EMC® VNX® Series

Release 8.1

File Extension Filtering on VNX®

P/N 300-014-337 Rev 01

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Published August 2013

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.

Corporate Headquarters: Hopkinton, MA 01748-9103

Contents

Preface

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

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

Special notice conventions

EMC uses the following conventions for special notices:

Note: Emphasizes content that is of exceptional importance or interest but does not relate to personal injury or business/data loss.

NOTICE Identifies content that warns of potential business or data loss.

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

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

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

Where to get help

EMC support, product, and licensing information can be obtained as follows:

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

Troubleshooting—Go to EMC Online Support at http://Support.EMC.com. After logging in, locate the applicable Support by Product page.

Technical support—For technical support and service requests, go to EMC Customer Service on EMC Online Support at http://Support.EMC.com. After logging in, locate the applicable Support by Product page, and choose either **Live Chat** or **Create a service request**. To open a service request through EMC Online Support, 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.

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

Your comments

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

Please send your opinion of this document to:

techpubcomments@EMC.com

1 Introduction

The EMC VNX for File uses the extension of a file to filter the types of files that Microsoft Windows users can save to a CIFS share or a Data Mover. For example, you can prevent users from saving graphic files to a CIFS share by filtering out the extension of graphic files, such .gif and .jpg.

Topics include:

System requirements

Table 1 on page 8 describes the EMC® VNX® software, hardware, network, and storage configurations.

Table 1. System requirements for file extension filtering

Software	VNX for File version 8.1
Hardware	No specific hardware requirements
Network	CIFS services configured on VNX
Storage	No specific storage requirements

Restrictions

The File extension filtering limitations are as follows:

- This feature works only for CIFS access. If your environment is a mixture of CIFS and NFS, NFS users are not affected by file extension filtering and are able to store prohibited files on the file system.
- The Data Mover user authentication must be set to the recommended default, NT.
- File extension filtering can be circumvented by using file extensions that do not pertain to the contents of a file. For example, even if filtering for .gif files, you could still store .gif image files on a share by giving them a fake extension like .gfi.

User interface choices

This document describes how to configure file extension filtering by using the command line interface (CLI). You cannot use other VNX management applications to configure file extension filtering.

Related information

The following documents provide specific information related to the features and functionality described in this document:

- *EMC VNX Command Line Interface Reference for File*
- VNX for File man pages
- *Parameters Guide for VNX for File*

EMC VNX documentation on EMC Online Support

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

VNX wizards

Unisphere software provides wizards for performing setup and configuration tasks. The Unisphere online help provides more details on the wizards.

2 Concepts

The file extension filtering concepts are as follows:

Concepts

The file extension filtering mechanism uses a combination of a file's extension and access control lists (ACLs) to allow or disallow access to files with certain file extensions. The combination of file extensions and ACLs provides fine-grain control of filtering, and allows you to perform the following:

- Prevent certain types of files from being saved on a share.

Example: You do not require any video files stored on a share. You can configure file extension filtering to block .mpg, .avi, .mp2, and other video files on the share.

- Prevent a particular user or group from accessing a certain type of file on a share.

Example: You create a share where you store confidential Microsoft PowerPoint presentations. Regular employees are allowed to view these presentations. However, contractors are not. You can configure file extension filtering to allow everyone except the people in the Contractors group to view .ppt files on the share.

- Allow only certain types of files to be saved on a share.

Example: You create a share and want to reserve it for Microsoft Word and PowerPoint files. You configure file extension filtering to allow only .doc and .ppt files to be saved on the share. In addition, if you do not want the files deleted from the share, you can also configure file extension filtering to prevent that action.

What is filtered:

Files are filtered based on a file's three-letter extension, not on the contents of the file.

Where is filtering done:

File extension filtering occurs at the Data Mover or CIFS share level and cannot be done at the folder level within a share.

If a file system contains nested shares, the share name used to map the network drive determines what filtering policy is in effect and does not change at nested share boundaries.

Example: You have two shares, where one, \Product_announcements, is nested inside of the other, \Marketing, and have filtering set as shown in Figure 1 on page 12.

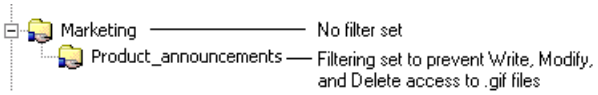

Figure 1. Nested shares example

In the previous example, if a user connects to the \Product_announcements share, they can view .gif files, but create or modify them. However, a user connecting to the \Marketing share is still able to access \Product_announcements, and has full control over .gif files because the share they connect to does not have a filter and the ACL is set to Full Control.

