FUJITSU Storage
ETERNUS DX S4/S3 series
Hybrid Storage Systems

Configuration Guide (NAS)

System configuration design/basic settings for NAS environments
# Table of Contents

## 1. NAS System Design

- Unified Configuration .................................................................................................................... 11
- Supported Protocols...................................................................................................................... 12
  - CIFS ....................................................................................................................................................................... 12
  - NFS ....................................................................................................................................................................... 13
  - FTP/FPX ................................................................................................................................................................. 13
- Operating Environment for Clients ................................................................................................ 14
  - Confirmed OS ........................................................................................................................................................ 14
- NAS System (NAS Volume Management) ...................................................................................... 16
  - NAS File Systems ................................................................................................................................................... 18
  - NAS Volume .......................................................................................................................................................... 20
  - Block Size .............................................................................................................................................................. 23
- File System Specification ............................................................................................................... 24
- Data Encryption ............................................................................................................................ 26

## 2. Designing NAS Operations

- NAS Server Name (Host Name) ..................................................................................................... 27
- User Management ........................................................................................................................ 28
  - Authentication Server ........................................................................................................................................... 29
  - Fixed User Account ................................................................................................................................................ 34
  - Local User Authentication ............................................................................................................................... 34
- Access Control (ACL Function) ....................................................................................................... 36
  - Access Control in a CIFS Environment .................................................................................................................... 37
  - Access Control in an NFS Environment .................................................................................................................. 37
  - Access Control in a Shared CIFS/NFS Environment ................................................................................................. 38
- CIFS Access Permission Settings .................................................................................................... 38
- File Sharing ................................................................................................................................... 39
  - CIFS Operation ....................................................................................................................................................... 41
  - NFS Operation ....................................................................................................................................................... 45
- Home Directories .......................................................................................................................... 47
- Quota ............................................................................................................................................ 48
3. Connection Interface Configuration .............................................................. 67
   NAS Interface (NIC-CA) .................................................................................. 67
   Redundant Method .......................................................................................... 70
      Single Path Connection .................................................................................. 70
      Multipath Connection (Active-Active Connection) .......................................... 70
      Bonding .......................................................................................................... 73
   Network Path Control ....................................................................................... 78
   FTP/FXP ............................................................................................................ 79

4. NAS Environment Configuration ............................................................... 81
   Thin Provisioning Pool (TPP) Creation ............................................................ 83
   NAS Volume Creation ...................................................................................... 84
   Bonding Settings ............................................................................................. 86
   NAS Interface Settings ................................................................................... 89
   VLAN Settings .................................................................................................. 92
   DNS Server Settings ........................................................................................ 93
   NAS Server Name Settings ............................................................................... 95
   Authentication Server Settings ....................................................................... 97
   Local User Authentication Settings ............................................................... 100
      Local Group Creation ................................................................................... 100
      Local User Creation ..................................................................................... 101
# Table of Contents

- Authentication Method Change ................................................................. 104
- Shared Folder Creation (CIFS/NFS) .......................................................... 105
- Home Directories .................................................................................. 110
- FTP/FXP Settings ................................................................................ 113
  - FTP Setting ......................................................................................... 113
  - FXP Setting ....................................................................................... 114
- Quota Settings ...................................................................................... 115
- Snapshot Settings ................................................................................ 121
  - Basic Settings for Snapshot .............................................................. 121
  - Snapshot Restoration ...................................................................... 129
- Audit Log Setup .................................................................................... 132
- Meta Cache Distribution Settings ......................................................... 135
  - Manual Execution of Meta Cache Distribution .................................. 135
  - Automatic Execution of Meta Cache Distribution ............................ 136

5. **Packet Trace Acquisition Settings** .................................................. 138

6. **System Status Check** ................................................................. 142
  - Checking the Shared Folders ............................................................ 142
  - Checking the Home Directories ....................................................... 144
  - Checking the NAS Interfaces .......................................................... 145
  - Checking the NAS Environment Settings ....................................... 147
  - Checking the Quota Management .................................................... 149
  - Checking the Snapshots ................................................................. 151
  - Checking the Backup Information .................................................. 152

