## Preface

## Chapter 1: Introduction

- System requirements
- Related information

## Chapter 2: Concepts

- Local groups
- User rights
- Auditing

## Chapter 3: Managing the Windows Server

- Open Computer Management MMC
- Create local groups on a Data Mover using MMC
- Assign user rights using Celerra Management Console
- Create shares and set ACLs using MMC
- Monitor Data Mover connections and resource usage using MMC
- Monitor users on the Data Mover
- Monitor access to shares on the Data Mover
- Monitor use of files on the Data Mover
- Audit CIFS users and objects using Celerra Management Console
- Specify the audit policy
- Set the audit log parameters
- Change log file size
- View the audit events
- Disable auditing
- Connect the MMC to a CIFS server
Chapter 4: Managing Windows NT

Access Windows NT management interfaces for a CIFS server........44
Access User Manager for Domains.............................................44
Access Server Manager for Domains.........................................46
Access Event Viewer.................................................................47
Create local groups on a Data Mover using User Manager............48
Assign user rights using User Manager.......................................50
Create shares and set ACLs using Server Manager.....................52
Monitor Data Mover connections and resource usage using Server
Manager..................................................................................54
Monitor users on the Data Mover..............................................55
Monitor access to shares on the Data Mover...............................57
Monitor use of Data Mover resources.......................................58
Audit CIFS users and objects using Windows NT management
interfaces................................................................................59
Specify the auditing policy.......................................................59
Set the audit log parameters....................................................61
Change log file size....................................................................62
View the audit events...............................................................64
Disable auditing using User Manager........................................65
Enable auditing on a folder or file.............................................66

Chapter 5: Troubleshooting

Where to get help.........................................................................74
EMC E-Lab Interoperability Navigator.........................................74
EMC Training and Professional Services.....................................74

Terminology.................................................................................77

Index..........................................................................................79
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:

A caution contains information essential to avoid data loss or damage to the system or equipment.

Important: An important note contains information essential to operation of the software.

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

Hint: A note that provides suggested advice to users, often involving follow-on activity for a particular action.

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 the EMC Powerlink website (registration required) at http://Powerlink.EMC.com.

Troubleshooting — Go to Powerlink, search for Celerra Tools, and select Celerra Troubleshooting from the navigation panel on the left.

Technical support — For technical support, go to EMC Customer Service on Powerlink. After logging in to the Powerlink website, go to Support ➤ Request Support. To open a service request through Powerlink, you must have a valid support agreement. Contact your EMC Customer Support Representative for details about obtaining a valid support agreement or to answer any 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
The EMC® Celerra® Network Server supports the CIFS protocol that allows Windows clients to access files stored on the Celerra Network Server. After you configure the Celerra Network Server to support Windows clients on the network, use Windows tools to perform a variety of administrative tasks on the Data Mover.

The Configuring and Managing CIFS on Celerra provides more information about how to configure the Celerra Network Server for CIFS support.

This document is part of the Celerra Network Server documentation set and is intended for system administrators responsible for implementing the Celerra Network Server in their Windows network or for adding Windows clients to their existing UNIX network.

- System requirements on page 8
- Related information on page 8
System requirements

Table 1 on page 8 describes the Celerra Network Server software, hardware, network, and storage configurations.

Table 1. System requirements

<table>
<thead>
<tr>
<th>Software</th>
<th>Celerra Network Server version 5.6.47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>No specific hardware requirements</td>
</tr>
<tr>
<td>Network</td>
<td>No specific network requirements</td>
</tr>
<tr>
<td>Storage</td>
<td>No specific storage requirements</td>
</tr>
</tbody>
</table>

Related information

For specific information related to the features and functionality described in this document:

- Configuring and Managing CIFS on Celerra
- Managing Celerra for a Multiprotocol Environment
- Using International Character Sets with Celerra
- Using Wizards to Configure Celerra
- Configuring Celerra User Mapping
- Using NT Migrate with Celerra
- Online Celerra man pages

EMC Celerra Network Server Documentation CD

The EMC Celerra Network Server Documentation CD, supplied with Celerra and also available on the EMC Powerlink® website, provides the complete set of EMC Celerra customer publications. After logging in to Powerlink, go to Support ➤ Technical Documentation and Advisories ➤ Hardware/Platforms Documentation ➤ Celerra Network Server. On this page, click Add to Favorites. The Favorites section on your Powerlink home page provides a link that takes you directly to this page.

To request an EMC Celerra Network Server Documentation CD, send an email request to:

techpubcomments@EMC.com
Celerra Support Demos

Celerra Support Demos are available on Powerlink. Use these instructional videos to learn how to perform a variety of Celerra configuration and management tasks. After logging in to Powerlink, go to Support ➤ Product and Diagnostic Tools ➤ Celerra Tools ➤ Celerra Support Demos.

Celerra wizards

Celerra wizards can be used to perform Celerra Manager tasks. Using Wizards to Configure Celerra provides you with an overview of the steps required to configure a Celerra Network Server by using the Set Up Celerra wizard in Celerra Manager.
Introduction
The concepts to understand the administrative tools are:

- Local groups on page 12
- User rights on page 12
- Auditing on page 13
Local groups

When a new CIFS service is created on a Data Mover and it becomes a domain member, there are no local groups resident on the Data Mover. After you create a CIFS service on a Data Mover and add the Data Mover to the domain, use Windows NT User Manager to create and manage local groups on the Data Mover.

A local group is granted permissions and rights from its own computer to only those resources on its own computer on which the group resides.

In the Windows Server native domain, local groups can contain user accounts, global groups, and domain local groups, but not other local groups.

Celerra Network Server supports all types of Microsoft Windows Server user groups and nested groups. Celerra Network Server also supports local user accounts if they are set up. Configuring and Managing CIFS for Celerra provides more information about local groups.

In a Windows NT domain, local groups can contain user accounts and global groups, but not other local groups. Celerra Network Server supports all types of Windows NT user groups. However, Celerra Network Server does not support local user accounts.

Windows NT online help provides more information on creating and managing local groups.

User rights

You can use user rights assignments to manage which users and groups can log in to or execute tasks on a Data Mover. User rights assignments are local policies that apply only to the selected Data Mover.

Local groups, individual users, and global groups can be assigned privileges to:

- Access this computer from the network
- Back up files and directories
- Bypass traverse checking (improves performance)
- Perform EMC Virus Checking
- Generate security audits
- Increase quotas
- Log in as a batch job
- Log in as a service
- Log in locally
- Manage auditing and security log
- Restore files and directories
- Set security audit (users with this privilege can manage audits on the server)
Take ownership of files or object (all administrators have this capability)

Note: This capability is not supported for Data Movers in the current release.

To set user rights for individual users and global groups on a Data Mover, use the Celerra Data Mover Security Management Console, which is an MMC snap-in to the Celerra Management Console.