How filtering is accomplished:

The File extension filtering uses two components:

- A set of filter files named with a special naming convention that includes the name of the extension and share that you want to filter. You must store these files in the \.filefilter directory, a special directory on the Data Mover. If there are no filter files in the \.filefilter directory, filtering does not occur.
- The ACL set on the filter file. You can use the ACL to set exceptions to the filter policy. The ACL allows you to limit file extension filtering on a domain-user basis.

Create filter files

To restrict files of certain types, you must create special filter files in the \.filefilter directory on the root share (C$) of the Data Mover. You must create one file for every extension/share combination that you want to filter. Therefore, if you want to restrict both .gif and .jpg files from a share, you must create two files: one to control filtering for .gif files and the other to control filtering for .jpg files. The filter files can be created with any text editor, and then named with the naming convention discussed in this section.

Note: To access the root share (C$) of the Data Mover, you need local administrator access rights. The Data Mover is in the /.filefilter directory under the Data Mover's root file system. The directory path for a Virtual Data Mover is /.etc/.filefilter under the Data Mover's root file system.

Name filter file

Use the filter files naming convention:

<*extension_name*>[@<*sharename*>[@<*netbios_name*>]]

where:

<*extension_name*> = file extension that you want to filter.

<*sharename*> = name of the share to which you want to apply the filter. The <*sharename*> is an optional part of the filename. If you do not include a <*sharename*>, the filter is applied to all shares on the Data Mover.

<*netbios_name*> = NetBIOS name to which you want to limit the filtering. The <*net bios_name*> element is an optional part of the filename. If you specify the NetBIOS name, you must also specify a share name. If the share is available on multiple NetBIOS names, this name element limits the filtering to a particular NetBIOS name.

Example: To prevent .mpg files from being saved on the \no_video share on Data Mover server_2, you would create a file in the \.filefilter directory of server_2 and name it mpg@no_video. This filter file would prevent any .mpg files from being created on the \no_video share.

To prevent .gif and .jpg files from being saved by users accessing the share \engineering_3 on server_2 through NetBIOS name field_eng, you would have to create two files with the following names and place them in the \.filefilter directory on Data Mover server_2:

gif@engineering_3@field_eng

jpg@engineering_3@field_eng

Enable file filtering

These file extension filtering characteristics are controlled by the CIFS enableFileFiltering parameter:

- Filtering: Determines whether file extension filtering is in effect. Value 0 disables filtering.
- Pop-up messages: Displays the following message on the client whenever a user is blocked from performing some function on a client:

Note: For the pop-up messages to work, the messenger service must be running on the client. On a Windows 2000 client, this messenger service starts by default; on a Windows 2003 client, this service does not start by default.

```
File extension not allowed
```

- Auditing: Audits the access attempts against filtered extensions. You can view the audits through the Windows Event Viewer.

Note: The parameter value 1 enables file filtering; value 3 enables file filtering and generates pop-up messages; value 5 enables file filtering and audit; and value 7 enables file filtering, pop-ups, and auditing.

The *Parameters Guide for VNX* provides additional information about the CIFS enableFileFiltering parameter.

3 Configuring

The tasks for configuring file extension filtering are as follows:

- Create a filter file on page 16
- Configure exceptions to file extension filtering on page 16
- Disable file extension filtering for specific users and groups on page 17
- Use file extension filtering to control privileges on page 17
- Use file extension filtering to control privileges for specific users on page 18

Create a filter file

To create a filter file:

1. From a Windows workstation on the domain, log in as the domain administrator.
2. From Windows Explorer, map a drive to the root file system of the Data Mover (\\<movername>\C$).

   where:

   <movername> = name of the CIFS server.
3. Move to the \.filefilter directory on the root of the file system (C$ share).
4. Use Windows Notepad to create a blank file.
5. Name the file in accordance with the naming convention discussed in Name filter file on page 13.

   Note: You should test applications thoroughly when using file extension filtering. Some applications may create files with special or undocumented extensions that may be problematic. Special considerations for filtering Microsoft Office application files on page 21 provides examples.
6. Optionally, you can configure exceptions to the filter policy by configuring the filter file's ACL through the file's Properties sheet. Configure exceptions to file extension filtering on page 16 provides more information.

   Note: When you originally create the filter file, there are no ACEs in the file's ACL.

Configure exceptions to file extension filtering

When you create a filter file with no ACLs, all actions against that file type are restricted so that a user cannot list, read, write, execute, or delete the restricted file. In effect, the filter file creates a blanket restriction to the specified file type.

