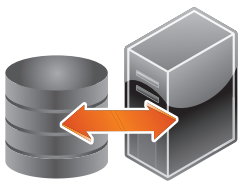
EMC® VNXe™ Series

Using a VNXe System with CIFS Shared Folders

VNXe Operating Environment Version 2.4

P/N 300-010-548
REV 04



Connect to Storage

EMC²

Published January, 2013

Chapter 4 Using File-Level Retention with the VNXe System

Chapter 5 Using the VNX Event Enabler Common Solution with the VNXe System

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. 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 EMC representative if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. New versions of this document might be released on the EMC online support website. Check the EMC online support website to ensure that you are using the latest version of this document.

Purpose

This document is part of the EMC VNXe documentation set. It describes how to set up Windows hosts with clients that need to access network file system (CIFS) Shared Folder storage on a VNXe system with VNXe Operating Environment version 1.7.0 or later.

Audience

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

Readers of this document a should be familiar with VNXe CIFS Shared Folder storage and the Windows operating system running on hosts with clients that will access VNXe CIFS Shared Folder storage.

Related documentation

Other VNXe documents include:

- *EMC VNXe3100 Hardware Information Guide*
- *EMC VNXe3100 System Installation Guide*
- *EMC VNXe3150 Hardware Information Guide*
- *EMC VNXe310 Installation Guide*
- *EMC VNXe3300 Hardware Information Guide*
- *EMC VNXe3300 System Installation Guide*
- *Using the VNXe System with NFS Shared Folders*
- *Using the VNXe System with Microsoft Exchange 2007 or Microsoft Exchange 2010*
- *Using the VNXe System with Generic iSCSI Storage*
- *Using the Using the VNXe System with Microsoft Windows Hyper-V*
- *Using the VNXe System with VMware NFS or VMware VMFS*
- *VNXe CLI User Guide*

EMC Unisphere help provides specific information about the VNXe storage, features, and functionality. The Unisphere help and a complete set of VNXe customer documentation are located on the EMC Online Support website (http://www.emc.com/vnxesupport).

Conventions used in this document

EMC uses the following conventions for special notices:

⚠DANGER

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

⚠WARNING

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

⚠CAUTION

CAUTION, used with the safety alert symbol, indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to personal injury.

Note: A note presents information that is important, but not hazard-related.

IMPORTANT

An important notice contains information essential to software or hardware operation.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities • URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, and notifications
Bold	Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages Used in procedures for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • What the user specifically selects, clicks, presses, or types

Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis, for example, a new term • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, filenames, prompts, and syntax when shown outside of running text
`Courier bold`	Used for specific user input, such as commands
`Courier italic`	Used in procedures for: • Variables on the command line • User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

You can find VNXe support, product, and licensing information as follows:

Product information — For documentation, release notes, software updates, or information about EMC products, licensing, and service, go to the EMC online support website (registration required) at:

`http://www.emc.com/vnxesupport`

Technical support — For technical support, go to EMC online support. Under Service Center, you will see several options, including one to create a service request. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

`techpubcomments@emc.com`

CHAPTER 1
Setting Up a Host to Use VNXe CIFS Shared Folder Storage

This chapter describes how to set up a Windows host or virtual machine to use EMC VNXe CIFS Shared Folder storage.

Topics include:

Requirements for setting up a host to use VNXe CIFS storage

Before you can set up a host to use VNXe CIFS storage, the following VNXe system and network requirements described in this section must be met.

VNXe system requirements

- You have installed and configured the VNXe system using the VNXe Configuration Wizard, as described in the *EMC VNXe3100 System Installation Guide*, the *EMC VNXe3150 Installation Guide*, or the *EMC VNXe3300 System Installation Guide*.
- You have used Unisphere or the VNXe CLI to perform basic configuration of one or more VNXe Shared Folder Servers on the VNXe system.

Network requirements

The host (client) must be in a LAN environment with the VNXe Shared Folder Storage Server. The VNXe Shared Folder Server can be either a member of a Windows Active Directory domain or operate independently of any Windows domain as a stand-alone CIFS server.

VNXe CIFS Shared Folder Server in a Windows Active Directory domain

A CIFS Shared Folder 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 a CIFS Shared Folder Server with a Windows domain allows any users in the domain to connect to the CIFS server. In addition, authentication and authorization settings maintained on the Active Directory server apply to the files and folders on the CIFS Shared Folder.

A CIFS Shared Folder Server with Active Directory enabled requires a Windows domain with an Active Directory (AD) server and a DNS server.

Stand-alone VNXe CIFS Shared Folder Server

A stand-alone CIFS Shared Folder 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 CIFS Shared Folder Server can access the server, and the CIFS server performs user authentication.

A stand-alone CIFS Shared Folder Server requires a Windows workgroup.

Celerra host software for VNXe hosts in a CIFS environment

This section describes the EMC Celerra® host software that is available for VNXe system in a CIFS environment and tells how to install this software on a host that will use VNXe CIFS

Shared Folder storage.

Overview of software for VNXe hosts in a CIFS environment

The EMC Celerra® host software that is available for a VNXe system in a CIFS environment is:

- VNX Event Enabler (VEE) Common AntiVirus Agent
- Management snap-ins

VNX Event Enabler Common AntiVirus Agent

The VNX Event Enabler (VEE) Common AntiVirus Agent (CAVA) provides an antivirus solution for CIFS clients using EMC 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 VNX Event Enabler (VEE) software package. The VNXe support matrix on the EMC Online Support website (http://www.emc.com/vnxesupport) provides information about the third-party antivirus software that CAVA supports.

Management snap-ins

A VNXe Shared Folder Server supports the Celerra Management snap-ins, 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 Shared Folder Server from a Windows Server 2003, Windows Server 2008, or Windows 8 computer:

- Celerra Home Directory Management snap-in
- Celerra Data Mover Security Settings snap-in
- Celerra AntiVirus Management snap-in

Celerra Home Directory Management snap-in

You can use the Celerra 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.

Celerra Data Mover Security Settings snap-in

The Celerra Data Mover Security Settings snap-in consists of the Audit Policy node and the User Rights Assignment node.

Celerra Audit Policy node

You can use the Celerra Audit Policy node to determine which Shared Folder 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 Shared Folder Server. You cannot use the Audit Policy node to manage GPO audit policies.

Celerra User Rights Assignment node

You can use the Celerra User Rights Assignment node to manage which users and groups have login and task privileges to a Shared Folder 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 Shared Folder Server. You cannot use the User Rights Assignment node to manage GPO policies.

Celerra AntiVirus Management snap-in

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

Installing host software for a CIFS environment

Table 1 lists the host software in a VNXe CIFS environment, describes why you would install it, and lists the hosts on which you would install it.