*Installing Celerra Management Applications* provides information about installing the Celerra Management Console. The Celerra Data Mover Security Management snap-in online help provides information about setting user rights.

Note: You cannot use Microsoft Windows Local Policy Setting tools to manage user rights assignments on a Data Mover because in Windows servers, these tools do not support managing user rights on a remote computer.

**Auditing**

To audit CIFS servers on a Data Mover, use the Celerra Data Mover Security Management Console, which is a MMC snap-in to the Celerra Management Console.

By default, auditing is disabled for all Windows object classes. To enable auditing, you must explicitly turn it on for specific events on specific Data Movers. After it is enabled, auditing is initiated whenever the CIFS service on the relevant Data Mover is started, and terminated whenever the CIFS service is stopped.

*Installing Celerra Management Applications* contains information about installing the Celerra Management Console. The Celerra Data Mover Security Management snap-in online help provides information on setting audit policies.

If the Group Policy Object (GPO) is configured and enabled on the Data Mover, then the GPO configuration of the audit settings is used. *Configuring and Managing CIFS on Celerra* provides more information about configuring audit settings.

The log files (security.evt, application.evt, and system.evt) are typically stored in the root file system, which has a maximum capacity of 128 MB. If you expect to retain large Event Viewer logs, you should select a different directory for storing these log files. To do so, edit the Registry residing on the Data Mover.

⚠️ If you do not have experience editing the Registry, seek assistance.

You can use the Windows NT Event Viewer to audit Data Movers for certain events and activities. Many of the event types available for monitoring and auditing on a Windows NT server can be audited on a Data Mover.

Auditing is available only on the specific object classes and events listed in Table 2 on page 14. Only members of the Administrators local group can set auditing on a server.
Table 2. Auditing object classes

<table>
<thead>
<tr>
<th>Object class</th>
<th>Event</th>
<th>Audited for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon/logoff</td>
<td>• CIFS user login</td>
<td>success</td>
</tr>
<tr>
<td></td>
<td>• CIFS guest login</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows NT/UNIX mapping (user/domain combination not found)</td>
<td>failure</td>
</tr>
<tr>
<td></td>
<td>• Password authentication error returned by domain controller (DC)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DC returned a nonprocessed error code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No reply from DC (insufficient resources or bad protocol)</td>
<td></td>
</tr>
<tr>
<td>File and object access</td>
<td>Object Open:</td>
<td>success</td>
</tr>
<tr>
<td></td>
<td>• File and directory access, if system access control list (SACL) is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set, for read, write, delete, execute, set permissions, and take</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ownership</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Security Access Manager (SAM) local group modification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Close Handle:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• File and directory access (if SACL set) for read, write, delete,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>execute, set permissions, and take ownership</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SAM database close</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Object Open for Delete:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• File and directory access (if SACL set)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete Object:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• File and directory access (if SACL set)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAM database access (lookup)</td>
<td>success and failure</td>
</tr>
<tr>
<td>Process tracking</td>
<td>Not supported</td>
<td>N/A</td>
</tr>
<tr>
<td>System restart/shutdown</td>
<td>Restart:</td>
<td>success</td>
</tr>
<tr>
<td></td>
<td>• CIFS service startup (includes DART release number)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CIFS service shutdown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Audit log cleared</td>
<td></td>
</tr>
</tbody>
</table>
Table 2. Auditing object classes (continued)

<table>
<thead>
<tr>
<th>Object class</th>
<th>Event</th>
<th>Audited for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security policies</td>
<td>Session Privileges:</td>
<td>success</td>
</tr>
<tr>
<td></td>
<td>◆ Enumerate user privileges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◆ User rights assigned</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◆ User rights deleted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy Change:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◆ List policy categories and associated audit state</td>
<td></td>
</tr>
<tr>
<td>Use of user rights</td>
<td>Not supported</td>
<td>N/A</td>
</tr>
<tr>
<td>User and group management</td>
<td>◆ Create local group</td>
<td>success</td>
</tr>
<tr>
<td></td>
<td>◆ Delete local group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◆ Add member to local group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◆ Remove member from local group</td>
<td></td>
</tr>
</tbody>
</table>

When auditing is enabled, the Event Viewer creates a Security log with the default settings shown in Table 3 on page 15.

Table 3. Default log settings

<table>
<thead>
<tr>
<th>Log type</th>
<th>Windows NT filename</th>
<th>Maximum file size</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>C:\security.evt</td>
<td>512 KB</td>
<td>10 days</td>
</tr>
</tbody>
</table>

Note: Before you can modify these values, you must complete the procedure in “Change log file size on page 62”

All Windows NT network users can establish auditing on directories or files they own, or to which they have read, write, and execute rights. The Celerra Network Server supports auditing on individual folders and files.
The administrative tasks to manage Windows on the CIFS server are:

**Note:** For purposes of illustrating management steps, Windows 2000 is used in this document. Depending on your version of Windows the steps required to accomplish these steps may vary.

- Open Computer Management MMC on page 18
- Create local groups on a Data Mover using MMC on page 20
- Assign user rights using Celerra Management Console on page 22
- Create shares and set ACLs using MMC on page 24
- Monitor Data Mover connections and resource usage using MMC on page 26
- Audit CIFS users and objects using Celerra Management Console on page 30
- Disable auditing on page 39
- Connect the MMC to a CIFS server on page 40
Open Computer Management MMC

Many Windows administrative tasks can be performed from the Computer Management Microsoft Management Console (MMC). This procedure opens the Computer Management MMC for a specific Data Mover.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to Windows Server with administrator privileges for the Data Mover.</td>
</tr>
<tr>
<td>2.</td>
<td>From the Start menu, select Programs ➤ Administrative Tools ➤ Computer Management.</td>
</tr>
<tr>
<td>3.</td>
<td>Double-click EMC Celerra, and then click Computers.</td>
</tr>
</tbody>
</table>

*Note:* This is the default location. This might have changed after the CIFS server was joined to the domain.
4. In the Computer panel, right-click the Data Mover to manage, and then select Manage from the shortcut menu.

As an alternative: From the Start menu, select Programs ➤ Administrative Tools ➤ Computer Management. The Computer Management window opens. To connect to a Data Mover, click Computer Management (local), and then select Connect to another computer. Type the name of the Data Mover, and then click OK.
Create local groups on a Data Mover using MMC

Use this procedure to create local groups on a Data Mover.

