directories. For example, user Bob in domain company has `\HomeDirShare \company\Bob` as his home directory.
comp	[a-d].*	`\HomeDirShare \FolksA-D\<d> \<u>\`	Auto Create Directory = True Regexp=True	Users whose username start with a, b, c or d in domain company have `\HomeDirShare\FolksA-D\company\` as their home directory, where u is their username.

Using Group Policy objects

In a Windows Server version 2008 SP2 through 2016 host domain controller, administrators can use Group Policy to define configuration options for groups of users and computers. Windows GPO can control elements such as local, domain, and network security settings. The Group Policy settings are stored in GPOs that are linked to the site, domain, and organizational unit (OU) containers in the Active Directory. The domain controller replicates GPOs on all domain controllers within the domain.

Audit Policy is a component of the Unity NAS Management snap-in, which is installed as a Microsoft Management Console (MMC) snap-in into the Management Console on a Windows Server version 2008 SP2 thru 2016 system.

You can use audit policies to determine which NAS server security events are logged in the security log. You can choose to log successful attempts, failed attempts, both, or neither. Audited events are viewed in the security log of the Windows Event Viewer.

The audit policies that appear in the Audit Policy node are a subset of the policies available as GPO in Active Directory Users and Computers (ADUC). These audit policies are local policies and apply only to the selected NAS server. You cannot use the Audit Policy node to manage GPO audit policies.

If an audit policy is defined as a GPO in ADUC, the GPO setting overrides the local setting. When the domain administrator changes an audit policy on the domain controller, that change is reflected on the NAS server and you can view it by using the Audit Policy node. You can change the local audit policy, but it is not in effect until the GPO for that audit policy is disabled. If auditing is disabled, the GPO setting remains in the Effective setting column.

GPO support on a NAS server

A NAS server provides support for GPOs by retrieving and storing a copy of the GPO settings for each NAS server joined to a Windows Server domain. A NAS server stores the GPO settings in its GPO cache.

When the storage system powers up, it reads the settings stored in the GPO cache, and then retrieves the most recent GPO settings from the Windows domain controller. After retrieving the GPO settings, a NAS server automatically updates the settings based on the domain's refresh interval.

Supported GPO settings

A NAS server currently supports the following GPO Security settings:

Kerberos

- Maximum tolerance for computer clock synchronization (clock skew). Time synchronization is done per NAS server.
- Maximum lifetime for user ticket

Audit policy

- Audit account logon events
- Audit account management
- Audit directory service access

- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

Auditing SMB users and objects on page 31 provides more information.

User rights

- Access this computer from the network
- Back up files and directories
- Bypass traverse checking
- Deny access to this computer from the network
- Virus checking
- Generate security audits
- Manage auditing and security log
- Restore files and directories
- Take ownership of files or other objects

Security options

- Digitally sign client communication (always)
- Digitally sign client communication (when possible)
- Digitally sign server communication (always)
- Digitally sign server communication (when possible)
- LAN Manager Authentication Level

Event logs

- Maximum application log size
- Maximum security log size
- Maximum system log size
- Restrict guest access to application log
- Restrict guest access to security log
- Restrict guest access to system log
- Retain application log
- Retain security log
- Retain system log
- Retention method for application log
- Retention method for security log
- Retention method for system log

Group policy

- Disable background refresh of Group Policy

- Group Policy refresh interval for computers

Using SMB signing

SMB signing ensures that a packet has not been intercepted, changed, or replayed. The signing guarantees that a third party has not changed the packet. Signing adds a signature to every packet. The client and Unity NAS servers use this signature to verify the integrity of the packet. The Unity NAS servers support SMB1, SMB2, and SMB3.

For SMB signing to work, the client and the server in a transaction must have SMB signing enabled. SMB signing is always enabled on the Unity NAS servers, but is not required. As a result, if SMB signing is enabled on the client, signing is used, and if SMB signing is disabled on the client, no signing is used. Signing can be enforced by Active Directory domain policy

Monitoring NAS server connections and resource usage

You can use Windows administrative tools to monitor users, share access, and file use on NAS servers.

Monitoring users on a NAS server

This topic lists the steps to monitor the number of users connected to a NAS server.