Table 1 Host software for VNXe CIFS environments

Software	Install software if you want to	Install on
Celerra Home Directory Management snap-in	Manage user home directories.	The Windows Server 2003, Windows Server 2008, or Windows 8 system from which you will manage the VNXe Shared Folder Servers in the domain.
Celerra Data Mover Security Settings snap-in	Audit Shared Folder Server security events in the security log and manage user and group access and task privileges for a Shared Folder Server.	The Windows Server 2003, Windows Server 2008, or Window 8 system from which you will manage the VNXe Shared Folder Servers in the domain.
VEE AntiVirus Management snap-in	Manage virus checking parameters used in conjunction with CAVA and third-party antivirus programs.	The 32-bit Windows Server 2003, Windows Server 2008, or Windows 8 host (client) that uses VNXe storage. Requires one or more Windows hosts that are AntiVirus (AV) servers. These AV servers can also be hosts that use VNXe storage.

To install the host software for a CIFS environment on a VNXe host:

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 on the EMC Online Support website (http://www.emc.com/vnxesupport).
   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, 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 (CA)

Windows 8/SMB3 environments provide the ability to add high-availability functionality to CIFS resources. Windows CA allows applications running on hosts connected to shares with this property to support transparent server failover.

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.

With CA enabled, you can achieve a transparent server failover for implementations where the failover time is no longer than the application timeout. In such implementations, hosts can continue to access a CIFS resource without the loss of a CIFS session state, following a failover event

.Using network high availability

The VNXe system provides network high-availability or redundancy with Fail-Safe Networks (FSNs) that extend link failover out into the network by providing switch-level redundancy. On a VNXe system, each port on a storage processor (SP) is configured in an FSN with the corresponding port on the peer SP. When you assign a port to a VNXe Shared Folder Server interface, the VNXe automatically designates that port on the SP where the Shared Folder Server resides as the primary port in the FSN and the port on the peer SP as the secondary port in the FSN. You cannot create, delete, or change the configuration of the VNXe FSNs. For these reasons, to take advantage of FSN in a VNXe3100 system with two SPs, a VNXe3150 with two SPs, or a VNXe3300 system, the Ethernet (eth) ports on each SP must be cabled identically. For example if you cable eth2 and eth4 ports on SP A and create a separate storage server on each port, you must cable eth2 and eth4 ports on SP B the same way.

In addition, the VNXe system supports link aggregations that allows up to four Ethernet ports connected to the same physical or logical switch to be combined into a single logical link. This behavior is called link aggregation. To configure link aggregation on a VNXe system, each storage processor (SP) must have the same type and number of Ethernet ports because configuring link aggregation actually creates two link aggregations — one on each SP. This provides high availability as follows. 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 all the ports in the aggregation fail, FSN fails over to the corresponding link aggregation on the peer SP so that network traffic continues. If you add an Ethernet I/O module to each SP in a VNXe 3100, 3150, or 3300 system, you can create one additional link aggregation group on the set of ports in the I/O module.

The rest of this section describes:

- “Fail-Safe Networks” on page 14
- “Link aggregations” on page 15

- "Configuring a link aggregation" on page 15

For additional information on data availability in your VNXe system and your connectivity infrastructure, refer to the *EMC VNXe High Availability Overview* in the White Papers section of the VNXe support website (http://www.emc.com/vnxesupport).

Fail-Safe Networks

A Fail-Safe Network (FSN) is a high-availability feature that extends links failover into the network by providing switch-level redundancy. An FSN appears as a single link with a single MAC address and potentially multiple IP addresses. On a VNXe system, an FSN consists of one port on one SP and the corresponding port on the other SP. Each port is considered a single connection. Both connections making up the FSN share a single hardware (MAC) address. If the VNXe system detects that the active connection fails, it automatically switches to the standby connection in the FSN, and that connection assumes the network identity of the failed connection.

To ensure host connectivity to the VNXe system in the event of a hardware failover, connect the VNXe system to different switches that are connected to FSN devices on multiple NICs in the host. As a result, the FSN components are connected to different switches. If the switch for the active connection fails, the FSN fails over to a connection using a different switch, thus extending link failover out into the network.

As shown in Figure 1, when the VNXe SP detects loss of the active communications link to the FSN, the connection automatically fails over to an operational standby connection. This action is independent of any switch features. If a connection in the FSN goes down, the link fails over to the surviving link. If both connections in an FSN fail, the link is down.

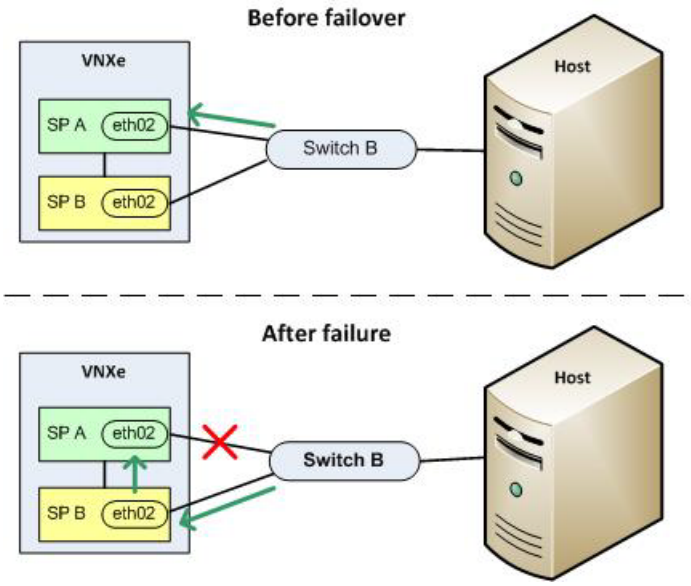


Figure 1 Failover with Fail-Safe Networking

Link aggregations

Link aggregations use the Link Aggregation Control Protocol (LACP) IEEE 802.3ad standard. A link aggregation appears as a single Ethernet link and has the following advantages:

- High availability of network paths to and from the VNXe 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 VNXe system, you can configure up to four ports in a link aggregation. When you configure a link aggregation, you are actually configuring two link aggregations — one on each SP. If one of the ports in a aggregation fails, the system directs network traffic to one of the other ports in the group. If all the ports in the group fail, FSN fails over to the corresponding link aggregation on the peer SP.

Switch requirements

If the VNXe ports are connected to different network switches, you should configure all switch ports connected to the VNXe 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 VNXe port to guarantee that the switch forwards the Ethernet frame that the VNXe 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

Windows 7 and Windows Server 2003 do not provide link aggregation (NIC teaming) support. Some NIC vendors provide drivers that support NIC teaming. For more information, contact your NIC vendor. Windows Server 2008 does support NIC teaming.

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 VNXe port in the aggregation.

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

- "Configuring link aggregation from the switch to the VNXe system" on page 16
- "Configuring link aggregation from the host to the switch" on page 16

Configuring link aggregation from the switch to the VNXe system

1. Configure the switch ports, which are connected to the VNXe, for LACP in active mode, as described in the documentation provided with your switches.
2. Join the VNXe ports into a link aggregation using the Unisphere Advanced Configuration option (**Settings › More configuration › Advanced Configuration**). For information on using the Advanced Configuration option, refer to the Unisphere online help. Two link aggregations are created with the same ports — one aggregation on each SP.