**Note:** The task instructions shown are for Windows 2000. Depending on your Windows version the steps required to accomplish these tasks may vary.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Open the **Computer Management MMC** for the Data Mover on which you want to create a local group.  
*Open Computer Management MMC on page 18* provides instructions. |
<p>| 2.   | Under <strong>System Tools</strong>, double-click <strong>Local Users and Groups</strong>. |
| 3.   | Right-click <strong>Groups</strong>, and then select <strong>New Group</strong> from the shortcut menu. |
| 4.   | In the <strong>New Group</strong> dialog box, type a group name and a description. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Click <strong>Add</strong>. The <strong>Select Users or Groups</strong> dialog box appears.</td>
</tr>
<tr>
<td>6.</td>
<td>Select user or group names and then click <strong>Add</strong> to add users or groups to the new group.</td>
</tr>
<tr>
<td>7.</td>
<td>Click <strong>OK</strong>. You return to the <strong>New Group</strong> dialog box.</td>
</tr>
<tr>
<td>8.</td>
<td>Click <strong>Create</strong>. The group is added to the <strong>Groups</strong> list.</td>
</tr>
</tbody>
</table>
## Assign user rights using Celerra Management Console

After the Celerra Management Console is installed, use this procedure to access the Security Management snap-in.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to a Windows Server with administrator privileges for the Data Mover.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Start, and then select Programs ➤ Administrative Tools ➤ EMC Celerra Management.</td>
</tr>
</tbody>
</table>
| 3.   | If a Data Mover name appears after Data Mover Management, go to step 4. Otherwise:  
  1. Right-click Data Mover Management, and then select Connect to Data Mover from the shortcut menu.  
  2. In the Select Data Mover dialog box, select a Data Mover by using one of the following methods:  
     - In the Look in list, select the domain in which the Data Mover you want to manage is located, and then select the Data Mover from the list.  
     - In the Name field, type the computer name, IP address, or the NetBIOS name of the Data Mover. |
| 4.   | Double-click Data Mover Management, and then double-click Data Mover Security Settings. |
5. Select User Rights Assignment.
The assignable rights appear in the right panel.

6. Double-click a user right to assign it to a particular group or user.
The Celerra Data Mover Security Management snap-in online help provides more information on setting rights.
Create shares and set ACLs using MMC

Before you begin

To create a share with MMC, you must:

◆ Have assigned UNIX UIDs and GIDs to CIFS users. Configuring and Managing CIFS on Celerra and Configuring Celerra User Mapping provides instructions for assigning UIDs.
◆ Have mounted the file system and created directories you want to share.
◆ Be a member of the local Administrators group on a Data Mover.

Procedure

Use the MMC to create shares and set ACLs on shares after you create a CIFS server on a Data Mover, join it to the domain, and start the CIFS service.

Note: Shares created through Windows administrative tools are accessible only from the NetBIOS name used by the Windows client. If you want the share to be globally accessible by all NetBIOS names, create a share with the Celerra server_export command and omit the option netbios=<netbiosName>.

This procedure creates a share on a Data Mover for Windows Server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Open the Computer Management MMC for the Data Mover.  
      | Open Computer Management MMC on page 18 provides instructions. |
2. In the console tree, click **Shared Folders ➤ Shares**.

The current shares in use appear on the right.

3. Right-click **Shares**, and then select **New File Share** from the shortcut menu.

4. Provide:

   - The name of the folder to share. Type the path of the folder, or click **Browse** and locate the folder.
   - The share name for the folder. You cannot create a NetBIOS share name with the same name as a global share. The Celerra Network Server supports only ASCII share names. Share name length is limited to 12 ASCII characters unless Unicode support is enabled, in which case the limit is 80 multibyte characters. Share names cannot include the following characters: /, \, %, "", NUL (Null character), STX (start of header), SOT (start of text), and LF (line feed). Share names can contain spaces and other nonalphanumeric characters, but must be enclosed by quotas if spaces are used. Share names cannot begin with a - (hyphen). Share names are case-sensitive.
   - A share description.

5. Click **Next**.

You are prompted for share permissions.

6. For Windows Server, set permissions by selecting one of the options. With the Customize Share and Folder Permissions option, you can assign permissions to individual groups and users.

7. Click **Finish**.
Monitor Data Mover connections and resource usage using MMC

You can use Windows administrative tools to:

- Monitor users on the Data Mover on page 27
- Monitor access to shares on the Data Mover on page 28
- Monitor use of files on the Data Mover on page 29
Monitor users on the Data Mover

For Windows servers, use this procedure to monitor the number of users connected to a CIFS server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Open the Computer Management MMC for the Data Mover you want to monitor.  
Open Computer Management MMC on page 18 provides instructions. |
| 2.   | In the console tree, click Shared Folders ➤ Sessions.  
The current users connected to the CIFS server appear on the right. |
| 3.   | Optionally:  
• To force disconnections from the CIFS server, right-click the username, and then select Close Session from the shortcut menu.  
• To force all users to disconnect, right-click Sessions, and then select Disconnect All Sessions from the shortcut menu. |
## Monitor access to shares on the Data Mover

Use this procedure to monitor access to shares on the CIFS server.

**Note:** The steps and instruction screens for this task are for Windows 2000. Depending on your Windows version, the steps required to accomplish this task may vary.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the <strong>Computer Management MMC</strong> for the Data Mover. &lt;br&gt;&lt;br&gt;<strong>Open Computer Management MMC on page 18</strong> provides instructions.</td>
</tr>
<tr>
<td>2.</td>
<td>In the console tree, click <strong>Shared Folders ➤ Shares</strong>. &lt;br&gt;The current shares in use appear on the right.</td>
</tr>
<tr>
<td>3.</td>
<td>Optionally, to force disconnections from a share, right-click the share name, and then select <strong>Stop Sharing</strong> from the shortcut menu.</td>
</tr>
</tbody>
</table>
## Monitor use of files on the Data Mover

For Windows servers, use this procedure to monitor open files on the CIFS server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Open the **Computer Management MMC** for the Data Mover.  
      **Open Computer Management MMC on page 18** provides instructions. |
| 2.   | In the console tree, click **Shared Folders ➤ Open Files**.  
The files in use appear on the right. |
| 3.   | Optionally, to close an open file, right-click the file, and then select **Close Open File** from the shortcut menu.  
To close all open files, right-click the Open Files folder, and then select **Disconnect All Open Files** from the shortcut menu. |
Audit CIFS users and objects using Celerra Management Console

Complete the following steps to enable auditing on a Data Mover:

◆ Specify the audit policy on page 31
◆ Set the audit log parameters on page 33
◆ Change log file size on page 34
◆ View the audit events on page 37