7. **How to Access from Clients** ...................................................... 153
  - Access from CIFS Clients ............................................................... 153
  - Access from NFS Clients ............................................................... 154

8. **Backup/Restore Settings** ............................................................ 156
  - Backup Settings ................................................................................ 156
  - Backup .............................................................................................. 156
## Table of Contents

Restoration ................................................................................................................................. 156

9. **Backup Software Settings** 157

   Notes When Using Arcserve Backup ...................................................................................... 157
   Notes When Using NetVault SmartDisk ................................................................................. 158
   Notes When Using NetWorker .............................................................................................. 158
   Notes When Using NetBackup ............................................................................................. 159
   Notes When Using ETERNUS SF TSM...................................................................................... 159

10. **Troubleshooting** 160

    Configuration Errors .............................................................................................................. 160
    Operation Errors .................................................................................................................. 164
    Required Information for Inquiries ....................................................................................... 170

A. **Function Specification List** 172

   NAS Volume Specifications .................................................................................................... 172
   File System Specifications .................................................................................................... 174
   Available Functions for Each Software ................................................................................. 176

B. **Snapshot Configurable NAS Volume Capacity (Guideline)** 178

C. **Audit Log Messages** 184

   Audit Log Format .................................................................................................................. 184
   Output Examples of the Audit Logs ....................................................................................... 186

D. **Notes for Data Migrations** 188

   Actions to Take Before Data Migrations ................................................................................ 188
   Property Information of the Files that are Migrated from the Windows OS ............................ 189