Procedure

1. Open the Computer Management MMC for the NAS server you want to monitor as described in Opening Computer Management MMC on page 24.
2. In the console tree, click **Shared Folders** > **Sessions**.

   The current users connected to the NAS server appear on the right.
3. Optionally:
   - To force disconnections from the NAS server, right-click the username, and select **Close Session** from the shortcut menu.
   - To force all users to disconnect, right-click **Sessions**, and select **Disconnect All Sessions** from the shortcut menu.

Monitoring access to shares on the NAS server

This topics lists the steps to monitor access to shares on a NAS server.

Procedure

1. Open the Computer Management MMC for the NAS server as described in Opening Computer Management MMC on page 24.
2. In the console tree, click **Shared Folders** > **Sessions**.

   The current users connected to the NAS server appear on the right.
3. Optionally, to force disconnections from a share, right-click the share name, and select **Stop Sharing** from the shortcut menu.

Monitoring file use on the NAS server

This topic lists the steps to monitor file use on a NAS server by using the Computer Management MMC.

Procedure

1. Open the Computer Management MMC for the NAS server as described in Opening Computer Management MMC on page 24.
2. In the console tree, click **File Systems** > **Open Files**.

   The files in use appear on the right.
3. Optionally, to close an open file, right-click the file, and select **Close Open File** from the shortcut menu.
4. To close all open files, right-click the **Open Files** folder, and select **Disconnect All Open Files** from the shortcut menu.

Auditing SMB users and objects

To audit a NAS server, use the Unity NAS Management snap-in, which is an MMC snap-in. Installing host software for SMB on page 11 provides information about installing MMC snap-ins.

By default, auditing is disabled for all Windows object classes. To enable auditing, you must explicitly turn it on for specific events on a specific NAS server. After it is enabled, auditing is initiated on the relevant NAS server. The Unity NAS Management snap-in online help provides information about setting audit policies.

If the Group Policy Object (GPO) is configured and enabled on the NAS server, then the GPO configuration of the audit settings is used.

Auditing is available only on the specific object classes and events listed in Table 5 on page 31. Only a Unity advanced administrator can set auditing on a NAS server.

Table 5 Auditing object classes

Object class	Event	Audited for
Logon/logoff	SMB user login SMB guest login	success
	Domain controller returned a password authentication error Domain controller returned an unprocessed error code No reply from DC (insufficient resources or bad protocol)	failure
File and object access	Object open: • File and directory access; if system access control list (SACL) set, for read, write, delete, execute, set permissions, take ownership	success

Table 5 Auditing object classes (continued)

Object class	Event	Audited for
	• Security Access Manager (SAM) local group modification Close handle: • File and directory access; if SACL set for read, write, delete, execute, set permissions, take ownership • SAM database closed Object open for delete: File and directory access (if SACL set) Delete object: File and directory access (if SACL set)	
	SAM database access (lookup)	success and failure
Process tracking	Not supported	N/A
System restart/shutdown	Restart: • SMB service startup • SMB service shutdown • Audit log cleared	success
Security policies	Session privileges: • List user privileges • User rights assigned • User rights deleted Policy change: List policy categories and associated audit state	success
Use of user rights	Not supported	N/A
User and group management	Create local group Delete local group Add member to local group Remove member from local group	success

When auditing is enabled, the Event Viewer creates a Security log with the default settings shown in Table 6 on page 33.

Table 6 Default log settings

Log type	Maximum file size	Retention
Security	512 KB	10 days

The Unity NAS servers support auditing on individual folders and files.

Enabling auditing on a NAS server

Complete the following steps to enable auditing on a NAS server:

- Specifying the audit policy on page 33
- Setting the audit log parameters on page 34

Specifying the audit policy

This topic lists the steps to access the Security Management snap-in and specify audit policies.

After the Unity NAS Management Console is installed:

Procedure

1. Open the Computer Management MMC for the NAS server as described in Opening Computer Management MMC on page 24.
2. Click **Start**, and select **Programs or All Programs** > **Administrative Tools** > **Unity NAS Management**.
3. In the **Unity NAS Management** window, do one of the following:
   - If a NAS server is selected (a name appears after NAS Server Management), go to step 4.
   - If a NAS server is not selected:
     a. Right-click **NAS Server Management**, and select **Connect to NAS Server** from the shortcut menu.
     b. In the **Select NAS Server** box, select a NAS server using one of the following methods:
        - In the **Look in** list, select the domain where the NAS server you want to manage is located, and then select the NAS server from the list.
        - In the **Name** field, type the network name or IP address of the NAS server.
4. Double-click **NAS Server Management**, and double-click **NAS Server Security Settings**.
5. Select **Audit Policy**.