**Note:** Ensure that the CIFS service is running on the Data Mover.
Specify the audit policy

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to a Microsoft Windows server by using an account that is a member of the local Administrators group on the Data Mover.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Start, and then select Programs ➤ Administrative Tools ➤ EMC Celerra Management.</td>
</tr>
</tbody>
</table>
| 3.   | In the Celerra Management window:  
  - If a Data Mover is selected (name appears after Data Mover Management), go to step 4.  
  - If a Data Mover is not selected:  
    1. Right-click Data Mover Management, and then select Connect to Data Mover from the shortcut menu.  
    2. In the Select Data Mover box, to select a Data Mover:  
      - In the Look in list, select the domain in which the Data Mover you want to manage is located, and then select the Data Mover from the list.  
      - In the Name field, type the computer name, IP address, or the NetBIOS name of the Data Mover.  
  4. Double-click Data Mover Management, and then double-click Data Mover Security Settings. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Select Audit Policy. The audit policies appear in the right panel.</td>
</tr>
<tr>
<td>6.</td>
<td>Right-click Audit Policy, and then select Enable Auditing from the shortcut menu.</td>
</tr>
<tr>
<td>7.</td>
<td>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 on audit policy.</td>
</tr>
</tbody>
</table>
### Set the audit log parameters

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the <strong>Computer Management MMC</strong> for the Data Mover. &lt;br&gt;Open Computer Management MMC on page 18 provides more details.</td>
</tr>
<tr>
<td>2.</td>
<td>Double-click <strong>Event Viewer</strong>. The specific log files are displayed.</td>
</tr>
<tr>
<td>3.</td>
<td>Right-click a log file, and then select <strong>Properties</strong> from the shortcut menu. &lt;br&gt;The property sheet for the log appears.</td>
</tr>
<tr>
<td>4.</td>
<td>Normally, the <strong>Maximum log size</strong> field is locked. You cannot modify the log file size unless you complete the procedure described in Change log file size on page 34. &lt;br&gt;After you have completed the procedure, return to the <strong>Application Properties</strong> dialog box for the log and click the arrows to increase or decrease the size of the logs.</td>
</tr>
</tbody>
</table>

**Audit CIFS users and objects using Celerra Management Console**
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 type a value. The file size specified in step 4 is not exceeded. New events will not be 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.

Change log file size

Auditing must be enabled on the Data Mover for the log file size changes to take effect.

**Note:** The steps and instruction screens for this task are for Windows 2000. Depending on your Windows version, the steps required to accomplish these tasks may vary.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>On the Windows Server system used to manage the Data Movers, start the Registry Editor as follows:</td>
</tr>
<tr>
<td></td>
<td>1. Select Start Run.</td>
</tr>
<tr>
<td></td>
<td>2. Type regedit.exe in the Open field.</td>
</tr>
<tr>
<td></td>
<td>3. Click OK.</td>
</tr>
<tr>
<td></td>
<td>The Registry Editor opens.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>From the Registry menu, select Connect Network Registry. The Connect Network Registry dialog box appears.</td>
</tr>
</tbody>
</table>

**Note:** Depending on how the CIFS account is set up, you might receive an error message stating, “Unable to connect to all roots in the computer’s registry.” Click OK to continue.
3. In the **Computer** name field, type the name of the CIFS server and click **OK**

   The **Registry Editor** is updated to display the Registry information for the CIFS server.

4. Navigate to the following Registry key on the CIFS server:

   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\Security`

   The settings for the Registry key appear in the right panel.

5. Right-click the **File** icon in the right panel, and then select **Modify**.

   The **Edit String** dialog box appears.

6. In the **Value data** field, edit the path for the log file. For example,

   `C:\<mntpt>\<directory_name>\security.evt`

   Where:

   - `<mntpt>` = mount point of the file system (not the root file system)
   - `<directory_name>` = name of the directory that contains the log file

   Example:

   `C:\CIFS_FS_1\Win2KLog\security.evt`

   **Warning:** Do not change the name of the log file.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Click OK.</td>
</tr>
<tr>
<td>8.</td>
<td>Close the Registry Editor. The changes take effect immediately.</td>
</tr>
</tbody>
</table>
View the audit events

Use this procedure to view the audit events.

Note: The steps and instruction screens provided are for Windows 2000. Depending on your Windows version, the steps required to accomplish these tasks may vary.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click Start, and then select Programs ➤ Administrative Tools ➤ Event Viewer.</td>
</tr>
<tr>
<td>2.</td>
<td>Right-click the Event Viewer icon in the right panel, and then select Connect to Another Computer from the shortcut menu. The Select Computer dialog box appears.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Browse, select the name of the Data Mover to which you want to connect, and then click OK. Click OK again to close the Select Computer dialog box.</td>
</tr>
<tr>
<td>4.</td>
<td>Click the log. The log entries appear in the right panel.</td>
</tr>
</tbody>
</table>
5. Double-click the log entry to view the event detail.

The **Event Properties** window opens.
Disable auditing

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to a Windows domain controller by using an account that is a member of the local Administrators group on the Data Mover.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Start, and then select <strong>Programs ➤ Administrative Tools ➤ EMC Celerra Management</strong>.</td>
</tr>
</tbody>
</table>
| 3.   | Do one of the following:  
|      | - If a Data Mover is already selected (name appears after Data Mover Management), go to step 4.  
|      | - If a Data Mover is not selected:  
|      | 1. Right-click **Data Mover Management**, and then select **Connect to Data Mover** from the shortcut menu.  
|      | 2. In the **Select Data Mover** dialog box, select a Data Mover by using one of the following methods:  
|      |   - In the **Look** in list, select the Domain in which the Data Mover you want to manage is located, and then select the Data Mover from the list.  
|      |   - In the **Name** field, type the computer name, IP address, or the NetBIOS name of the Data Mover.  
<p>|      | 4. Double-click <strong>Data Mover Management</strong>, and then double-click <strong>Data Mover Security Settings</strong>. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Right-click <strong>Audit Policy</strong>, and then select <strong>Disable Auditing</strong> from the shortcut menu.</td>
</tr>
</tbody>
</table>

### Connect the MMC to a CIFS server

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Right-click <strong>My Computer</strong> and select <strong>Manage</strong> from the menu to open the MMC.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>2.</td>
<td>In the MMC, right-click <strong>Computer Management (Local)</strong> and select <strong>Connect to another computer</strong>. The <strong>Select Computer</strong> appears.</td>
</tr>
<tr>
<td>3.</td>
<td>Type the Celerra CIFS server hostname in the <strong>Another Computer</strong> box and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
Once connected, use the **Event Viewer**, **Shared Folders**, and **Local Users and Groups** panels in the MMC to manage the CIFS server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Once connected, use the <strong>Event Viewer</strong>, <strong>Shared Folders</strong>, and <strong>Local Users and Groups</strong> panels in the MMC to manage the CIFS server.</td>
</tr>
</tbody>
</table>
The administrative tasks to manage Windows NT on the CIFS server are:

- Access Windows NT management interfaces for a CIFS server on page 44
- Create local groups on a Data Mover using User Manager on page 48
- Assign user rights using User Manager on page 50
- Create shares and set ACLs using Server Manager on page 52
- Monitor Data Mover connections and resource usage using Server Manager on page 54
- Audit CIFS users and objects using Windows NT management interfaces on page 59
- Disable auditing using User Manager on page 65
- Enable auditing on a folder or file on page 66

Note: You cannot use Windows NT administrative tools to manage server General Information and Password Relative Information for Data Movers.
Access Windows NT management interfaces for a CIFS server

To perform Windows NT administrative tasks, open one of the Windows NT management interfaces and select a CIFS server.