However, you can modify this blanket restriction by configuring the filter file's ACL.

Note: When you initially create a filter file in the \.filefilter directory, the file has only one ACE, which is its owner with Full Control privileges.

You can modify the ACL on the filter file so that:

- Only certain users and/or groups can access files with the pertinent extension.

Disable file extension filtering for specific users and groups on page 17 provides more information.

- Only certain actions can be performed against the specified file type.

Use file extension filtering to control privileges on page 17 provides more information.

- Only specific users or groups are allowed to or prohibited from performing certain actions against the specified file type.

Use file extension filtering to control privileges for specific users on page 18 provides more information.

Disable file extension filtering for specific users and groups

If you have restricted a specific file type on a share, you can permit exceptions to the filter by configuring the ACL on the filter file to allow specific users or groups Full Control privilege on the file.

Example: You have a filter file named gif@engineering_files. You can set the ACL, so that people in the Engineering group have full access to .gif files, while users outside the Engineering group are denied all access to .gif files on the share.

To disable file extension filtering:

1. Right-click the filter file gif@engineering_files, and click **Properties ➤ Security**.
2. Click **Add** to add the Engineering group.
3. Under **Permissions**, select the checkboxes **Full Control**, **Modify**, **Read & Execute**, **Read**, and **Write** to allow specific permissions for the user.
4. Click **Apply**, and then click **OK**.

Use file extension filtering to control privileges

Instead of enforcing a blanket restriction against a type of file, you can configure the filter file's ACL so that everyone can perform (or is prevented from performing) certain actions against a file type. To do this, you would add an ACE for Everyone, and then modify the Advanced properties to allow or deny specific actions.

Example: You can allow everyone access to .gif files on \engineering_files, while preventing anyone from deleting .gif files from the share. In this case, you create the filter file, gif@engineering_files, and in the file's ACL, create an ACE for Everyone and set privileges to Modify, Read & Execute, Read, and Write. Then, under Advanced properties, you can explicitly deny Delete privilege to Everyone.

To use file extension filtering to control privileges:

1. Right-click the filter file, gif@engineering_files, and click **Properties ➤ Security**.

2. Under **Name**, click **Everyone**.

3. Under **Permissions**, select the checkboxes to allow users **Full Control**, **Modify**, **Read & Execute**, **Read**, and **Write** privileges.

4. Click **Apply**. Click **Advanced** and select the checkboxes under **Deny** to deny privileges to the user.

Use file extension filtering to control privileges for specific users

You can combine options Disable file extension filtering for specific users and groups on page 17 and Use file extension filtering to control privileges on page 17 to gain a very fine level of control over file extension filtering. By modifying the filter file's ACL, you can restrict a few users from performing certain actions, while allowing other users to perform other actions.

Example: You create the filter file, gif@engineering_files, and you want the following users to have these privileges to .gif files on the share /engineering_files.

User or group	Includes	Type of privilege
Everyone	All personnel in the company	View .gif files
Engineering	All personnel in the Engineering department	View, create, and modify .gif files but not delete them
Bob Smith	Manager of Engineering department	Full Control over .gif files including the ability to delete them

To use file extension filtering to control privileges for specific users:

1. Right-click the filter file, gif@engineering_files, and click **Properties ➤ Security**.

2. Click **Add** to add different users.

3. Select user, and then under **Permissions**, set the permissions you want for that user. Click **Apply**. Click **Advanced** to define advanced permissions, and click **OK**.

4. Repeat the steps for each user.

4 Managing

The tasks to manage file extension filtering are as follows:

Reserve a share for a specific type of file

You can also configure file extension filtering so that a share is reserved for a specific file type. In this case, instead of a filter file prohibiting a file type from a share, it prohibits all file types from the share, except the type identified by the filter file.

Use the following special filter files with a regular filter file to reserve a share for a specific type of file. Table 2 on page 20 describes the special files and their purposes.

Table 2. Special filter files for reserving a share

Filter filename	Purpose
allfiles[@<sharename>][@<netbios_name>]	Prohibits all file types from the share. File types that are exceptions to this blanket restriction are identified by regular filter files.
noext[@<sharename>][@<netbios_name>]	Prohibits files with no extension from the share. Prevents users from circumventing the allfiles restriction by saving files with no filename extension.
<extension_name>[@<sharename>[@<netbios_name>]]	Identifies the file types allowed on the share. You must configure the ACLs on the filter files to identify users and groups (or Everyone) that can create files on the share. File types specified by regular filter files are the exceptions to the allfiles restriction.