   The audit policies appear in the right panel.
6. Right-click **Audit Policy**, and select **Enable Auditing** from the shortcut menu.
7. Double-click an audit object in the right panel to define the audit policy for that object.

   The NAS Management snap-in online help provides more information about audit policy.

Setting the audit log parameters

This topic lists the steps to set the audit log parameters by using the Computer Management MMC for the NAS server.

Procedure

1. Open the Computer Management MMC for the NAS server as described in Opening Computer Management MMC on page 24.
2. Double-click **Event Viewer** and, for Windows Server versions 2008 SP2 through 2016, select **Windows Logs**.

   The specific log files are displayed.
3. Right-click the log file, and select **Properties** from the shortcut menu.

   The property sheet for the log appears. Normally, the **Maximum log size** field is locked.
4. After you have completed the procedure, return to the **Application Properties** dialog box for the log and click the arrows to increase or decrease the size of the log.
5. In the **Log size** area of the dialog box, specify what happens when the maximum log size is reached:
   - **Overwrite events as needed**: Specifies whether all new events are written to the log, even if the log is full. When the log is full, each new event replaces the oldest event.
   - **Overwrite events older than (*n*) days**: Overwrites events older than the number of days specified. Use the arrows to specify the limit, or click the field to enter the limit. The log file size specified in step 4 is not exceeded. New events are not added if the maximum log size is reached and there are no events older than this period.
   - **Do not overwrite events**: Fills the log up to the limit specified in step 4. When the log is full, no new events are written to it until you clear the log.
6. Click **OK** to save the settings.

Viewing the audit events

This topic lists the steps to view the audit events.

Procedure

1. Click **Start**, and select **All Programs** > **Administrative Tools** > **Event Viewer**.
2. Right-click the **Event Viewer** icon in the right panel, and select **Connect to Another Computer** from the shortcut menu.

   The **Select Computer** dialog box appears.
3. In the **Select Computer** dialogue, directly enter the name or IP of the NAS server. You may also select **Browse** to find the NAS server.
4. For a Windows Server version 2008 SP2 through 2016, click **Windows Logs**.
5. Click the log.

   The log entries appear in the right panel.
6. Double-click the log entry to view the event detail.

   The **Event Properties** window opens.

Disabling auditing

This topic lists the steps to disable auditing.

Procedure

1. Log in to a Windows Server version 2008 SP2 through 2016 domain controller with domain administrator privileges.
2. Click **Start**, and select **Programs or All Programs** > **Administrative Tools** > **Unity NAS Management**.
3. Do one of the following:
   - If a NAS server is already selected (name appears after NAS Server Management), go to step 4.
   - If a NAS server is not selected:
     a. Right-click **NAS Server Management**, and select **Connect to NAS Server** from the shortcut menu.
     b. In the **Select NAS Server** dialog box, select a NAS server using one of the following methods:
        - In the **Look in** list, select the domain in which the NAS server you want to manage is located, and select the NAS server from the list.
        - In the **Name** field, type the network name or IP address of the NAS server.
4. Double-click **NAS Server Management**, and double-click **NAS Server Security Settings**.
5. Right-click **Audit Policy**, and select **Disable Auditing** from the shortcut menu.

Accessing the security log for a NAS server

By default, each NAS server stores its Windows security log at `c:\security.evt`, which has a size limit of 512 KB. You can directly access this security log through the `C$` share of each NAS server with:

`\\`*`storage_server_netbios_name`*`\C$\security.evt`

where *storage_server_netbios_name* is the NetBIOS name of the NAS server.

Copying a share snapshot

This topic lists the steps to copy a share snapshot by using Windows Explorer.