To select a CIFS server:

- Access User Manager for Domains on page 44
- Access Server Manager for Domains on page 46
- Access Event Viewer on page 47

Access User Manager for Domains

Use this procedure to open User Manager for Domains and select a CIFS server to manage.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to a Windows NT server from an account that is a member of the local Administrators group on the Data Mover.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Start, and then select Programs ➤ Administrative Tools ➤ User Manager for Domains.</td>
</tr>
</tbody>
</table>
3. From the User menu, select Select Domain.

   ![Select Domain Window]

   In the Domain field, type the UNC name of the Data Mover’s CIFS server (for example, \DM101) or the CIFS server’s IP address, and then click OK. The User Manager window displays the default groups for the CIFS server.

4. In the Domain field, type the UNC name of the Data Mover’s CIFS server (for example, \DM101) or the CIFS server’s IP address, and then click OK. The User Manager window displays the default groups for the CIFS server.

   Note: User Manager for Domains works only if the CIFS server is a member of an NT 4.0 or Windows 2000 mixed mode domain.
### Access Server Manager for Domains

Use this procedure to open Server Manager and select a CIFS server to manage.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Log in to a Windows NT server from an account that is a member of the local Administrators group on the Data Mover.  
**Note:** To access the Server Manager as someone else or from another domain, the username or group should be added to that Data Mover’s Administrators local group by using User Manager for Domains. |
| 2.   | Click Start, and then select **Programs ➤ Administrative Tools ➤ Server Manager**.  
The **Server Manager** window displays a list of servers in the domain. |
Access Event Viewer

Use this procedure to open Event Viewer and select a CIFS server to view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click Start, and then select Programs ➤ Administrative Tools ➤ Event Viewer.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Event Viewer screenshot" /></td>
</tr>
<tr>
<td>2.</td>
<td>From the Log menu, select Select Computer.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Select Computer window" /></td>
</tr>
<tr>
<td>3.</td>
<td>In the Computer field, type the UNC name of the Data Mover's CIFS server (for example, \DM101) or the CIFS server's IP address, and then click OK. The User Manager window displays the default groups for this Data Mover.</td>
</tr>
</tbody>
</table>
Create local groups on a Data Mover using User Manager

For Windows NT, use the following procedure to add a local group to a Data Mover.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open User Manager for the CIFS server.</td>
</tr>
<tr>
<td></td>
<td><em>Access User Manager for Domains on page 44</em> provides instructions on opening User Manager.</td>
</tr>
<tr>
<td>2.</td>
<td>From the User menu, select New Local Group.</td>
</tr>
<tr>
<td>3.</td>
<td>In the New Local Group window, type the name of the local group in the Name field.</td>
</tr>
<tr>
<td></td>
<td>Optionally, type a description in the Description field.</td>
</tr>
<tr>
<td>4.</td>
<td>Click Add.</td>
</tr>
<tr>
<td></td>
<td>The Add Users and Groups window appears.</td>
</tr>
<tr>
<td>5.</td>
<td>Click the down arrow in the List Names From list box to display the list of domains.</td>
</tr>
<tr>
<td>6.</td>
<td>Select a domain. The Names field displays the users and global groups in this domain.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| 7.   | Select the users or global groups to add to the local group and click Add. Each selected name appears in the **Add Names** field.  
To add only selected users from a global group, do the following:  
1. Select the global group.  
2. Click **Members**. The **Global Group Membership** window lists all members of this group.  
3. Select the users to add, and then click **Add**. The users are added to the local group, and their names appear in the **Add Names** field in the **Add Users and Groups** window. |
| 8.   | When you have finished, click **OK**.  
The added users and groups appear in the **Members** field of the **New Local Group** window. |
| 9.   | Click **OK** to create the local group. |
### Assign user rights using User Manager

For Windows NT, use this procedure to set user rights on the Data Mover.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open User Manager for the CIFS server. &lt;br&gt;Access User Manager for Domains on page 44 provides instructions on opening User Manager.</td>
</tr>
<tr>
<td>2.</td>
<td>From the Policies menu, select User Rights.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the access right to assign to the local group by clicking the down arrow in the Right list box. &lt;br&gt;For example, to assign the right to take ownership of files, click the down arrow, and then select Take ownership of files or other objects. &lt;br&gt;Note: Click Show Advanced User Rights to display all possible user rights.</td>
</tr>
<tr>
<td>4.</td>
<td>Click Add. The Add Users and Groups window appears.</td>
</tr>
<tr>
<td>5.</td>
<td>Click the down arrow in the List Names From list box, and then select the UNC name of the Data Mover's CIFS service (for example, \DM101). &lt;br&gt;The list of local groups with accounts on the Data Mover appears in the Names field.</td>
</tr>
<tr>
<td>6.</td>
<td>Select the local group name, and then click Add. &lt;br&gt;The local group appears in the Add Names field.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| 7.   | Click OK.  
The local group appears in the **Grant To** field of the **User Rights Policy** window. |
| 8.   | Repeat steps 3 through 7 for each access right to grant to the local group. |
| 9.   | When you have finished assigning rights, click **OK** in the **User Rights Policy** window. |
Create shares and set ACLs using Server Manager

After you create a CIFS service on a Data Mover and add the Data Mover to the domain, use the Windows NT Server Manager for Domains to create shares and set ACLs on shares.

**Before you begin**

To create shares with Server Manager, you must:

- Have assigned UNIX UIDs and GIDs to CIFS users and groups. *Configuring and Managing CIFS on Celerra* and *Configuring Celerra User Mapping* provides detailed information about how to assign UIDs and GIDs.
- Have mounted the file system and created directories you want to share.
- Be the Administrator or a user who is a member of the Administrators local group on a Data Mover for the domain to which the Data Mover belongs. To use the Windows NT Server Manager as someone else or from another domain, the username or group should be added to that Data Mover’s Administrators local group by using User Manager for Domains.

**Procedure**

**Note:** Shares created through Windows administrative tools are accessible only from the NetBIOS name used by the Windows client. If you want the share to be globally accessible by all NetBIOS names, create a share with the Celerra server_export command and do not specify the netbios=<netbiosName> option.