E. **Firmware Release Information** 191
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SAN/NAS Connection Diagrams</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>NAS File Systems</td>
<td>17</td>
</tr>
<tr>
<td>3</td>
<td>Initial Deployment of Meta Cache</td>
<td>20</td>
</tr>
<tr>
<td>4</td>
<td>How Free Space Is Recognized</td>
<td>25</td>
</tr>
<tr>
<td>5</td>
<td>Authentication Server</td>
<td>29</td>
</tr>
<tr>
<td>6</td>
<td>Process for Acquiring the Authentication Information (CIFS)</td>
<td>32</td>
</tr>
<tr>
<td>7</td>
<td>Process for Acquiring the Authentication Information (NFS)</td>
<td>33</td>
</tr>
<tr>
<td>8</td>
<td>Home Directories</td>
<td>47</td>
</tr>
<tr>
<td>9</td>
<td>Quota (for Each User or Group)</td>
<td>48</td>
</tr>
<tr>
<td>10</td>
<td>Quota (for Each Shared Folder)</td>
<td>49</td>
</tr>
<tr>
<td>11</td>
<td>Snapshot</td>
<td>51</td>
</tr>
<tr>
<td>12</td>
<td>Packet Trace Acquisition</td>
<td>54</td>
</tr>
<tr>
<td>13</td>
<td>Audit Log</td>
<td>56</td>
</tr>
<tr>
<td>14</td>
<td>Meta Cache Distribution</td>
<td>57</td>
</tr>
<tr>
<td>15</td>
<td>Single Path Connection (When a NAS Connection Is Used)</td>
<td>70</td>
</tr>
<tr>
<td>16</td>
<td>Multipath Connection (Active-Active Connection) (When a NAS Connection Is Used)</td>
<td>72</td>
</tr>
<tr>
<td>17</td>
<td>Bonding</td>
<td>73</td>
</tr>
<tr>
<td>18</td>
<td>Multipath Connection When Using Bonding</td>
<td>76</td>
</tr>
<tr>
<td>19</td>
<td>FTP/FXP</td>
<td>79</td>
</tr>
<tr>
<td>20</td>
<td>Bonding Settings</td>
<td>86</td>
</tr>
<tr>
<td>21</td>
<td>Example Schedule Settings for Snapshots</td>
<td>122</td>
</tr>
<tr>
<td>22</td>
<td>Example of Creating Operation Volume and NAS Snapshot Destination Volume</td>
<td>123</td>
</tr>
<tr>
<td>23</td>
<td>RAID Group Creation</td>
<td>124</td>
</tr>
<tr>
<td>24</td>
<td>Snapshot Destination Volume (SDPV) Creation</td>
<td>124</td>
</tr>
<tr>
<td>25</td>
<td>Snapshot Restoration</td>
<td>129</td>
</tr>
<tr>
<td>26</td>
<td>Operational Configuration (When a Backup Is Performed Using QuickOPC with OPC Restoration)</td>
<td>178</td>
</tr>
<tr>
<td>27</td>
<td>Operational Configuration (When a Secondary Backup Is Performed Using a Backup between ETERNUS DX Storage Systems (REC))</td>
<td>181</td>
</tr>
</tbody>
</table>
List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Number of File Systems</td>
<td>16</td>
</tr>
<tr>
<td>Table 2</td>
<td>System Volumes</td>
<td>19</td>
</tr>
<tr>
<td>Table 3</td>
<td>Expanded System Volume</td>
<td>19</td>
</tr>
<tr>
<td>Table 4</td>
<td>Maximum Capacity of Files and Volumes for Each Block Size</td>
<td>23</td>
</tr>
<tr>
<td>Table 5</td>
<td>Maximum Number of Quota Settings</td>
<td>49</td>
</tr>
<tr>
<td>Table 6</td>
<td>Maximum Number of Generations (per ETERNUS DX or Volume) and Number of Target Volumes for Snapshots</td>
<td>50</td>
</tr>
<tr>
<td>Table 7</td>
<td>Required Capacity of SDV/SDPV (Guideline)</td>
<td>51</td>
</tr>
<tr>
<td>Table 8</td>
<td>Specifications of the Client Resource Deallocation Function (through ETERNUS CLI)</td>
<td>59</td>
</tr>
<tr>
<td>Table 9</td>
<td>Operations That Are Stopped during a Re-Notification Grace Period of the NFS File Lock Information</td>
<td>61</td>
</tr>
<tr>
<td>Table 10</td>
<td>Maximum Number of File Locks That Can Be Taken Over (per Controller)</td>
<td>61</td>
</tr>
<tr>
<td>Table 11</td>
<td>Performance Requirements (during Random Access) for the ETERNUS DX</td>
<td>63</td>
</tr>
<tr>
<td>Table 12</td>
<td>Number of Available NAS Interfaces (per ETERNUS DX)</td>
<td>67</td>
</tr>
<tr>
<td>Table 13</td>
<td>NAS Firewall</td>
<td>68</td>
</tr>
<tr>
<td>Table 14</td>
<td>Estimated Required Time for Failover or Failback</td>
<td>72</td>
</tr>
<tr>
<td>Table 15</td>
<td>Features of the Bonding Operation Mode</td>
<td>74</td>
</tr>
<tr>
<td>Table 16</td>
<td>Recovery Requirements After a Link Down State for All Member Ports</td>
<td>75</td>
</tr>
<tr>
<td>Table 17</td>
<td>Configuration Errors</td>
<td>160</td>
</tr>
<tr>
<td>Table 18</td>
<td>Operation Errors</td>
<td>164</td>
</tr>
<tr>
<td>Table 19</td>
<td>Maximum Number of TPPs/NAS TPVs (NAS Volumes) That Can Be Created (For the ETERNUS DX100 S4/DX200 S4 and the ETERNUS DX500 S4/DX600 S4)</td>
<td>172</td>
</tr>
<tr>
<td>Table 20</td>
<td>Maximum Number of TPPs/NAS TPVs (NAS Volumes) That Can Be Created (For the ETERNUS DX100 S3/DX200 S3 and the ETERNUS DX500 S3/DX600 S3)</td>
<td>173</td>
</tr>
<tr>
<td>Table 21</td>
<td>File System Specifications (Max.)</td>
<td>174</td>
</tr>
<tr>
<td>Table 22</td>
<td>Available Functions for Operation Management Interfaces</td>
<td>176</td>
</tr>
<tr>
<td>Table 23</td>
<td>Guidelines for Snapshot Configurable NAS Volume Capacity (When QuickOPC Is Used)</td>
<td>179</td>
</tr>
<tr>
<td>Table 24</td>
<td>Guidelines for Snapshot Configurable NAS Volume Capacity (When QuickOPC and REC Are Used)</td>
<td>181</td>
</tr>
<tr>
<td>Table 25</td>
<td>Details of Each Item in Audit Log Messages</td>
<td>184</td>
</tr>
<tr>
<td>Table 26</td>
<td>Details That Are Displayed in “syscall”</td>
<td>185</td>
</tr>
<tr>
<td>Table 27</td>
<td>Actions to Take Before Data Migrations</td>
<td>188</td>
</tr>
<tr>
<td>Table 28</td>
<td>Inheritable Property Information for Migrations from Windows OS</td>
<td>189</td>
</tr>
<tr>
<td>Table 29</td>
<td>Release Information List</td>
<td>191</td>
</tr>
</tbody>
</table>
Fujitsu would like to thank you for purchasing the FUJITSU Storage ETERNUS DX100 S4/DX200 S4, ETERNUS DX500 S4/DX600 S4, ETERNUS DX100 S3/DX200 S3, ETERNUS DX500 S3/DX600 S3 (hereinafter collectively referred to as ETERNUS DX).