Procedure

1. Access the NAS server that has the share that you want to copy by one of these methods:
   - Browse to the NAS server in Windows Explorer.
   - Select **Start** > **Run** > ***NAS_server_name***.
2. In the NAS server, right-click the share with the snapshot that you want to copy, select **Properties**.
3. Click the **Previous Versions** tab.
4. Select the snapshot (previous version) that you want to copy and click **Copy.**

A writeable copy of the snapshot is created in the location that you specify.

Restoring a share snapshot

This topic lists the steps to restore a share snapshot.

Restoring a storage resource to a snapshot returns (rolls back) the storage resource to the previous state captured by the snapshot. During the restore, the entire storage resource, including all files and data stored on it, is replaced with the contents of the snapshot.

NOTICE

To prevent data loss, ensure that all clients have completed all read and write operations to the storage resource that you want to restore.

Procedure

1. Access the NAS server that has the share that you want to copy by one of these methods:
   - Browse to the NAS server in Windows Explorer.
   - Select **Start** > **Run** > ***NAS_server_name***.
2. In the NAS server, right-click the share with the snapshot that you want to copy, select **Properties**.
3. Click the **Previous Versions** tab.
4. Select the snapshot (previous version) that you want to restore and click **Restore**.

Results

The restore operation does the following:

- For files that are in the current version, but not in the previous version being restored — Leaves these files unchanged on the share.
- For files that are in both the previous version being restored and the current version — Overwrites the files on the share with the contents of these files from the previous version.
- For files that are in the previous version being restored, but not in the current version — Adds these files to the share.

For example, suppose the following:

- The current version has files a, b, and f.
- The previous version being restored has files a, f, and g.

The restored version will have file b with the contents from the current version and files a, f, and g with the contents from the previous version.

CHAPTER 4

Using CEE CAVA with Unity

This chapter contains the following topics:

CAVA overview

The Common Event Enabler (CEE) package provides an antivirus solution (Common Anti-Virus Agent) for clients using the Unity system. It uses industry-standard SMB protocols in a Windows system. The Common Anti-Virus Agent (CAVA) uses third-party antivirus software to identify and eliminate known viruses before they infect files on the Unity system. Although the Unity NAS servers are resistant to viruses, Windows clients also require protection. The virus protection on the client reduces the chance that the client stores an infected file on the Storage Server and protects the client if it opens an infected file.

The CEE solution uses the following components:

- NAS server running the CEE CAVA virus-checking client
- Third-party antivirus (AV) engine
- CEE CAVA software

A third-party AV engine and the CEE CAVA software must be installed on at least one Windows Server version 2008 SP2 through 2016, or one Windows 8 workstation in the domain with the Unity system. This server is called an AV server.

This chapter describes how to use CEE CAVA with Unity. For in-depth information about managing CAVA, see *Using the Common Event Enabler on Windows Platforms* on the support website.

Unity NAS servers

The Unity NAS servers manage operations for Windows file systems and shares (SMB), Linux/UNIX file systems and shares (NFS), or both. For a CEE CAVA solution, the Unity system requires one or more NAS servers configured for SMB, and Windows user access to shares.

CEE CAVA virus-checking client

The virus-checking (VC) client is a CEE CAVA agent that runs on the Unity NAS server. The VC client interacts with the AV engine, which processes requests from the VC client. Scanning for viruses is supported only for SMB access. While the scan or other related actions take place, access to the file from any SMB client is blocked.

The VC client does the following:

- Queues and communicates the names of the files to CEE CAVA for it to scan.
- Provides and acknowledges event triggers for scans. Possible event triggers include:
  - A file is renamed on the Unity system.
  - A file is copied or saved to the Unity system.
  - A file is modified and closed on the Unity system.

Third-party antivirus software support

The CEE CAVA solution uses third-party antivirus software, called an AV engine, to identify and eliminate known viruses before they infect files on the Unity system. For the AV engines that CAVA supports, refer to the Unity Support Matrix on the support website.

CEE CAVA software

The CEE CAVA software is an application that runs on a Windows server (called an AV server). It communicates with a standard antivirus engine running on one or more servers to scan SMB files stored on a Unity system.

EMC Unity/VNX/VNXe NAS Management snap-in

The EMC Unity/VMX/VNXe NAS Management snap-in is an MMC snap-in to Unisphere. Use this snap-in to view or modify the CEE virus-checking parameters for the Unity NAS servers.