Configuring link aggregation from the host to the switch

To configure link aggregation from the host to the switch, perform these tasks:

- "Task 1: Configure switch ports for link aggregation" on page 16.
- "Task 2: Configure NIC teaming on the Windows Server 2008 or Windows 8 host" on page 16

Task 1: Configure switch ports for link aggregation

Configure the switch ports, which are connected to the host for link aggregation.

Task 2: Configure NIC teaming on the Windows Server 2008 or Windows 8 host

Note: Windows Server 2008 and Windows 8 hosts refers to link aggregation as NIC teaming.

Note: Windows 8 automatically detects NIC teaming on the VNXe, and configures the host to use the same interfaces as the VNXe. Manual configuration is not necessary.

The procedure below is for an Intel network interface driver.

1. In the Control Panel, select **Network and Internet › Network Connections**.
2. In the Network Connections dialog box, right-click one NIC you want in the team and click **Properties**.
3. Click **Configure**.
4. In the Properties dialog box, select the **Teaming** tab.
5. In the **Teaming** tab:
   a. Select **Team this adapter with other adapters**.
   b. Click **New Team**.

   The New Team Wizard opens.
6. 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**.

7. 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.

8. 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 apply, click **OK**.

Using CIFS encryption

Windows 8/SMB3 environments provide the ability to encrypt data stored on VNXe CIFS shared folders as that data moves between the VNXe and the Windows host.

CIFS encryption can also be set at the CIFS server level by modifying the registry settings of the Windows host.

Configuring VNXe CIFS Shared Folder storage for the host (client)

Use Unisphere for the VNXe CLI to create VNXe CIFS Shared Folder storage for the host (client).

For information on performing these tasks refer to the Unisphere online help.

Configuring user access to the CIFS share in the Active Directory

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

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

   The Windows host must have access to the domain with the VNXe Shared Folder Server for the CIFS share.

2. Open the Computer Management window:

   For Windows Server 2003 — Right-click **My Computer** or **Computer** and select **Manage**.

For Windows Server 2008 , Windows 7, or Windows 8— 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 of the VNXe Shared Folder Server to provide the client CIFS shares.
6. In the Computer Management tree, click **System Tools › Shared Folders › Shares**.
7. The available shares appear on the right.

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

Mapping the CIFS share on the host

On the Windows host, use the Windows Map Network Drive function to connect the host to the CIFS share and optionally to reconnect to the share whenever you log in to the host.

You will need the export path for the share (*SharedFolderServer**share*), which you can find in the VNXe configuration report for the shared folder with the share. To access this report, use EMC Unisphere™ software.

1. Select **Storage › Shared Folder Storage**.
2. Select the CIFS shared folder with the share and click **Details**.
3. Click **View Access Details**.

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

CHAPTER 2
Migrating CIFS Data to the VNXe System

You can migrate CIFS data to the VNXe 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:

CIFS migration environment and limitations

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

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

Table 2 outlines the environment required for CIFS data migration, and Table 3 lists the characteristics of a manual copy migration.

Table 2 Environment for CIFS data migration

Component	Requirement
VNXe storage	Shared folder 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 VNXe share for the migrated data
Share	Share that you migrate in its entirety to the VNXe share

Table 3 Characteristics of manual copy migration

Component	Requirement
Permissions	May not be preserved
Downtime	Relative to the time required for: • Copying the share contents to the VNXe share and • Reconfiguring the hosts to connect to the VNXe share

Migrating CIFS data

To migrate CIFS data to a VNXe CIFS share, perform these tasks:

- "Task 1: Set up access to a VNXe share for the CIFS host" on page 20.
- "Task 2: Migrate the CIFS data with a manual copy" on page 21.

Task 1: Set up access to a VNXe share for the CIFS host

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

1. Configure user access to the new share in the Active Directory, as described in "Installing host software for a CIFS environment" on page 12.
2. Map the new CIFS share, as described in"Mapping the CIFS share on the host" on page 18.

Task 2: Migrate the CIFS data with a manual copy

To minimize the time during which a host cannot access a CIFS share being migrated, migrate the data from one share at a time:

1. If any clients are actively using the CIFS 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 VNXe CIFS share.

   This method can be a simple cut and paste or drag and drop operation. Ensure that your chosen method preserves any metadata such as file attributes, timestamps, and access rights that you need preserved.
3. When the copy operation is complete, reconnect the clients to the new CIFS share exported by the VNXe system and map a drive to this share as needed.

CHAPTER 3
Managing VNXe CIFS Shared Folder Storage with Windows Tools

After you have configured the VNXe system for CIFS Shared Folder storage, you can use Unisphere and Windows tools, such as the Celerra MMC snap-ins, to manage the Shared Folder Servers and storage. This chapter describes how to perform some common management tasks using Windows tools. Unisphere online help provides information about performing management tasks with Unisphere.

Note: "Installing host software for a CIFS environment" on page 12 provides information about installing the Celerra CIFS management MMC snap-ins.

This chapter contains the following topics:

Opening Computer Management MMC

You can perform many Windows Server 2003, Windows Server 2008, and Windows 8 administrative tasks from the Computer Management Microsoft Management Console (MMC). Use the procedure below to open the MMC for a specific Shared Folder Server:

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

   The Windows host must have access to the domain with the VNXe Shared Folder Server.

2. Open the Computer Management page:

   For Windows Server 2003 — Right-click **My Computer or Computer** and select **Manage**.

   For Windows Server 2008 and Windows 8 — Click **Start** and select **Administrative Tools › Computer Management**.

3. Right-click **Computer Management (local)**.
4. Select **Connect to another computer**.
5. Enter the name of the VNXe Shared Folder Server, and click **OK**.

Before using the MMC snap-ins

You must be logged in as the Administrator with Administrator rights to use the MMC snap-ins.

Creating shares and setting ACLs with MMC

EMC recommends that you use Unisphere to create CIFS 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 a CIFS shared folder on the VNXe system, you can use the MMC to create shares within that folder.

Before creating shares or setting access (ACLS)

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

- Have assigned global identifiers (GIDs) to CIFS users.
- Have mounted the VNXe share of the root directory of the file system and created the directories you want to share in it.
- Be a VNXe administrator.

Setting ACLs on an existing share on a Shared Folder Server

1. Open the **Computer Management** MMC as described in "Opening Computer Management MMC" on page 24.
2. In the console tree, select **Shared Folders › 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 on a Shared Folder Server

1. Open the **Computer Management** MMC as described in "Opening Computer Management MMC" on page 24.
2. In the console tree, click **Shared Folders** › **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. Provide the following information:
   - Name of the folder to share.
   - Share name for the folder.
   - Share description.
5. Click **Next**.

   The wizard prompts you for share permissions.
6. 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.
7. Click **Finish**.

Using the home directory feature

The Celerra home directory feature, which is provided by the Celerra Home Directory snap-in, lets you create a single share, called HOME, to which all users connect. You do not have to create individual shares for each user.

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.