For Windows NT, use this procedure to create a share on a Data Mover.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Open Server Manager for the CIFS server.  
      | *Access Server Manager for Domains on page 46* provides instructions on opening Server Manager. |
### Action Steps

2. Select a CIFS server, and then from the **Computer** menu, select **Shared Directories**. The **Shared Directories** window displays the shares on the Data Mover.

   ![Shared Directories](image)

   **Shared Directories**

   Shared Directories on \dn112-cge0:

   - `C$`: C:\
   - `CHECK$`: C:\etc
   - `IPC$`: C:\etc
   - `ufs1`: C:\ufs1
   - `ufs2`: C:\ufs2

   ![New Share](image)

   **New Share**

   - **Share Name**: 
   - **Path**: 
   - **Comment**: 

   ![User Limit](image)

   **User Limit**

   - **Maximum Allowed**
   - **Allow**: Users

3. Click **New Share**.

4. In the **Share Name** field, type the name of the share.

   The Celerra Network Server supports only ASCII share names. The name length is typically limited to 12 bytes, but if Unicode is enabled, the limit is 240 bytes.

5. In the **Path** field, type the pathname of the share on the local machine.

   For example, to create the share `\News` under the `\Events` directory on the C: drive, type `C:\Events\News`. On a Data Mover, the local path name always starts with `C:`.

   **Note**: Create and mount the directory on the Data Mover before executing this step.

6. Ensure that the **Maximum Allowed** button in **User Limit** is selected.
To set ACLs on the share, click Permissions. The Access Through Share Permissions window displays the default permissions for this share.

8. Do one of the following:
   - To modify the ACLs for a displayed group or user, select the group or user, select the access in the Type of Access field, and click OK.
   - To add a group or user, click Add to display the Add Groups or Users window. Add the group or user you want to give access to the share, click Add, and click OK. You can then modify the permissions.
   - To delete a group or user, select the group or user, and then click Remove.

9. When you have completed the assignment of ACLs, click OK to return to the New Share window.

   Note: For CIFS users, the ACLs you create override any base ACLs on the file system.

10. Click OK to complete the share creation.

Monitor Data Mover connections and resource usage using Server Manager

You can use Server Manager for Domains to:
   - Monitor users on the Data Mover on page 55
   - Monitor access to shares on the Data Mover on page 57
Monitor use of Data Mover resources on page 58

Monitor users on the Data Mover

For Windows NT, use this procedure to monitor the number of users connected to a CIFS server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open Server Manager for the CIFS server you want to monitor. Access Server Manager for Domains on page 46 provides instructions on opening Server Manager.</td>
</tr>
<tr>
<td>2.</td>
<td>From the <strong>Computer</strong> menu, select <strong>Properties</strong>. The <strong>Properties for</strong> window appears, where the system name appears in the window name.</td>
</tr>
</tbody>
</table>

![Properties for dm112-cge0](image)
Click **Users**. The **Users Sessions** window appears, listing the users who have sessions on the specified Data Mover and the available network resources (such as shares).

### User Sessions on dm112-cge0

<table>
<thead>
<tr>
<th>Connected Users</th>
<th>Computer</th>
<th>Opens</th>
<th>Time</th>
<th>Idle</th>
<th>Guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>administrator</td>
<td>PLUTO</td>
<td>1</td>
<td>00:00</td>
<td>00:00</td>
<td>No</td>
</tr>
<tr>
<td>administrator</td>
<td>172.24.102.20</td>
<td>0</td>
<td>00:00</td>
<td>00:00</td>
<td>No</td>
</tr>
<tr>
<td>administrator</td>
<td>172.24.102.20</td>
<td>1</td>
<td>00:05</td>
<td>00:05</td>
<td>No</td>
</tr>
<tr>
<td>usr1</td>
<td>JUNO</td>
<td>1</td>
<td>00:08</td>
<td>00:05</td>
<td>No</td>
</tr>
</tbody>
</table>

**Connected Users:** 5

<table>
<thead>
<tr>
<th>Resource</th>
<th>Opens</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPC$</td>
<td>0</td>
<td>00:00</td>
</tr>
<tr>
<td>IPC$</td>
<td>0</td>
<td>00:01</td>
</tr>
<tr>
<td>ufs2</td>
<td>1</td>
<td>00:05</td>
</tr>
</tbody>
</table>

4. To force disconnections from the Data Mover, select the username and click **Disconnect** or **Disconnect All**.
Monitor access to shares on the Data Mover

For Windows NT, use this procedure to monitor access to shares on the CIFS server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open Server Manager for the CIFS server. Access Server Manager for Domains on page 46 provides instructions on opening Server Manager.</td>
</tr>
<tr>
<td>2.</td>
<td>From the Computer menu, select Properties.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Properties for dm112-cge0" /></td>
</tr>
<tr>
<td>3.</td>
<td>In the Properties window, click Shares. The Shared Resources window displays all active network resources (such as shares) available on the Data Mover, the number of users of the resource, and the path to the resource.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Shared Resources on BDC" /></td>
</tr>
<tr>
<td>4.</td>
<td>Click a resource to display the users connected to it.</td>
</tr>
</tbody>
</table>
To force disconnections from the resource, select the username, and then click Disconnect or Disconnect All.

### Monitor use of Data Mover resources

For Windows NT, use this procedure to monitor the use of Data Mover resources.

**Action**

1. Open Server Manager for the CIFS server.
   
   Access Server Manager for Domains on page 46 provides instructions on opening Server Manager.

2. From the Computer menu, select Properties.

   ![Properties for dm112-cge0](image)

   **Usage Summary**

   - Sessions: 3
   - Open Files: 1
   - File Locks: 0
   - Open Named Pipes: 0

   **Description:**

   EMC-SNAS.T5.3.5.2015

   ![Users Share In Use Replication Alerts](image)
Audit CIFS users and objects using Windows NT management interfaces

To audit CIFS users and objects:

- Specify the auditing policy on page 59
- Set the audit log parameters on page 61
- Change log file size on page 62
- View the audit events on page 64

Specify the auditing policy

To enable auditing on the Celerra Network Server, you must be an Administrator or a member of the Administrators local group on the Data Mover.
## Managing Windows NT

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>In the <strong>User Manager for Domains</strong> window, select <strong>Audit</strong> from the <strong>Policies</strong> menu.</td>
</tr>
<tr>
<td><img src="image" alt="Audit Policy" /></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>By default, <strong>Do Not Audit</strong> is selected. To enable auditing, select <strong>Audit These Events</strong>.</td>
</tr>
<tr>
<td><img src="image" alt="Audit Policy" /></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>For each supported object class you want to audit, select <strong>Success</strong> or <strong>Failure</strong>. <strong>Auditing on page 13</strong> lists the supported object classes</td>
</tr>
<tr>
<td>5.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>6.</td>
<td>Repeat steps 1 through 5 for each CIFS server you want to audit.</td>
</tr>
</tbody>
</table>
## Set the audit log parameters