System requirements and limitations

The CEE CAVA solution requires the following:

- A Unity system with at least one NAS server configured on the network.
- Each NAS server should have a CAVA pool consisting of a minimum of two CAVA servers. This is specified in the NAS server's `viruschecker.conf` file.
- EMC Unity/VNX/VNXe NAS Management snap-in installed on a client system that has access to the Unity domain. For information about installing this snap-in, see Installing host software for SMB on page 11.
- If you are using Windows Server 2008, you must manually compile the `cava.mof` file while using CAVA's cavamon sizing tool.
- Third-party antivirus software running on one or more AV servers in the domain. CEE CAVA supports 32-bit and 64-bit Windows environments and corresponding third-party AV engines. The version of the AV engine version that is required depends on the operating system. For the latest third-party software system requirements, consult the appropriate third-party vendor website or documentation.
- CEE CAVA software installed on each AV server in the domain.

Note

With the exception of Trend Micro, the third party AV program must be installed prior to CEE CAVA on each AV server. Trend Micro must be installed after CEE CAVA.

We strongly recommend that the AV administrator update the virus definition files on all resident AV engines in the CEE CAVA pools.

Non-SMB protocols

The CEE CAVA solution is for clients running the SMB protocol only. If clients use the NFS or FTP protocols to move or modify files, the CEE CAVA solution does not scan these files for viruses.

Setting up CEE CAVA for NAS servers

To implement a CEE CAVA solution for NAS servers, perform these tasks:

- Configuring the domain user account on page 40

- Configuring virus checker parameters on page 42
- Installing third-party antivirus software on page 47
- Installing CEE CAVA on page 47
- Starting the CEE AV engine on page 48

Configuring the domain user account

The CEE CAVA installation requires a Windows user account that the Unity NAS servers recognize as having the Unity virus-checking privilege. This user account lets the NAS servers distinguish CEE CAVA requests from all other client requests.

To configure the domain user account, perform these tasks:

1. Creating the domain user account on page 40
2. Creating the antivirus local groups on page 40
3. Configuring virus check rights on each NAS server on page 41

Creating the domain user account

To create an Active Directory domain user account for the antivirus user:

Procedure

1. Log in to a Windows Server version 2008 SP2 through 2016 as the Domain Administrator.
2. From the Control Panel select **Administrative Tools** > **Active Directory Users and Computers**.
3. In the console tree, right-click **Users**, and then select **New** > **User**.
4. In the **New Object - User** dialog box, specify the first name, last name, and user logon name for the new user, and click then **Next**.
5. In the **Password** dialog box:
   a. Enter and confirm a password.
   b. Select **Password never expires**.
   c. Click **Next**, and then click **Finish**.

Creating the antivirus local groups

Create a local group for each NAS server in the domain, and add the new antivirus user that you created in the previous section.

Note

If you did not add the antivirus user to Domain Admins, add the antivirus user to each AV server's local Administrators group.

Procedure

1. In **Active Directory Users and Computers**, double-click **EMC NAS Servers**, and click **Computers**.
2. In the **Computer** pane, right-click the NAS server, and select **Manage**.
3. In the **Computer Management** window, under **System Tools**, double-click **Local Users and Groups**.
4. Right-click **Groups** and select **New Group**.

5. In the **New Group** dialog box, enter a group name (for example, viruscheckers) and a description of the group, and click **Add.**
6. In the **Select Users, Computers, Service Accounts, or Groups** dialog box:
   a. Enter the name of the AV user account that you created in the previous section.
   b. Click **Check Names**.
   c. Click **OK** to close the **Select Users, Computers, or Groups** dialog box, and then click **OK** to return to the **New Group** dialog box.
7. Click **Create**, and then click **Close.**

   The group is created and added to the Groups list.

Configuring virus check rights on each NAS server

Assign the Unity virus-checking rights to the new local group.

Note

You cannot use Microsoft Windows Local Policy Setting tools manage user rights assignments on a Unity file system because these tools do not let you to manage user rights assignments remotely.