The ETERNUS DX is a unified storage system that is designed to be used as a SAN connection type storage system for Fujitsu servers (Fujitsu SPARC Servers, PRIMEQUEST, or PRIMERGY) or non-Fujitsu servers and as a network connection type storage system for servers and client PCs.

This manual provides the system design to use an ETERNUS DX in a NAS environment and explains how to configure the NAS environment.

This manual is intended for use of the ETERNUS DX in regions other than Japan.

This manual applies to controller firmware versions V10L14 to V10L87.

The supported functions and specifications depend on the controller firmware version of the ETERNUS DX. For the firmware release information, refer to "E. Firmware Release Information" (page 191).

Nineteenth Edition
April 2019

Trademarks

Third-party trademark information related to this product is available at:

About This Manual

Intended Audience

This manual is intended for field engineers who configure NAS environments in the ETERNUS DX or for system administrators.

Related Information and Documents

The latest version of this manual and the latest information for your model are available at:

Refer to the following manuals of your model as necessary:
* ETERNUS Web GUI User's Guide*
* ETERNUS CLI User's Guide*
* Design Guide (Basic)*
* Configuration Guide (Basic)*
* Operation Guide (Basic)*
Document Conventions

- **Third-Party Product Names**
  - Oracle Solaris may be referred to as "Solaris", "Solaris Operating System", or "Solaris OS".
  - Microsoft® Windows Server® may be referred to as "Windows Server".

- **Notice Symbols**
  The following notice symbols are used in this manual:
  - Indicates information that you need to observe when using the ETERNUS storage system. Make sure to read the information.
  - Indicates information and suggestions that supplement the descriptions included in this manual.

- **Icons Used in This Manual**
  The following icons show the availability of the settings for each software.
  - The black icon indicates that the setting is available for the relevant software.
  - Icons with colors other than black indicate that the setting is not available for the relevant software.

  **Example**
  The following example shows that the setting is available with ETERNUS CLI, ETERNUS SF Storage Cruiser, and ETERNUS SF Express.

  ![Example Icon]

- **Software Icons**
  - **GUI**: ETERNUS Web GUI
  - **CLI**: ETERNUS CLI
  - **SC**: ETERNUS SF Storage Cruiser (Web Console)
  - **EXP**: ETERNUS SF Express (Web Console)
  - **ACM**: ETERNUS SF AdvancedCopy Manager (Web Console)
  - **CLI**: ETERNUS SF (CLI)
Warning Signs

Warning signs are shown throughout this manual in order to prevent injury to the user and/or material damage. These signs are composed of a symbol and a message describing the recommended level of caution. The following explains the symbol, its level of caution, and its meaning as used in this manual.

This symbol indicates the possibility of serious or fatal injury if the ETERNUS DX is not used properly.

This symbol indicates the possibility of minor or moderate personal injury, as well as damage to the ETERNUS DX and/or to other users and their property, if the ETERNUS DX is not used properly.

This symbol indicates IMPORTANT information for the user to note when using the ETERNUS DX.

The following symbols are used to indicate the type of warnings or cautions being described.

The triangle emphasizes the urgency of the WARNING and CAUTION contents. Inside the triangle and above it are details concerning the symbol (e.g. Electrical Shock).