Note: If a client system (such as Citrix Metaframe or Windows Terminal Server) supports more than one Windows user concurrently and caches file access information, the VNXe home directory feature might not function as desired. With the VNXe home directory capability, a VNXe client sees the same path to the home directory for each user. For example, if a user writes to a file in the home directory, and then another user reads a file in the home directory, the second user's request is completed using the cached data from the first user's home directory. Because the files have the same pathname, the client system assumes they are the same file.

The home directory feature is disabled by default. You must have created a CIFS Shared Folder Server on the VNXe system before you can enable the home directory. On Windows Server 2003, Windows Server 2008, or WIndows 8 systems, you can enable and manage home directories through the Celerra Home Directory snap-in for MMC. The snap-in online help describes the procedures for enabling and managing home directories.

Restrictions when using the home directory

A special share name, HOME, is reserved for the home directory. As a result, the following restrictions apply:

- If you have created a share called HOME, you cannot enable the home directory feature.
- If you have 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:

shared_folder_serve\HOME

where:

shared_folder_server is the IP address, computer name, or NetBIOS name of the VNXe Shared Folder 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.

Adding a home directory to the Active Directory

1. Log in to the Windows server from a domain administrator account.
2. Click **Start** and select **Programs or All Programs › 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:

      shared_folder_serve\HOME

      where:

      shared_folder_server is the IP address, computer name, or NetBIOS name of the VNXe Shared Folder Server.
6. Click **OK.**

Adding a home directory with expressions

1. Log in to the Windows server from a domain administrator account.
2. Click **Start** and select **Programs or All Programs › Administrative Tools › Celerra 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
      – `.*` (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
      – **`[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.**

Examples of expression formats

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

Table 4 Examples of expression formats for adding a home directory

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\<*u*> as their home directory, where *u* is their username.

Using Group Policy objects (GPOs)

In Windows Server 2003, 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 Data Mover Security Settings snap-in, which is installed as a Microsoft Management Console (MMC) snap-in into the Celerra Management Console on a Windows Server 2003, Windows Server 2008, or Windows 8 system.

You can use audit policies to determine which Shared Folder 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 Shared Folder 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 Shared Folder Server and you can be 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.

You cannot use Microsoft's Windows Local Policy Setting tools to manage audit policies on a Shared Folder Server because in Windows Server 2003 and Windows XP, the Windows Local Policy Setting tools do not allow you to manage audit policies remotely.

GPO support on a VNXe Shared Folder Server

A VNXe Shared Folder Server provides support for GPOs by retrieving and storing a copy of the GPO settings for each Shared Folder Server joined to a Windows Server 2003 domain. A VNXe Shared Folder Server stores the GPO settings in its GPO cache.

When the VNXe 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 VNXe Shared Folder Server automatically updates the settings based on the domain's refresh interval.

Supported settings

A VNXe Shared Folder Server currently supports the following GPO Security settings:

Kerberos

- Maximum tolerance for computer clock synchronization (clock skew)

  Time synchronization is done per Shared Folder 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 CIFS users and objects" on page 32 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
- EMC 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 VNXe Shared Folder Servers use this signature to verify the integrity of the packet. The VNXe Shared Folder 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 VNXe Shared Folder 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.

Monitoring Shared Folder Server connections and resource usage with MMC

You can use Windows administrative tools to monitor the following on the VNXe Shared Folder Servers:

- "Monitoring users on a Shared Folder Server" on page 31
- "Monitoring access to shares on the Shared Folder Server" on page 31
- "Monitoring use of files on the Shared Folder Server" on page 31

Monitoring users on a Shared Folder Server

Use this procedure to monitor the number of users connected to a Shared Folder Server:

1. Open the **Computer Management** MMC for the Shared Folder 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 Shared Folder Server appear on the right.

   Optionally:

   - To force disconnections from the Shared Folder 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 Shared Folder Server

Use this procedure to monitor access to shares on the Shared Folder Server:

1. Open the **Computer Management** MMC for the Shared Folder Server as described in "Opening Computer Management MMC" on page 24.
2. In the console tree, click **Shared Folders** › **Shares**.

   The current shares in use appear on the right.

   Optionally, to force disconnections from a share, right-click the share name, and select **Stop Sharing** from the shortcut menu.

Monitoring use of files on the Shared Folder Server

Use this procedure to monitor open files on the Shared Folder Server:

1. Open the **Computer Management** MMC for the Shared Folder Server as described in "Opening Computer Management MMC" on page 24.
2. In the console tree, click **Shared Folders** › **Open Files**.

   The files in use appear on the right.

   Optionally, to close an open file, right-click the file, and select **Close Open File** from the shortcut menu.

To close all open files, right-click the **Open Files** folder, and select **Disconnect All Open Files** from the shortcut menu.

Auditing CIFS users and objects

To audit a Shared Folder Server, use the Celerra Data Mover Security Management Console, which is a Celerra MMC snap-in. "Installing host software for a CIFS environment" on page 12 provides information about installing Celerra 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 Shared Folder Server. After it is enabled, auditing is initiated on the relevant Shared Folder Server. The Celerra Data Mover Security Management snap-in online help provides information about setting audit policies.

If the Group Policy Object (GPO) is configured and enabled on the Shared Folder 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. Only a VNXe advanced administrator can set auditing on a Shared Folder Server.

Table 5 Auditing object classes

Object class	Event	Audited for
Logon/logoff	• CIFS user login • CIFS 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 • 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)	success
	SAM database access (lookup)	success and failure
Process tracking	Not supported	N/A
System restart/shutdown	**Restart:** • CIFS service startup • CIFS service shutdown • Audit log cleared	success

Table 5 Auditing object classes

Object class	Event	Audited for
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.

Table 6 Default log settings

Log type	Maximum file size	Retention
Security	512 KB	10 days

The VNXe Shared Folder Servers support auditing on individual folders and files.

Enabling auditing on a Shared Folder Server

Complete the following steps to enable auditing on a Shared Folder Server:

- "Task 1: Specifying the audit policy" on page 33.
- "Task 2: Setting the audit log parameters" on page 34.

Task 1: Specifying the audit policy

After the Celerra Management Console is installed, use this procedure to access the Security Management snap-in and specify audit policies:

1. Open the **Computer Management** MMC for the Shared Folder Server as described in "Opening Computer Management MMC" on page 24.
2. Click **Start**, and select **Programs** or **All Programs** › **Administrative Tools** › **EMC Celerra Management**.
3. In the **Celerra Management** window, do one of the following:
   - If a Shared Folder Server is selected (a name appears after Data Mover Management), go to step 4.

     or
   - If a Shared Folder Server is not selected:
     a. Right-click **Data Mover Management**, and select **Connect to Data Mover** from the shortcut menu.

b. In the **Select Data Mover** box, select a Shared Folder Server using one of the following methods:

– In the **Look in** list, select the domain where the Shared Folder Server you want to manage is located, and then select the Shared Folder Server from the list.

– In the **Name** field, type the network name or IP address of the Shared Folder Server.

4. Double-click **Data Mover Management**, and double-click **Data Mover 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 Celerra Data Mover Security Management snap-in online help provides more information about audit policy.