Procedure

1. From the Control Panel, select **Administrative Tools** > **EMC Unity VNX VNXe NAS Management**.
2. If the NAS server is already selected (name appears after **Data Mover/NAS Server Management**), go to step 4.
3. If the NAS server is not selected:
   a. Right-click **Data Mover/NAS Server Management**, and then select **Connect to Data Mover/NAS Server**.
   b. In the **Select Data Mover/NAS Server** dialog box, select the NAS server either by selecting the domain in the **Look in**: list box and then selecting the NAS server from the list or by entering the computer name, IP address or NetBIOS name of the NAS server in the **Name** field.
4. Double-click **Data Mover/NAS Server Management**, and then double-click **Data Mover/NAS Server Security Settings**.
5. Click **User Rights Assignment**, and in the right pane, double-click **EMC Virus Checking**.
6. In the **Security Policy Setting** dialog box, click **Add.**
7. In the **Select Users or Groups** window:
   a. Select the NAS server from the **Look in:** field.
   b. Select the antivirus group that you created in Creating the antivirus local groups on page 40.
   c. Click **Add**, and then click **OK** to return to the **Security Policy Settings** dialog box.
8. Click **OK**.

   The Virus Checking policy now shows the file systems local group. Although this right is a local privilege and not a domain privilege, it still distinguishes antivirus users from other domain users.

9. Assign local administrative rights to the antivirus user account on each host that will run antivirus engine software, that is, that will be an AV server.

   Note

   If the AV server is a domain controller, the virus-checking user account should join the domain administrator group instead of the local administrator group, because the local administrator group is not managed on a domain controller.

   For each AV server in the domain:

   a. From the Control panel, select **Administrative Tools** > **Computer Management**.

   b. In the **Action** menu of the **Computer Management** window, select **Connect to Another Computer**.

   a. In the **Select computer** window, select the virus-checker (AV) server, and then click **OK**.

   b. In the **Computer Management** window:

      a. Expand **System Tools**.

      b. Expand **Local Users and Groups**.

      c. Click **Groups**.

   c. Right-click the **Adminstrators** group, add the domain antivirus user account, and then select **Properties**.

   d. In the **Account Properties** window, click the **Members of** tab, and click **Add**.

   e. In the **Select Groups** dialog box, in the **Enter the object names to select** box, enter **Administrators**, and click **OK**.

   f. Click **OK** to close the **Account Properties** dialog box.

Configuring virus checker parameters

This topic lists the steps to configure virus checker parameters.

Procedure

1. From the Control Panel, select **Administrative Tools** > **EMC Unity VNX VNXe NAS Management**.
2. In the console tree, expand the Data Mover/NAS Server Management node (for a Unity system, the entries represent the NAS servers).

   The AntiVirus node appears in the console tree. The status of the AntiVirus service for the selected NAS server is either Stopped or Running.

   Note

   If you did not select a NAS server, you must select one before you can use the AntiVirus Management snap-in. If a NAS server is selected, its name appears next to the Data Mover/NAS Server Management node in the console tree.

3. Click the AntiVirus node.

   The list of parameter settings appears in the details pane.

4. In the details pane:
   a. Right-click the parameter that you want to change, and then select **Properties.**

      The **Properties** dialog box for that parameter appears. For a description of the parameters, refer to Configurable AntiVirus node parameters on page 43.

   b. If the parameter contains multiple settings, enter the values for the settings, click **Add**, and then click **OK**.

   c. If the parameter contains a single setting, enter the value for the setting, and then click **OK**.

Configurable AntiVirus node parameters

For Unity systems, you can either create an antivirus configuration file in Unisphere, or you can upload an antivirus configuration file that you create offline. To access the antivirus configuration in Unisphere:

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

The following table describes the parameters you can configure in the `viruschecker.conf` file or use with the EMC Unity/VNX/VNXe NAS Management snap-in.