The barred "Do Not..." circle warns against certain actions. The action which must be avoided is both illustrated inside the barred circle and written above it (e.g. No Disassembly).

The black "Must Do..." circle indicates actions that must be taken. The required action is both illustrated inside the black disk and written above it (e.g. Unplug).

How Warnings are Presented in This Manual

A message is written beside the symbol indicating the caution level. This message is marked with a vertical ribbon in the left margin, to distinguish this warning from ordinary descriptions.

A display example is shown here.

Example warning

Warning level indicator

Warning type indicator

Warning details

Warning layout ribbon

To avoid damaging the ETERNUS storage system, pay attention to the following points when cleaning the ETERNUS storage system:
- Make sure to disconnect the power when cleaning.
- Be careful that no liquid seeps into the ETERNUS storage system when using cleaners, etc.
- Do not use alcohol or other solvents to clean the ETERNUS storage system.

CAUTION

Do
1. **NAS System Design**

This chapter describes the protocols and client OSs that are supported in a NAS environment of an ETERNUS DX, as well as the structure of a NAS system.

**Unified Configuration**

When using the ETERNUS DX as a unified storage system, install the Unified kit and the NAS interface (NIC-CA).

*Figure 1 SAN/NAS Connection Diagrams*
Supported Protocols

The ETERNUS DX supports Common Internet File System (CIFS), a file sharing protocol for Windows, and NFS, a file sharing protocol for UNIX/Linux. In addition to CIFS and NFS, the ETERNUS DX supports FTP/FXP.

NAS protocols other than CIFS, NFS, and FTP/FXP are not supported.

The CIFS protocol service for the ETERNUS DX is realized by using Samba software.

CIFS and NFS are client/server protocols that can perform file management such as exclusive control on the NAS side, which allows exclusive control over each file and simultaneous access. A file sharing environment with different OSs, such as Windows and UNIX/Linux, can be configured.

CIFS

The CIFS is a protocol that is used for file sharing in Windows system environments.

Files on the network can be shared.

■ SMB Version

The ETERNUS DX supports access from a Windows client using SMB1.0, SMB2.0, SMB2.1, SMB3.0, SMB3.0.2, or SMB3.1.1 protocol.

In addition, the following SMB functions are supported.

• SMB2.1 Large MTU
• SMB2.1 Unbuffered Handle
• SMB3.0 Large MTU
• SMB3.0 Encryption

The ETERNUS DX connects to Windows clients by using an SMB version that supports the protocol used by the Windows client for access.

When the SMB version is changed due to a controller firmware update on the ETERNUS DX, the change takes effect after the session is re-established.

Caution

During the design phase

If the controller firmware version is earlier than V10L61, the ETERNUS DX uses SMB1.0 to communicate with the Active Directory authentication server.

For this reason, disabling SMB1.0 in the Active Directory authentication server causes user authentication failures which in turn make the shared folder inaccessible.

Before disabling SMB1.0 of the Active Directory authentication server, update the ETERNUS DX controller firmware version to V10L61 or later.
### Symbolic Link

Creating and using symbolic links that are supported by SMB2.0, for directories/files in any shared folder (network drive) on the ETERNUS DX are available from the directories/files on the NTFS file system of the Windows client.

In addition, for shared folders created in shared CIFS/NFS environment, referencing and using the symbolic link for directories and files created by UNIX client from the Windows client are available.

Note that symbolic links between shared folders (network drives) are not supported (cannot be used from the Windows client).

### SMB Encryption

The ETERNUS DX provides a function to encrypt data communicated using SMB3.0 with an SMB protocol base. SMB Encryption is a function that encrypts file access communication but not the actual files.

SMB encryption can be enabled or disabled with ETERNUS Web GUI or ETERNUS CLI. Encryption is enabled for sessions that are established after enabling the encryption setting.

### Large MTU

The Maximum Transmission Unit (MTU) for communication using SMB3.0 can be extended from 64KB to 1,024KB. This enables effective utilization of the network bandwidth.

Large MTU is automatically enabled for communications that use SMB3.0. Changing the enable/disable setting is not possible.

### NFS

The Network File System (NFS) is a protocol that is used for file sharing in UNIX or Linux system environments. File sharing for NFS can be performed by mounting a shared directory from a client.