Task 2: Setting the audit log parameters

1. Open the **Computer Management** MMC for the Shared Folder Server as described in "Opening Computer Management MMC" on page 24.
2. Double-click **Event Viewer** and, for Windows Server 2008, 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

1. Click **Start**, and select **Programs** or **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. Type the name of the Shared Folder Server in the **Enter the object name to select** field or click **Advanced** to search for a computer, and click **OK** to close the **Select Computer** dialog box.
4. For Windows Server 2008, 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.

Disable auditing

1. Log in to a Windows Server 2003 or Windows Server 2008 domain controller with domain administrator privileges.
2. Click **Start**, and select **Programs** or **All Programs** › **Administrative Tools** › **EMC Celerra Management**.
3. Do one of the following:
   - If a Shared Folder Server is already selected (name appears after Data Mover Management), go to step 4.
   - If a Shared Folder Server is not selected:
     a. Right-click **Data Mover Management**, and select **Connect to Data Mover** from the shortcut menu.
     b. In the **Select Data Mover** dialog box, select a Shared Folder Server using one of the following methods:
        – In the **Look in** list, select the domain in which the Shared Folder Server you want to manage is located, and select the Shared Folder Server from the list.
        – In the **Name** field, type the network name or IP address of the Shared Folder Server.
4. Double-click **Data Mover Management**, and double-click **Data Mover Security Settings**.
5. Right-click **Audit Policy**, and select **Disable Auditing** from the shortcut menu.

Accessing the security log for a VNXe Shared Folder Server

By default, each Shared Folder 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 Shared Folder Server with:

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

where *storage_server_netbios_name* is the NetBIOS name of the Shared Folder Server.

Copying a share snapshot using Windows Explorer

1. Access the Shared Folder Server that has the share that you want to copy by either:
   - Browsing to it in Windows Explorer

     or

   - Using **Start** › **Run** › *shared_folder_server_name.*
2. In the Shared Folder 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 using Windows Explorer

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.

IMPORTANT

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

To restore a share snapshot using Windows Explorer:

1. Access the Shared Folder Server that has the shared folder with the snapshots you want to recover by either
   - Browsing to it in Windows Explorer

     or

   - Using **Start** › **Run** › *shared_folder_server_name.*
2. In the Shared Folder Server, right-click the share with the content that you want to recover and select **Properties.**
3. Click the **Previous Versions** tab.
4. Select the snapshot (previous version) that you want to restore and click **Restore**.

   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 File-Level Retention with the VNXe System

The VNXe Shared Folder Server supports file-level retention (FLR) for Shared Folder storage. FLR allows you to set file-based permissions on a file system to limit write access for a specified retention period. An FLR-enabled file system:

- Safeguards data while ensuring its integrity and accessibility by letting you create a permanent set of files and directories that users cannot alter through CIFS or FTP.
- Simplifies the task of archiving data on standard rewriteable magnetic disks through standard CIFS operations.
- Improves storage management flexibility.

NOTICE

Once you enable FLR for a file system, you cannot disable it. When FLR is enabled, you can get into situations where you may not be able to delete files that you need to delete. Do not enable FLR unless you are certain that you want to use it and you know what you are doing.

Do not use Windows Explorer to lock files in an FLR-enabled file system. Windows Explorer sets the time of the file to the current date and time before making it read-only, which causes the file to be locked forever. If you want to use Windows Explorer to set or manage retention dates or to lock files in an FLR-enabled file system, you must install the FLR tookkit.

This chapter contains the following topics:

FLR terminology and concepts

This section defines terms that are important for understanding file-level retention capabilities on the VNXe Shared Folder Servers.

FLR terminology

CLEAN state

Initial state of a file when it is created. You treat a CLEAN file in the same manner as any file in a file system not enabled for file-level retention. This means that clients and users can rename, modify, and delete a CLEAN file until it is committed to FLR.

EXPIRED state

State of a file when its retention period expires. Clients and users can revert a file in the EXPIRED state back to the FLR state or delete a file in the EXPIRED from the FLR file system.

FLR state

State of a file when its read/write permission is changed to read-only in a file system enabled for file-level retention. Clients and users cannot delete files committed to the FLR state until their retention period expires.

Basic FLR concepts

You can enable file-level retention on a specified file system only at creation time. When you create a new file system with file-level retention enabled, the file system is persistently marked as an FLR file system and clients and users can apply FLR protection on a per-file basis only.

A file in an FLR file system is in one of three possible states: CLEAN, FLR, or EXPIRED. You manage files in the FLR state by setting retention by directory or batch process, which means you manage the file archives on a file system basis, or by running a script to locate and delete files in the EXPIRED state.

You can delete an FLR file system, but you cannot delete or modify files that are in the FLR state. The path to a file in the FLR state is also protected from modification, which means that you cannot rename or delete a directory on an FLR file system unless it is empty.

How file-level retention works

A file in an FLR file system transitions between the three possible states: CLEAN, FLR, or EXPIRED. The transition between these states is based on the file's last access time (LAT) and read-only permission.

When a file is created, it is in the CLEAN state. A CLEAN file is treated exactly like a file in a file system that is not enabled for file-level retention; clients and users can rename, modify, or delete the file.

Note: The file's current state is not visible to the user. Also, access to a file in the CLEAN state causes the file's LAT to change. For example, antivirus scanning, backing up, or searching file contents modifies the LAT on a file.

When you change the permissions on a CLEAN file from read/write to read-only, the file transitions from the CLEAN state to the FLR state, and is committed to FLR. Clients and users cannot modify or delete a file in the FLR state. Also, the path to any file in the FLR state is protected from modification. This means that clients and users of a directory on an FLR file system cannot rename or delete the directory unless it is empty, and they can delete FLR files only after their retention period expires.

A retention period specifies the date and time when a file's FLR protection expires. EMC suggests specifying a retention period before you commit a file to FLR. Otherwise, the system defaults to a infinite retention period. In this case, you can explicitly set a shorter retention period. You can set a file's retention period by modifying the file's last access time through CIFS operations to a future expiration date and time. This future date and time represents the end of the file's retention period.

A file transitions from the FLR state to the EXPIRED state when its reaches its retention period. Only a file’s owner or administrator can delete a file in the EXPIRED state. File-level retention does not perform automatic deletion of files in an EXPIRED state. You must delete EXPIRED files explicitly using the FLR Toolkit.

If necessary, you can revert a file from the EXPIRED state back to the FLR state by extending its retention period to a date beyond the expiration date of the original retention date. To extend a retention period, change the file's LAT to a time beyond the original expiration date. Although you can extend a file's retention period, you cannot shorten it. If you specify a new access time that is before the current access time for the file, the VNXe Shared Folder Server rejects the command. With the exceptions of extending a file's retention period and modifying a user or group's read permissions to the file, you cannot edit the file's metadata during the retention period.

When you copy a read-only file from a regular file system to an FLR file system, the file is not committed to the FLR state. When the copy is complete, the file is in the CLEAN state.