Note

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 7 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:

Table 7 Parameters in the viruschecker.conf file (continued)

Parameter	Description	Example
		`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 CAVA service.
`CIFSserver=<CIFS_server_name>` (optional)	Identifies the interface on the NAS server used by the CAVA Client `<CIFS_server_name>` (NetBIOS name, compname, or the IP address) of the SMB/CIFS server on the NAS server. If the parameter is not given, the 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.	`CIFSserver=CIFS_Host2`
`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.	`maxsize=0xFFFFFFFF`

Table 7 Parameters in the viruschecker.conf file (continued)

Parameter	Description	Example
	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.	
`highWaterMark=<n>` (optional)	Edits the highWaterMark parameter. When the number of requests in progress becomes greater than the highWaterMark, 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 lowWaterMark, a log event is sent to 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`
`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 NAS server retries until RPCRequestTimeout is reached. If RPCRequestTimeout is reached, the NAS server goes to the next available AV machine. The default value is 25000 milliseconds.	`RPCRequestTimeout=20000 milliseconds`

Table 7 Parameters in the viruschecker.conf file (continued)

Parameter	Description	Example
	Note This value should be greater than the Symantec Protection Engine Container File Processing Limits value.	

`msrpcuser=` (optional)	Specifies the name assigned to either a simple user account or user account that is part of a domain that the 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 Unity share.) If strict data security is important in the environment, you should enable 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=cifs`
	• `shutdown=no` — Continues retrying list of AV machines if no AV machine is available. Two watermarks exist (low and high).	`shutdown=no`

Table 7 Parameters in the viruschecker.conf file (continued)

Parameter	Description	Example
	When each is reached, an Event log is sent. Use the Event log to take corrective action on the 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 Unity shares without virus checking.) The default is shutdown=no.	`shutdown=viruschecking`

Installing third-party antivirus software

You must install a supported third-party antivirus software package (AV engine) on each host in the domain that will be an AV server. To ensure that file scanning is maintained if an AV server goes offline or cannot be reached by the Unity NAS server, you must configure at least two AV servers in the domain. For the latest list of supported AV engines and versions, refer to the E-Lab™ Interoperability Navigator on the support website.

You must install any supported third-party antivirus software package, except for the Trend MicroServerProtect package, on a host before installing CEE CAVA on a host. If you want to install Trend MicroServerProtect antivirus software on a host, install CEE CAVA first as described in Installing CEE CAVA on page 47.

For more information about installing third-party antivirus software, see *Using the Common Event Enabler on Windows Platforms*.

Installing CEE CAVA

This topic provides important information that you should know before installing CAVA.

You must install CEE CAVA on each host in the domain that will be an AV server. For installation instructions, refer to *Using the Common Event Enabler on Windows Platforms* on Online Support. While running the installation wizard, if you want to install only CAVA instead of the full CEE software, at the Setup Type step, choose **Custom**, select **CAVA**, and click **Next**.

After you install CEE CAVA, open `Services.msc` on each AV server, change the CAVA service to Log On, and run the service using the domain antivirus account.

Removing old versions of CEE CAVA

If an AV server has a previous version of CEE CAVA installed, remove that version of CEE CAVA, reboot the server, and then install the new version of CEE CAVA. Use the Windows Control Panel's **Add/Remove Programs** window to remove old versions of CEE CAVA. You must have local administrative privileges to remove programs.

Note

If you do not remove the previous version of CEE CAVA before upgrading, you can choose the Remove option on the initial installation page to first remove the previous version, then continue with the installation.

Reinstallation of CEE CAVA

During a reinstallation of CEE CAVA, you may see an overwrite protection message if the installation files were previously unpacked to the temporary directory. If you see this message, from the **Overwrite Protection message** window, click **Yes to All** to overwrite the existing files. This process ensures that the latest version of the files exist in the temporary directory.

Starting the CEE AV engine

This topic lists the steps to start the CEE AV engine (virus-checking agent) in Unisphere.

Procedure

1. Access Unisphere.
2. Under **Storage**, select **File** > **NAS Servers**.
3. Select the relevant NAS server, and then select the **Edit** icon.
4. In the **Security** tab, select the **Antivirus** sub-tab.
5. Select **Enable antivirus service**.
6. Select **Retrieve Current Configuration** to obtain the current CAVA configuration file. Then save it locally as `cava.conf`. The first time you retrieve this file, it is an empty template with comments next to each field.
7. Edit the `cava.conf` file as appropriate. The first time you edit this file, remove the comments and specify the CAVA parameters (such as the list of servers running CAVA) in this file.
8. Select **Upload New Configuration** and upload the new configuration to the NAS server.

Results

The Antivirus status changes to `Antivirus is running`.