Note: If you want to use @ or % in an extension, sharename, or a NetBIOS name, replace @ with %40 and % with %25. Examples: @ext is %40ext and ext% is ext%25.

Example: You want to allow only Adobe Acrobat (.pdf) files on a share named \dept_plans. To reserve \dept_plans for .pdf files, you must create three filter files:

Filename	ACL	Purpose
pdf@dept_plans	Add an ACE so that Everyone (or specific users and groups) has Full Control privilege.	Allows the creation and modification of .pdf files on the \dept_plans share.
allfiles@dept_plans	No ACL.	Prohibits all file types (except those indicated by specific filter files) from the share.

Filename	ACL	Purpose
noext@dept_plans	No ACL.	Prohibits files with no extension from the share.

Reserve a share

To reserve a share:

1. Log in as a domain administrator and navigate to the \.filefilter directory on the root of the file system (C$ share).
2. Perform the following:
   a. Create a filter file in the \.filefilter directory.
   b. Name the filter file with the extension/sharename combination for the file type that you want to allow on the share.
   c. Add ACEs to the filter file's ACL to grant **Everyone** (or specific users and groups) privileges on the file. These privileges allow the specified users access to the file types identified by the filter file.

   Note: If you want to allow more than one file type on a share, create multiple filter files and set the ACLs accordingly.
3. Create a filter file and name it:

   allfiles*[@<sharename>][@<netbios_name>]*
4. Create another filter file and name it:

   noext*[@<sharename>][@<netbios_name>]*

Special considerations for filtering Microsoft Office application files

Creating filter policies for Microsoft Office applications, such as Microsoft Word, is a little more complicated than creating policies for other file types. The Microsoft applications create, merge, rename, and delete several temporary files during the process of creating one Microsoft Office file. Therefore, you must create filter files that allow the Microsoft applications to create the temporary file types on the share.

Note: File extensions for Microsoft 2007 Office products use four-letter characters instead of three. Four-letter extensions are used the same way as three-letter extensions.

Special considerations for Microsoft Word

All temporary files created by Microsoft Word all have the extension, .tmp. If you want to restrict the \marketing share to only Word documents, you can create the following filter files in the \.filefilter directory. Table 3 on page 22 provides information for creating filter files for Microsoft Word.

Table 3. Filter files for Microsoft Word

Filter file	ACL	Purpose
allfiles@marketing	No ACL.	Prohibits all file types (except those indicated by specific filter files) from the share.
doc@marketing	Create an ACE that allows Everyone (or specific users and groups) Full Control.	Allows the creation and modification of .doc files by the specified users.
tmp@marketing	Create an ACE that allows Everyone (or specific users and groups) Full Control.	Allows the creation and modification of .tmp files by the specified users.
noext@marketing	No ACL.	Prohibits files with no extension from the share.

Special cases for Word

In addition to the basic Word files, you may also need to create the following filter files to handle other special file types. Table 4 on page 22 provides information for creating special file types for Microsoft Word.

Table 4. Special filter files for Microsoft Word

Filter file	ACL	Description
asd@marketing	Create an ACE that allows Everyone (or specific users and groups) Full Control.	If a user has enabled Word's AutoRecovery option, temporary .asd files are created.
wmf@marketing	Create an ACE that allows Everyone (or specific users and groups) Full Control.	When a user links OLE objects in a Word document (for example, to Excel spreadsheets), Word creates temporary .wmf files to represent the linked objects.

Table 4. Special filter files for Microsoft Word *(continued)*

Filter file	ACL	Description
rtf@marketing	Create an ACE that allows Everyone (or specific users and groups) Full Control.	If a user saves a Word document in another word processor format, Word's converter files temporarily create .rtf files.

Special considerations for Microsoft PowerPoint

Like Microsoft Word, the temporary files created by PowerPoint use the .tmp extension. To restrict the \marketing share to only PowerPoint (.ppt) files, you can create filter files in the \.filefilter directory. Table 5 on page 23 provides additional information.

Table 5. Filter files for Microsoft PowerPoint

Filter file	ACL	Purpose
allfiles@marketing	No ACL.	Prohibits all file types (except those indicated by specific filter files) from the share.
ppt@marketing	Create an ACE that allows Everyone (or specific users and groups) Full Control.	Allows the creation and modification of .ppt files by the specified users.
tmp@marketing	Create an ACE that allows Everyone (or specific users and groups) Full Control.	Allows the creation and modification of .tmp files by the specified users.
noext@marketing	No ACL.	Prohibits files with no extension from the share.