FLR restrictions

The following restrictions apply to FLR:

- You must set the level of file-level retention when you create the file system and you cannot change it after file system creation.
- VNXe clients or users cannot modify or delete Files that are in the FLR state. The path to a file in the locked state is also protected from modification, which means that a directory on an FLR-enable file system cannot be renamed or deleted unless it does not contain any protected files.
- If you are using the EMC Celerra AntiVirus Agent (CAVA), EMC strongly recommends that you update all the virus definition files on all resident antivirus (AV) engines in the CAVA pools, and periodically run a full scan of the file system to detect infected FLR files. When an infected locked file is discovered, the resident AV cannot repair or remove an infected file. Although you can delete the file only after its retention date has passed, you can change the file’s permission bits to restrict read access to make the file unavailable to users. CAVA’s scan-on-first read functionality does not detect a virus in a locked file. The CAVA documentation on the EMC Online Support website (http://www.emc.com/vnxesupport) provides information about CAVA.

- Although file-level retention supports all backup functionality, the FLR attribute is not preserved in a Network Data Management Protocol (NDMP) backup. As a result, when you use NDMP backup, you must make sure that the files are restored to a VNXe file system with file-level retention enabled. If you restore a file from an NDMP backup whose retention date has expired, the file system has an infinite retention date after it is restored. If you want to protect the file, but do not want it to have an infinite retention date, restore the file to a non-FLR file system, and then copy it back into an FLR system.
- The root file system of a nested mount cannot be a file system with file-level retention enabled.

System requirements for file-level retention

This section describes the software, hardware, network, and storage configurations required for using file-level retention with the VNXe Shared Folder Server. Table 7 lists the FLR system requirements.

Table 7 File-level retention system requirements

Component	Requirement
Software	FLR Toolkit, version 3.5 Enterprise (FLR-E).
Hardware	Host running a Windows operating system supported by the FLR Toolkit. The support matrix on the EMC Online Support website (http://www.emc.com/vnxesupport) provides information about the supported operating systems.
Network	No specific network requirements.
Storage	No specific storage requirements.

Windows .NET Framework requirement

The Windows .NET Framework 2.0 must be installed on the host for the FLR Toolkit installation to be successful.

Window services and service account privilege requirements for the FLR Monitor

Table 8 lists the scenarios for the FLR Monitor service account and domain trust relationships. Each scenario describes the required privilege actions that you should perform to ensure that the Monitor can run as a service on the Windows host. In Windows domain trust relationships, the direction of trust is very important. The terms “trusted” and “trusting” and their defined directions in the table are used in the same way that Microsoft describes them.

Table 8 Scenarios and required privilege-granting actions

Is the service account a member of its domain’s Domain Admins group?	Is the host a member of a domain that is trusted by the service account’s domain?	Is the host a member of the same domain as the service account?	Actions required
Yes	Yes	No	Add either the Domain Admins group or the service account to the host’s local administrators group. For example, if the server account is **domain A\someuser**, add either **domainA/Domain Admins** or **domainA\someuser**.
Yes	No	Yes	Add either the Domain Admins group or the service account to the host’s local administrators group. For example, if the server account is **domain A\someuser**, add either **domainA/Domain Admins** or **domainA\someuser**.
Yes	No	No	Add the service account to the server’s local administrators group. The Domain Admins group is not sufficient. For example, if the service account is **domainA\someuser**, add **domainA\someuser**.
No	Yes	Yes	Add the service account to the server’s local administrators group. For example, if the service account is **domainA\someuser**, add **domainA\someuser**.
No	No	No	Add the service account to the server’s local administrators group. The Domain Admins group is not sufficient. For example, if the service account is **domainA\someuser**, add **domainA\someuser**.

Installing the FLR Toolkit on a host

You can install the FLR Toolkit on any Windows host that is running in the network that has access to the VNXe Shared Folder Server with the files that you want to retain:

1. Log in to the Windows 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 on the EMC Online Support website (http://www.emc.com/vnxesupport).
   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 **Welcome** page, click **Next**.

5. Read the License Agreement and accept the terms of License agreement by clicking **Next**.
6. Enter the username and organization, and click **Next**.
7. Specify the destination folder for the installation of the FLR Toolkit, and click **Next**.
8. On the **Setup type** page, select **Complete** or **Custom** as the setup type, and click **Next**.
9. In the Logon information page, specify and/or browse for the domain credentials for the user logon account that will log on to the FLR Toolkit, and click **Next**.

   These credentials are:

   - Username, which should be *domain*/Administrator, where *domain* is the domain name
   - Password for *domain*/Administrator
10. Review the installation settings and if they are correct, click **Install**.
11. Click **Finish** to complete the installation.

Configuring the FLR monitor

1. Open the FLR monitor service, which is included with the FLR Toolkit.
2. On the **FLR Connections** tab, click **Add.**
3. On the **Directory Options** tab in the **Retention Source Configuration** page, click **Browse** to select the retention source.
4. Select the CIFS share that was created over the FLR file system as the retention source.
5. In the **Retention Source Configuration** page:
   a. Select the option to monitor subdirectories and click **OK**.
   b. On the **Monitoring Options** tab, select the monitoring method:

      Fast (event based) — The retention policy is applied as soon as the archive files are generated.

      Polling (schedule-based) — The retention policy is applied according to a particular schedule.

   c. On the **FLR options** tab, set retention to the required retention policy, and click **OK**.

      Note: The incremental date and time policy applies the retention so that the retention date is applied incrementally for the archive files generated at different points of time.
6. In the **FLR monitor service** page, on the **FLR Connections** tab, select the connection entry and click **Apply**.
7. In the **Confirmation** page, click **Yes** to confirm the application of the retention policy, and click **OK**.

Using the FLR monitor

This section describes how to:

- "Commit a read-only file to the FLR state" on page 45.
- "Create FLR queries" on page 45.

Commit a read-only file to the FLR state

After copying a file to a CIFS file system enabled for file-level retention, you must:

1. Change permission on the file to read/write.
2. Set a retention period.
3. Commit the file to the FLR state.

Additionally, file systems with file-level retention enabled always enforce synchronization of the DOS (CIFS) read-only bit.

Create FLR queries

After the FLR monitor service is started, you can use the FLR Explorer tool, which is automatically installed with the FLR ToolKit, to create queries for viewing retained or expired files. You can execute queries on the retention source with the build a query feature of FLR Explorer. You can provide the following parameters for the query:

- Type of files — Retained files, files in a non-WORM state, files in specific retention state
- Retention source
- Extension of files to include or exclude
- Subdirectories also in the search path

Sample query

The following steps describe the process of executing the FLR query with the FLR Explorer:

1. Open the FLR Explorer application from:

   C:\Program Files (x86)\EMC\FLR Toolkit\FLR Explorer
2. In the FLR Explorer, select **Build a Query**.
3. In the **Query Builder** page, provide the type of file to search for, such as retained files, files in specific retention state, or files in non-WORM state.
4. Provide the retention source.
5. Optionally include or exclude files by specifying their extensions.
6. Click **OK.**

A list of expired files from the FLR Explorer is displayed. Similarly you can display the list of retained files by building another query using the FLR explorer.