Note

If the `shutdown` antivirus node parameter is set to `no`, the status "running" does not necessarily mean that the antivirus is working. Check **Events** > **Alerts** to verify that the antivirus servers are online. To avoid issues with client access, ensure that all the antivirus servers are accessible and there are no issues with the configuration. For more information on the `shutdown` antivirus node parameter or other related parameters, refer to Configurable AntiVirus node parameters on page 43.

CHAPTER 5

Using CEE Events Publishing with Unity

This chapter contains the following topics:

Events Publishing overview

The Common Event Enabler (CEE) provides an events publishing solution (Common Event Publishing Agent) for Unity clients that allows third-party applications to register to receive event notification and context from the storage system when accessing file systems. The Events Publishing agent (CEPA) delivers to the application both event notification and associated context in one message. Context can consist of file metadata or directory metadata that is needed to decide business policy. To use the Events Publishing agent, you must have a Unity system with at least one NAS server configured on the network.

You must define at least one event option (pre-, post-, or post-error event) when Events Publishing is enabled:

- Pre-event notifications are sent before processing an SMB client request.
- Post-event notifications are sent after a successful SMB client request.
- Post-error event notifications are sent after a failed SMB client request.

Table 8 Event descriptions

Value	Definition
`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).
`OpenFileRead`	Sends a notification when a file is opened for read access.
`OpenFileReadOffline`	Sends a notification when an offline file is opened for read access.
`OpenFileWrite`	Sends a notification when a file is opened for write access.
`OpenFileWriteOffline`	Sends a notification when an offline file is opened for write access.
`OpenDir`	Sends a notification when a directory is opened.
`CreateFile`	Sends a notification when a file is created.
`CreateDir`	Sends a notification when a directory is created.
`DeleteFile`	Sends a notification when a file is deleted.
`DeleteDir`	Sends a notification when a directory is deleted.
`CloseModified`	Sends a notification when a file is changed before closing.
`CloseUnmodified`	Sends a notification when a file is not changed before closing.
`CloseDir`	Sends a notification when a directory is closed.
`RenameFile`	Sends a notification when a file is renamed.
`RenameDir`	Sends a notification when a directory is renamed.
`SetAclFile`	Sends a notification when the security descriptor (ACL) on a file is changed.
`SetAclDir`	Sends a notification when the security descriptor (ACL) on a directory is changed.

Events publishing restrictions and limitations

Before you begin

Before you can set up Events Publishing for a NAS server:

- You cannot enable Events Publishing for a NAS server that is acting as a replication destination.
- At least one file system must exist for the NAS server.
- You must obtain the IP addresses of the CEPA servers.
- Ensure that events notifications for the SMB protocol is enabled on the **File Systems Properties Advanced** window.

CEPA pools
In 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.

CEPA servers
Each NAS Server should specify a CEPA pool consisting of a minimum of two CEPA servers.

Installing CEE CEPA

For installation instructions, refer to *Using the Common Event Enabler on Windows Platforms* on Online Support. While running the installation wizard, if you want to install only CEPA instead of the full CEE software, at the Setup Type step, choose **Custom**, select **CEPA**, and click **Next**.

Setting Up Events Publishing

You can use the Unisphere GUI to set up Events Publishing per NAS server.

- You cannot enable Events Publishing for a NAS server that is acting as a replication destination.
- At least one file system must exist for the NAS server.
- You must obtain the IP addresses of the CEPA servers.

Procedure

1. Under **Storage**, select **File** > **NAS Servers**.
2. Select the relevant NAS Server, and then select the **Edit** icon.
3. On the **Protection & Events** tab, select the **Events Publishing** sub-tab.
4. Select the **Enable Common Event Publishing** checkbox.
5. On the **New Event Pool** window, specify the required items. You must configure at least one event from one of the available categories (pre-event, post-event, or post-error event).
6. Click **Configure**.
7. Optionally, select **Show policy settings** to configure pre-events and post-events failure policies.
8. Optionally, select **Show advanced settings** to configure CEPA server options.
9. Click **Apply** after you finish configuring events.

After you finish

Once you set up Events Publishing for a NAS server, you can optionally enable it for each associated file system. To do this, select **Enable SMB Events publishing** on the **Advanced** tab of the file system properties page.