Enable file filtering

Action
To enable file filtering, use this command syntax: `$ server_param <movername> -facility [<facility_name> -modify ] [<param_name> ] [-value <new_value>] [ ]` where: *<movername>* = name of the Data Mover *<facility_name>* = name of the facility to which the parameter belongs *<param_name>* = name of the parameter *<new_value>* = value you want to set for the specified parameter Example: Note: Parameter and facility names are case-sensitive. To set the enableFileFiltering parameter to 7, type: `$ server_param server_2 -facility cifs -modify enableFileFiltering -value 7`
Output
`server_2 : done`

Customize file filtering pop-up message

The Windows Messenger Service must be enabled for Windows clients to receive pop-up messages:

1. Log in to the Control Station as **root**.
2. Edit the cifsmsg.txt file on the Data Mover by copying the file to the Control Station by using this command syntax:

   ```
   # server_file server_<x> -get cifsmsg.txt cifsmsg.txt
   ```

   where:

   <x> = Data Mover that has the cifsmsg.txt file that you want to edit

   Example:

   To copy the file from server_2, type:

   ```
   # server_file server_2 -getcifsmsg.txt cifsmsg.txt
   ```

   If this file does not exist, you must create it and specify the information shown in the following steps. If you do not create this file, VNX uses default messages in the pop-up windows.

3. Open cifsmsg.txt with a text editor.

   For file filtering, there are no warnings, and only the error.File_ReservedName error message appears in cifsmsg.txt:

   ```
   #
   # Error for file filtering
   #
   $ error.File_ReservedName=
   File extension not allowed
   For more information, contact your administrator
   .
   #
   # End Of File /.etc/cifsmsg.txt
   #
   ```

4. To change an error message, use this syntax:

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

```
$error. <status>=

<popup message line 1>
.
.
.

<pop-up message line n>
.
```

where:

<status>= Condition upon which you want the message sent

Options are as follows:

FileDeletedByVC

FileRenamedByVC

FileModifiedByVC = Virus detected and file has been cleaned up

File_ReservedName = File extension filtering block access

Remote = Pop-up generated when recover of an offline file is taking time

NoSpace = FS Full

QuotaExceeded

GroupQuotaExceeded

TreeQuotaExceeded <pop-up message line> = Message you want to send (such as the nature of the condition, contact information, and suggested action)

Note: The last line must be a period (.).

All pop-up messages also contain the share name and filename.

Note: To avoid repeating the same text for different messages, use the following syntax:

```
$ error.<status3>=$ error.<status2>
```

5. Save and close the file, and then type:

   ```
   $ server_file server_ <x> -put cifsmsg.txt cifsmsg.txt
   ```

6. To implement the changes you made to the cifsmsg.txt file, restart (stop and start) the CIFS service on the Data Mover (<x>) by using this command syntax:

   ```
   $ server_setup server_<x> -P cifs -o stop
   $ server_setup server <x> -P cifs -o start
   ```

If you have also changed the parameter, as described in Enable file filtering on page 24, restart the Data Mover (instead of restarting CIFS) to perform all the changes at once.

5 Troubleshooting

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

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

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

Topics included in this chapter are:

EMC E-Lab Interoperability Navigator

The EMC E-Lab™ Interoperability Navigator is a searchable, web-based application that provides access to EMC interoperability support matrices. It is available on EMC Online Support at http://Support.EMC.com. After logging in, in the right pane under **Product and Support Tools**, click **E-Lab Navigator**.

VNX user customized documentation

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

Error messages

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

To view message details, use any of these methods:

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

EMC Training and Professional Services

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

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

Glossary

A

access control entry (ACE)
In a Microsoft Windows environment, an element of an access control list (ACL). This element defines access rights to a file for a user or group.

access control list (ACL)
List of access control entries (ACEs) that provide information about the users and groups allowed access to an object.

access policy
Policy that defines which access control methods (NFS permissions or Windows ACLs or both) are enforced when a user accesses a file on VNX for file in an environment configured to provide multiprotocol access to some file systems. The access policy is set with the server_mount command and also determines which actions a user can perform against a file or directory.

C

CIFS
See Common Internet File System.

Common Internet File System (CIFS)
File-sharing protocol based on the Microsoft Server Message Block (SMB). It allows users to share file systems over the Internet and intranets.

F

filter file
File that specifies the types of files to filter and the share on which files are filtered.

S

security mode
Setting that specifies how a Data Mover performs authentication for CIFS users. The security mode is set for each Data Mover not for a file system.

share

File system, directory, or service that has been made available to CIFS users on the network. Also, the process of making a file system, directory, or service available to CIFS users on the network.

Index