CHAPTER 5
Using the VNX Event Enabler Common Solution with the VNXe System

The VNX Event Enabler (VEE) provides an antivirus solution (VEE Common Anti-Virus Agent) for clients using the VNXe system. It uses industry-standard Common Internet File System (CIFS) protocols in a Windows 8, Windows 7, Windows Server 2008, Windows Server 2003, or Windows 2000 domain. The VEE Common Anti-Virus Agent (VEE CAVA) uses third-party antivirus software to identify and eliminate known viruses before they infect files on the VNXe system. Although the VNXe Storage Servers (Data Movers) 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.

This chapter contains the following topics:

CAVA overview

As shown in Figure 2, the VEE solution uses the following components:

- VNXe Shared Folder Server running the VEE CAVA virus-checking client
- Third-party antivirus (AV) engine
- VEE CAVA software

A third-party AV engine and the VEE CAVA software must be installed on at least one Windows Server 2008, Windows Server 2003, or Windows 2000 server or one Windows 7 or Windows 8 workstation in the domain with the VNXe system. Such a server is an AV server.

Note: If the third-party AV software runs on a Windows 7 or Windows 8 workstation, VEE CAVA can also run on the Windows 7 workstation.

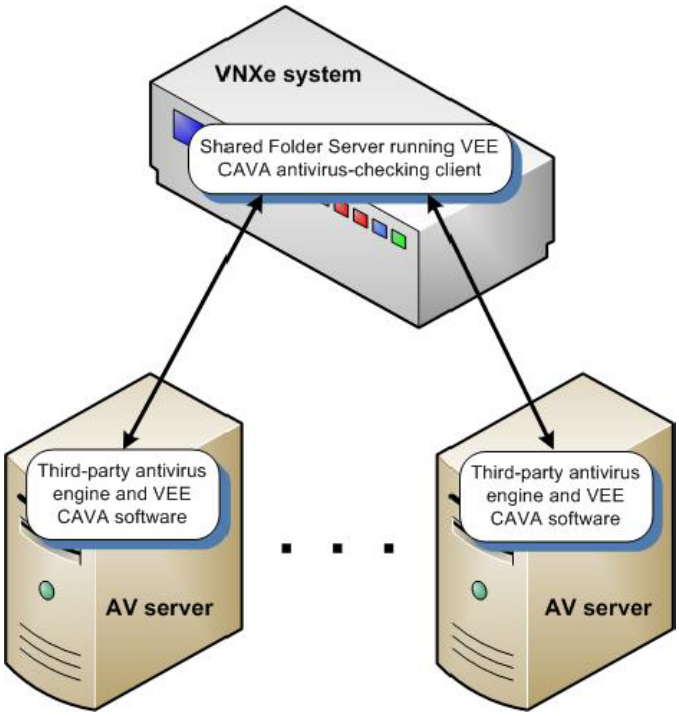


Figure 2 CAVA solution components

VNXe Shared Folder Servers

The VNXe Shared Folder Servers manage operations for Windows shared folders and shares (CIFS), Linux/UNIX shared folders and shares (NFS), or both. For a VEE CAVA solution, the VNXe system requires one or more Shared Folder Servers configured for CIFS shares or for both CIFS and NFS shares.

VEE CAVA virus-checking client

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

The VC client does the following:

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

Third-party antivirus software support

The VEE CAVA solution uses third-party antivirus software, called an AV engine, to identify and eliminate known viruses before they infect files on the VNXe system. For the AV engines that EMC supports, refer to the VNXe support matrix on the EMC Online Support website (http://www.emc.com/vnxesupport).

VEE CAVA software

The VEE CAVA software is an application developed by EMC 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 CIFS files stored on a VNXe or VNX system or Celerra Network Server.

Celerra MMC snap-in AntiVirus Management software

Celerra AntiVirus Management software is an MMC snap-in to Unisphere. Use this snap-in to view or modify the VEE virus-checking parameters for the VNXe Shared Folder Servers.

System requirements and limitations

The VEE CAVA solution requires the following:

- A VNXe system with a Shared Folder Server configured on the network.
- Celerra MMC AntiVirus Management snap-in software installed on a client system that has access to the VNXe domain. For information about installing this snap-in, see "Installing host software for a CIFS environment" on page 12.
- Third-party antivirus software running on one or more AV servers in the domain. VEE 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.
- VEE CAVA software installed on each AV server in the domain.

File-level retention

We strongly recommend that the antivirus (AV) administrator update the virus definition files on all resident AV engines in the VEE CAVA pools, and periodically run a full scan of the file system to detect infected file-level retention (FLR) files.

Non-CIFS protocols

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

Setting up VEE CAVA for VNXe Shared Folder Servers

To implement a VEE CAVA solution for VNXe Shared Folder Servers, perform these tasks:

- "Task 1: Configure the domain user account with virus-checking rights" on page 50.
- "Task 2: Configure virus checker parameters for the Shared Folder Server" on page 53.
- "Task 3: Install third-party antivirus software on the AV servers in the domain" on page 55.
- "Task 4: Install VEE CAVA on the Windows AV servers" on page 55.
- "Task 5: Start the VEE AV engine (virus-checking agent) on the VNXe system" on page 56.

Task 1: Configure the domain user account with virus-checking rights

The VEE CAVA installation requires a Windows user account that the VNXe Shared Folder Servers recognize as having the EMC virus-checking privilege. This user account lets the Shared Folder Servers distinguish VEE CAVA requests from all other client requests.

To configure the domain user account:

1. Create an Active Directory domain user account for the antivirus user:
   a. Log in to the Windows Server 2008, Windows Server 2003, or Windows 2000 server as the Domain Administrator.
   b. From the taskbar, click **Start** and select **Settings › Control Panel › Administrative Tools › Active Directory Users and Computers**.
   c. In the VNX Management Console tree, right-click **Users**, and select **New › User.**
   d. In the **New Object - User** dialog box, specify the first name, last name, and user logon name for the new user, and click **Next**.

      You can give the domain user any name you want, although it should be meaningful name.

e. In the **Password** dialog box:

- Enter and confirm a password.
- Select **Password never expires**.
- Click **Next**.
- Click **Finish**.

The VEE CAVA service will run in the context of this account.

2. Create a local group for each Shared Folder Server in the domain, and add the new antivirus user (virususer), which you created in "Task 1: Configure the domain user account with virus-checking rights" on page 50, to the group:

a. In **Active Directory Users and Computers**, double-click **EMC Celerra**, and click **Computers**.

b. In the **Computer** pane, right-click the Shared Folder Server, and select **Manage**.

c. In the **Computer Management** window, under **System Tools**, double-click **Local Users and Groups**.

d. Right-click **Groups** and select **New Group**.

e. In the **New Group** dialog box, enter a group name (for example, viruscheckers) and a description of the group, and click **Add**.

f. In the **Select Users, Computers, or Groups** dialog box:

For Windows 8, Windows 7, Windows Server 2008 or Windows Server 2003:

- Enter the name of the AV user account that you created in "Task 1: Configure the domain user account with virus-checking rights" on page 50.
- Click **Check Names**.
- Click **OK** to close the **Select Users, Computers, or Groups** dialog box, and then click **OK** to return to the **New Group** dialog box.