NFSv2, v3, and v4.0 are supported for the ETERNUS DX.

File lock using Network Lock Manager (NLM) v4 is supported.

For the NFSv4.0 protocol, the lease period and the grace period are each 100 seconds. In addition, the NFSv4.0 protocol supports stateful access.

#### Note

- The lease period indicates the time for the ETERNUS DX to determine whether the NFS client has stopped. During this period, resources in the NFS clients such as locks are retained in the ETERNUS DX.
- The grace period indicates a time to prevent the lock from becoming lost by notifying the NFS client that the NFS service has been restarted and securing time to reclaim the existing lock again.
- In the ETERNUS DX, the port that is used by the NFS client must be specified with port number 1023 or less.

### FTP/FXP

With File Transfer Protocol (FTP), the shared folder can be accessed. With File eXchange Protocol (FXP), data in the shared folder can be transferred between ETERNUS DX storage systems.
Operating Environment for Clients

The ETERNUS DX can be connected to OSs that support available protocols for the ETERNUS DX. For details on the protocols that are supported by the ETERNUS DX, refer to "Supported Protocols" (page 12). For NFS access, it is necessary for the client to use a port number of less than 1024.

The confirmed OS for NFSv4.0 can be connected to the ETERNUS DX.

Confirmed OS

The following OSs are confirmed to connect to the ETERNUS DX as a NAS client.

• The confirmed OSs with the CIFS protocol
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows 7
  - Windows 8.1
  - Windows 10

• The confirmed OSs with the NFSv3 protocol
  - Red Hat Enterprise Linux 5
  - Red Hat Enterprise Linux 6
  - Red Hat Enterprise Linux 7.0
  - Red Hat Enterprise Linux 7.1
  - Red Hat Enterprise Linux 7.2
  - Red Hat Enterprise Linux 7.3
  - Red Hat Enterprise Linux 7.4
  - Solaris 9
  - Solaris 10 1/13 (Update 11)
  - Solaris 11.2
  - Solaris 11.3
  - VMware vSphere 5.0 Update 3
  - VMware vSphere 5.1 Update 3
  - VMware vSphere 5.5 Update 3b
  - VMware vSphere 6.0 Update 1b
  - VMware vSphere 6.5
  - Oracle VM 3
  - AIX 7.1
  - HP-UX 11i v3

• The confirmed OSs with the NFSv4.0 protocol
  The confirmed OSs for the NFSv4.0 protocol are used as supported OSs.
  - Red Hat Enterprise Linux 6.7
  - Red Hat Enterprise Linux 6.8
- Red Hat Enterprise Linux 6.9
- Red Hat Enterprise Linux 7.0
- Red Hat Enterprise Linux 7.1
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Solaris 10 1/13 (Update 11)
- Solaris 11.2
- Solaris 11.3

The confirmed OSs with FTP / FXP
Regardless of the OS type, access is possible as long as an FTP client is used.

**Caution**

**During the design phase**
- Microsoft-provided Windows NFS service cannot be used.
- Mounting a CIFS shared folder from UNIX/Linux by specifying "cifs" in the "mount" command is not supported.
- When accessing with a Solaris OS client, there are combinations with the network environment where connections may not be possible. The following table shows connectivity.

<table>
<thead>
<tr>
<th>OS</th>
<th>Connectibility</th>
<th>IPv4 environment</th>
<th>IPv6 environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris 9</td>
<td>○</td>
<td>■</td>
<td>× (※1)</td>
</tr>
<tr>
<td>Solaris 10</td>
<td>○</td>
<td>■</td>
<td>× (※1)</td>
</tr>
<tr>
<td>Solaris 11</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

○: Connectable, ×: Not connectable

※1: The client port number must be less than 1024 in order to connect to the NAS port of the ETERNUS DX. Since the port number is 1024 or more for the connected port on a Solaris 9 client and a Solaris 10 client, these clients cannot connect to the NAS port of the ETERNUS DX.

**During the configuration phase**
- To use the NFS client in the ETERNUS DX, apply the following patches or errata.
  If the patches or errata are not applied, the NFS mount may fail, an I/O error may occur, or a file lock takeover may not be possible.