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open Event Viewer for the CIFS server.  &lt;br&gt; <em>Access Event Viewer on page 47</em> provides instructions on opening Event Viewer.</td>
</tr>
<tr>
<td>2.</td>
<td>From the Log menu, select Log Settings. In the Event Log Settings dialog box, you can modify the Security, System, or Application log settings. &lt;br&gt; <em>Auditing on page 13</em> lists the default log settings.</td>
</tr>
<tr>
<td>3.</td>
<td>From the Change Settings for list box, select a log.</td>
</tr>
<tr>
<td>4.</td>
<td>The Maximum Log Size field is typically locked. You cannot modify this value until you complete the procedure <em>Change log file size on page 62</em>.</td>
</tr>
<tr>
<td>5.</td>
<td>In the Event Log Wrapping area, specify the log wrapping setting: &lt;br&gt; - Overwrite Events as Needed: Overwrites the earliest events in the event log after the file size specified in step 4 is reached. &lt;br&gt; - Overwrite Events Older than (&lt;n&gt;) Days: Overwrites events older than the specified number of days. Use the arrows to set the limit or click the field and type a value. The file size specified in step 4 is not exceeded. New events will not be added if the maximum log size is reached and there are no events older than this period. &lt;br&gt; - Do Not Overwrite Events: If the limit specified in step 4 is reached, no new events are written until the log is cleared.</td>
</tr>
<tr>
<td>6.</td>
<td>Click OK.</td>
</tr>
<tr>
<td>7.</td>
<td>Repeat steps 2 through 6 to modify each log file.</td>
</tr>
</tbody>
</table>
## Change log file size

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>On the Windows NT system used to manage the Data Movers, select Run from the Start menu.</td>
</tr>
<tr>
<td></td>
<td><img src="image1.png" alt="Run dialog box" /> Type regedt32.exe, and then click OK. The Registry Editor appears:</td>
</tr>
<tr>
<td></td>
<td><img src="image2.png" alt="Registry Editor" /></td>
</tr>
<tr>
<td>2.</td>
<td>Type regedt32.exe, and then click OK. The Registry Editor appears:</td>
</tr>
<tr>
<td></td>
<td><img src="image3.png" alt="Registry Editor" /></td>
</tr>
<tr>
<td>3.</td>
<td>From the Registry menu, select Select Computer. The Select Computer dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>If you receive an autorefresh warning message, click OK to continue.</td>
</tr>
<tr>
<td>4.</td>
<td>In the Computer Name field, type the NetBIOS name of the Data Mover, and then click OK.</td>
</tr>
<tr>
<td></td>
<td>The Registry Editor displays the updated information for the Data Mover.</td>
</tr>
<tr>
<td>5.</td>
<td>Navigate to the following key:</td>
</tr>
<tr>
<td></td>
<td>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\security\File</td>
</tr>
<tr>
<td>6.</td>
<td>Right-click the File icon. The Edit File Value window displays the absolute path for the security log file (C:\security.evt by default) in the File field.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| 7.   | In the **File** field, edit the path where you want to store the log file. For example,  
\[ C:\{mntpt}\{directory_name}\security.evt \]  
Where: 
\[ {mntpt} = \text{mount point of the file system (not the root file system)} \]  
\[ {directory_name} = \text{name of the directory that contains the log file} \]  
Example  
\[ C:\CIFS\_FS\_1\WinNTlogs\security.evt \]  
⚠️ Do not change the name of the log file. |
| 8.   | Click **OK**. |
| 9.   | Select **Exit** from the **Registry** menu. Changes take effect immediately. |
View the audit events

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Open Event Viewer for the CIFS server.  
      | *Access User Manager for Domains on page 44* provides instructions on opening Event Viewer. |
| 2.   | Double-click an event to view the event detail. |
| 3.   | Click Close to close the Event Detail window. |
| 4.   | Repeat steps 2 and 3 for each event of interest. |
Disable auditing using User Manager

To disable auditing modify the audit policies in User Manager for Domains.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Open User Manager for the CIFS server.  
      | Access User Manager for Domains on page 44 provides instructions on opening User Manager. |
| 2.   | In the **User Manager for Domains** window, select **Audit** from the **Policies** menu. |
|      | ![Audit Policy](image) |
| 3.   | Do one of the following:  
      | • To suspend auditing on all object classes, select **Do Not Audit**, and then click **OK**.  
      | • To suspend auditing on individual object classes, clear **Success** or **Failure** for each object class, and then click **OK**. |
| 4.   | Repeat steps 1 through 3 for each CIFS server to audit. |
Enable auditing on a folder or file

Use this procedure to enable auditing on a folder or file stored on the Celerra Network Server (or, you can use the My Computer interface on the desktop).

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Ensure that auditing is enabled on the share in which the file or folder you want to audit resides. Specify the auditing policy on page 59 provides details on how to enable auditing on a Celera-resident share.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Start</strong>, and then select <strong>Programs ➤ Windows NT Explorer</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>In the <strong>All Folders</strong> panel, navigate to the folder or file you want to audit.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>4.</td>
<td>Right-click the folder or file, and then select Properties from the shortcut menu.</td>
</tr>
</tbody>
</table>

**test.txt Properties**

- **Type:** Text Document
- **Location:** \dm1\12-cge0\uts2
- **Size:** 14 bytes (14 bytes)
- **MS-DOS name:** test.txt
- **Created:** Friday, June 11, 2004 4:05:23 PM
- **Modified:** Friday, June 11, 2004 4:05:30 PM
- **Accessed:** Friday, June 11, 2004 4:14:07 PM

**Attributes:**
- Read-only
- Archive
- Hidden
- System
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Click the <strong>Security</strong> tab.</td>
</tr>
</tbody>
</table>

**test.txt Properties**

- **Permissions**
  - View or set permission information on the selected item(s).
  - Permissions

- **Auditing**
  - View or set auditing information on the selected item(s).
  - Auditing

- **Ownership**
  - View or take ownership of the selected item(s).
  - Ownership

[OK] [Cancel] [Apply]
6. Click Auditing. The **File Auditing** or **Directory Auditing** window appears.