For Windows 2000:

- Select the domain from the **Look in:** list box.
- Select the name of the AV user account that you created in "Task 1: Configure the domain user account with virus-checking rights" on page 50 from the list.
- Click **Add**.
- Click **OK** to return to the **New Group** dialog box.

g. Click **Create**, and click **Close**.

The group is created and added to the Groups list.

3. Assign the EMC virus-checking rights to the new local group:

Note: You cannot use Microsoft Windows Local Policy Setting tools manage user rights assignments on a VNXe Shared Folder because these tools do not let you to manage user rights assignments remotely.

---

a. Click **Start** and select **Settings > Control Panel > Administrative Tools > Celerra Management**.

b. If the VNXe Shared Folder Server is already selected (name appears after Data Mover Management), go to Step e.

c. If the VNXe Shared Folder Server is not selected:

- In the VNX Management window, right-click **Data Mover Management** and select **Connect to Data Mover.**
- In the **Select Data Mover** dialog box, select the VNXe Shared Folder Server either by selecting the domain in the **Look in:** list box and then selecting the Shared Folder Server from the list or by entering the computer name, IP address or NetBIOS name of the VNXe Shared Folder Server in the **Name** box.

d. Double-click **Data Mover Management**, and double-click **Data Mover Security Settings**.

e. Click **User Rights Assignment**, and in the right pane, double-click **EMC Virus Checking**.

f. In the **Security Policy Setting** dialog box, click **Add**.

g. In the **Select Users or Groups** window:

- Select the Shared Folder Server from the **Look in:** list box.
- Select the antivirus group that you created in Step 2.
- Click **Add**, and then click **OK** to return to the **Security Settings** dialog box.

h. Click **OK**.

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

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

Note: If the AntiVirus 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. Click **Start** and select **Settings > Control Panel > Administration Tools > Computer Management**.

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

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

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

- Expand **System Tools**.
- Expand **Local Users and Groups**.
- Click **Users**.

e. Right-click the name of the AV user account that you created in "Task 1: Configure the domain user account with virus-checking rights" on page 50, and select **Properties.**

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

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

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

Task 2: Configure virus checker parameters for the Shared Folder Server

1. From the taskbar, click **Start** and select **Settings › Control Panel › Administrative Tools › Celerra Management**.
2. In the VNX Management Console tree, expand the Data Management node (for a VNXe system, the entries represent the Shared Folder Servers).

   The AntiVirus mode appears in the console tree. The status of the AntiVirus service for the selected VNXe Shared Folder Server is either Stopped or Running.

   Note: If you did not select a Shared Folder Server, you must select one before you can use the Celerra AntiVirus Management snap-in. If a Shared Folder Server is selected, its name appears next to the Data 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 select **Properties**.

      The **Properties** dialog box for that parameter appears. For a description of the parameters, refer to "Configurable AntiVirus node parameters" on page 54.

   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 click **OK**.

Configurable AntiVirus node parameters

Table 9 lists the configurable parameters for an AntiVirus node.

Table 9 Configurable AntiVirus node parameters

Parameter	Description	Example
masks=	File extensions to scan.	Scan all files: *.* Scan only .exe, .com, .doc, and .ppt files: *.exe:*.com:*.doc:*.ppt
excl=	Files or file extensions to exclude during scanning.	pagefile.sys:*.tmp
addr=	IP addresses of the AV servers.	Single server: 192.16.20.29 Multiple servers: 192.16.20.15:192.16.20.16:192.16.20.17
CIFSserver	Name of the Shared Folder Server. If you do not provide a name, the default Shared Folder Server is used.	cifsserver1
maxsize=n	Maximum file size in hex that is checked. Files that exceed this size are not checked.	0x1000000
RPCRequestTimeout	RPC request timeout in msec. The default is 25000 msec.	25000
RPCRetryTimeout	RPC retry timeout in msec. If the AV server does not answer a request from the Shared Folder Server within the time specified in the PRCRetryTImeout interval, the Shared Folder Server retries sending the request until the RPCRequestTimeout value is reached. The default RPCRetryTimout is 500 msec.	500
surveyTime=n	Time interval in seconds to scan for all known AV servers. This parameter works with the shutdown parameter below. If an AV server does not answer a request, the selected shutdown parameter determines the action to take. The minimum surveyTime is 1 second, the maximum is 4,294,967,295 seconds, and the default is 60 seconds.	60
highWaterMark=xxx	When the number of requests in progress becomes greater than the highWaterMark, a log event is sent to the Shared Folder Server. The default highWaterMark is 200.	200
lowWaterMark=xxx	When the number of requests in progress becomes lower than the lowWaterMark, a log event is sent to the Shared Folder Server. The default lowWaterMark value is 50.	50
shutdown	Action taken when an AV server is not available. For shutdown=no, continue retrying the list of AV servers if no AV server is available. Two watermarks exist: low and high. When each is reached, a log event is sent to the VNXe Shared Folder Server. For shutdown=cifs, stop CIFS if no AV server is available. (Windows clients cannot access any VNXe shares.) For shutdown=viruschecking, stop virus checking if no AV server is available. (Windows clients can access any VNXe shares without virus checking.)	Options include: • shutdown=no • shutdown=cifs • shutdown=viruschecking

Task 3: Install third-party antivirus software on the AV servers in the domain

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 VNXe Shared Folder 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 EMC E-Lab™ Interoperability Navigator and the EMC *Celerra Network Server Release Notes* on the EMC Online Support website (http://support.emc.com).

NOTICE

You must install any supported third-party antivirus software package, except for the Trend MicroServerProtect package, on a host *before* installing VEE CAVA on a host. If you want to install Trend MicroServerProtect antivirus software on a host, install VEE CAVA first as described in "Task 4: Install VEE CAVA on the Windows AV servers" on page 55.

To install a third-party antivirus software package on a host, follow the procedure for the package in *EMC Celerra Network Server - Using the Celerra AntiVirus Agent*.

Task 4: Install VEE CAVA on the Windows AV servers

You must install VEE CAVA on each host in the domain that will be an AV server.

Prerequisites

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

Removing old versions of VEE CAVA

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

Note: If you do not remove the previous version of VEE 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 VEE CAVA

During a reinstallation of VEE 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.

To install VEE CAVA

Install VEE CAVA software from the VNX Event Enabler CD as described in *EMC VNX Network Server - Using the VEE Common AntiVirus Agent*.

Task 5: Start the VEE AV engine (virus-checking agent) on the VNXe system

1. In the VNXe Unisphere, select **Settings › Shared Folder Server Settings**.
2. In the **Other Options** section, click **Start Antivirus**.

The Antivirus status changes to `Antivirus is running`.