Enable auditing on a folder or file.
### Managing Windows NT

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td><strong>Click Add.</strong> The <strong>Add Users and Groups</strong> window appears.</td>
</tr>
</tbody>
</table>

#### Add Users and Groups

- **List Names From:** `\dm112-cge0`

#### Names:

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Operators</td>
<td>Account operators of the machine</td>
</tr>
<tr>
<td>Administrators</td>
<td>Members can fully administer the machine</td>
</tr>
<tr>
<td>Authenticated Users</td>
<td>All authenticated users</td>
</tr>
<tr>
<td>Backup Operators</td>
<td>Members can bypass file security to back up data</td>
</tr>
<tr>
<td>Everyone</td>
<td>All Users</td>
</tr>
<tr>
<td>Guests</td>
<td>Users granted guest access to the computer</td>
</tr>
<tr>
<td>INTERACTIVE</td>
<td>Users accessing this object locally</td>
</tr>
<tr>
<td>NETWORK</td>
<td>Users accessing this object remotely</td>
</tr>
</tbody>
</table>

#### Add Names:

- **Everyone**

#### Buttons:

- **Add**
- **Show Users**
- **Members...**
- **Search...**
- **OK**
- **Cancel**
- **Help**
8. You can audit activity on this directory or file by local group or by individual user, as follows:
   
   To audit activity by local group:
   1. Select the local group.
   2. Click **Add**. The local group is added to the **Add Names** box.
   3. Repeat steps 1 and 2 for each local group to audit.
   4. When you have finished, click **OK** to return to the **Directory Auditing** window.

   To audit activity by user:
   1. Select the local group that contains the user.
   2. Click **Show Users**. The users in the selected local group appear at the bottom of the **Names** field. You might need to scroll down to view them.
   3. Select the user.
   4. Click **Add**. The user is added to the **Add Names** box.
   5. Repeat steps 1 through 5 for each user to audit.
   6. When you have finished, click **OK** to return to the **File Auditing** window.

   **Note:** You can audit local groups and domain users.

9. After you add the local groups and users, select the events to audit, as follows:
   
   1. In the **File Auditing** window, select the events for the folder or file. You can select Read, Write, Execute, Delete, Change Permissions, or Take Ownership, and you can choose to audit Success or Failure for each.
   2. Click **OK**. The **File Auditing** window closes.
   3. Click **OK** in the **Properties** window to apply the changes and close the window.
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, please contact your EMC Customer Support Representative.

- Where to get help on page 74
- EMC E-Lab Interoperability Navigator on page 74
- EMC Training and Professional Services on page 74
Where to get help

To obtain EMC support, product, and licensing information:

**Product information**

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

**Troubleshooting**

For troubleshooting information, go to Powerlink, search for Celerra Tools, and select Celerra Troubleshooting from the navigation panel on the left.

**Technical support**

For technical support, go to EMC Customer Service on Powerlink. After logging in to the Powerlink website, go to Support ➤ Request Support. To open a service request through Powerlink, you must have a valid support agreement. Contact your EMC Customer Support Representative for details about obtaining a valid support agreement or to answer any questions about your account.

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

*Problem Resolution Roadmap for EMC Celerra* contains additional information about using Powerlink and resolving problems.

**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 at http://Powerlink.EMC.com. After logging in to Powerlink, go to Support ➤ Interoperability and Product LifeCycle Information ➤ E-Lab Interoperability Navigator.

**EMC Training and Professional Services**

EMC Customer Education courses help you learn how EMC storage products work together within your environment in order 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 Powerlink at http://Powerlink.EMC.com for course and registration information.

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

**CIFS server**
Logical server using the CIFS protocol to transfer files. A Data Mover can host many instances of a CIFS server. Each instance is referred to as a CIFS server.

**CIFS service**
CIFS server process running on the Data Mover that presents shares on a network as well as on Microsoft Windows-based computers.

**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.

**D**

**Data Mover**
In a Celerra Network Server, a cabinet component running its own operating system that retrieves data from a storage device and makes it available to a network client. This is also referred to as a blade. A Data Mover is sometimes internally referred to as DART since DART is the software running on the platform.

**F**

**file system**
Method of cataloging and managing the files and directories on a storage system.

**N**

**network file system (NFS)**
Network file system (NFS) is a network file system protocol allowing a user on a client computer to access files over a network as easily as if the network devices were attached to its local disks.
**Network Information Service (NIS)**

Distributed data lookup service that shares user and system information across a network, including usernames, passwords, home directories, groups, hostnames, IP addresses, and netgroup definitions.
A
access rights
   Windows 2000 22
   Windows NT 44
ACLs setting
   for Windows 2000 groups 24
   for Windows NT groups 52
Windows 2000
   auditing 30
   changing log file size 34
   CIFS users on Data Mover 38
   setting log parameters 33
   specifying policy 31
   viewing audit events 37
Windows NT
   CIFS users on Data Mover 52
   disabling 65
   enabling for folder or file 66
   setting log parameters 61
   specifying policy 59
   viewing events 64

D
creating local groups
   for Windows NT 48
editing Registry
   for Windows 2000 34
   for Windows NT 62
Windows 2000
   monitoring shares 28
   monitoring user 27
Windows NT
   monitoring user 55
disabling
   user auditing for Windows 2000 39
   (continued)
   user auditing for Windows NT 65

E
EMC E-Lab Navigator 74
   enabling
      auditing for folder or file for Windows NT 66
Event Viewer
   Windows 2000 37
   Windows NT 64

F
files, monitoring on Data Mover for Windows 2000
   26

L
Windows 2000
   setting user rights 20, 22
Windows NT
   creating local groups on Data Mover 48
   setting user rights 50
log file, changing size
   for Windows 2000 34
   for Windows NT 62

M
MMC, opening 18
Windows 2000
   files on Data Mover 29
   shares on Data Mover 28
   users on Data Mover 27
Windows NT
   shares on Data Mover 57
moniting (continued)
Windows NT (continued)
users on Data Mover 55

R
Registry, editing
Windows 2000 34
Windows NT 62

S
security log file, changing size
for Windows 2000 34
for Windows NT 62
Server Manager for Domains 46
Windows 2000
creating 24
monitoring on Data Mover 28
setting ACLs 24
Windows NT
creating 52
monitoring on Data Mover 57
setting 
ACLs 52

T
tools
Event Viewer
Windows 2000 37
Windows NT 64
MMC 13
Server Manager for Domains 46
User Manager for Domains 44

U
Windows 2000
disabling 39
viewing events 37
Windows NT
disabling 65

user auditing (continued)
Windows NT (continued)
viewing events 64
User Manager for Domains 44
auditing
from Windows 2000 38
from Windows NT 59

W
Windows 2000
changing log file size 34
creating shares 24
disabling user auditing 39
MMC 18
monitoring
files on Data Mover 29
shares on the Data Mover 28
users on the Data Mover 27
setting
ACLs on shares 24
log parameters 33
user rights 22
specifying audit policy 31
Windows NT
ACLs
setting 50, 52, 61
auditing a file or folder 66
changing log file size 62
creating
local groups on the Data Mover 48
shares 57
disabling user auditing 65
Event Viewer 47
monitoring
shares on the Data Mover 57
users on the Data Mover 55
Server Manager for Domains 46
setting 50, 52, 61
audit log parameters 61
user rights 50
specifying audit policy 59
User Manager for Domains 44
viewing audit events 64