<table>
<thead>
<tr>
<th>NFS protocol</th>
<th>OS</th>
<th>Patch or errata</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFSv3</td>
<td>Red Hat Enterprise Linux 6</td>
<td>Red Hat Enterprise Linux 6.6 or later</td>
</tr>
<tr>
<td>NFSv4.0</td>
<td>Solaris 10</td>
<td>150401-21 or later</td>
</tr>
<tr>
<td></td>
<td>Solaris 11</td>
<td>SRU16061 (Oracle SRU11.3.9.4.0) or later</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7.1</td>
<td>RHSA-2015:1534-1</td>
</tr>
</tbody>
</table>
During the operation phase

- If the load of the NAS system is high, NFS access may fail.
  If an error occurs, re-execute the application with the NFS client.
  The following table shows the relevant OSs.

<table>
<thead>
<tr>
<th>NFS protocol</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFSv3</td>
<td>None</td>
</tr>
<tr>
<td>NFSv4.0</td>
<td>Red Hat Enterprise Linux 6 (6.7 or later)</td>
</tr>
</tbody>
</table>

NAS System (NAS Volume Management)

File systems of up to 128TB can be created in the ETERNUS DX NAS system. One file system can be created for a NAS volume. The number of file systems (NAS volumes) that can be created varies depending on the models.

Table 1 Number of File Systems

<table>
<thead>
<tr>
<th>Model</th>
<th>Number of file systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETERNUS DX100 S4</td>
<td>2</td>
</tr>
<tr>
<td>ETERNUS DX200 S4</td>
<td>4</td>
</tr>
<tr>
<td>ETERNUS DX500 S4</td>
<td>4</td>
</tr>
<tr>
<td>ETERNUS DX600 S4</td>
<td>8</td>
</tr>
<tr>
<td>ETERNUS DX100 S3</td>
<td>1 (*1)</td>
</tr>
<tr>
<td></td>
<td>2 (*2)</td>
</tr>
<tr>
<td>ETERNUS DX200 S3</td>
<td>2 (*3)</td>
</tr>
<tr>
<td></td>
<td>4 (*4)</td>
</tr>
<tr>
<td>ETERNUS DX500 S3</td>
<td>4</td>
</tr>
<tr>
<td>ETERNUS DX600 S3</td>
<td>8</td>
</tr>
</tbody>
</table>

*1: Number of file systems when any of the following conditions is applied.
- When the controller firmware version is earlier than V10L53
- When the Memory Extension (ETFMC / ETFMCA-L / ETDMCAU / ETDMCAU-L) is installed
- When the cache memory included in the Unified kit is installed

*2: Number of file systems when the Memory Extension (ETFMCC / ETFMCC-L / ETDMCCU / ETDMCCU-L) is installed for controller firmware version V10L53 or later.

*3: Number of file systems when the Memory Extension is not installed (but cache memory included in the Unified kit is installed).

*4: Number of file systems when the Memory Extension is installed for controller firmware version V10L33 or later.

System volumes are required in the ETERNUS DX to control the NAS system. In addition, system management area is required for each file system.
After creating a shared folder in the file system, accessing the shared folder from the client becomes available, and directories and files can be stored in it. Access control can be set for each shared folder, directory, and file.

**Figure 2 NAS File Systems**

![Diagram of NAS File Systems]

- **$SYSVOL1**
- **$SYSVOL2**
- **$SYSVOL3**
- **cm0-nas-ex-sysvol**
- **cm1-nas-ex-sysvol**
- **TPV#0 for NAS**
  - System management area
  - (Approx. 300GB)
  - User Data
- **TPV#1 for NAS (Backup destination)**
  - System management area
  - (Approx. 300GB)
  - User Data
- **TPV#x for SAN**
  - User Data
- **RAID group**
  - **SDV#x (Generation management data)**
  - **SDPV#1 (Saved snapshot data)**

**Thin Provisioning Pool (TPP)**

**System management area**

**User Data**

**TPV#1 for NAS (Backup destination)**

**User Data**

**RAID group**

**SDV#x (Generation management data)**

**SDPV#1 (Saved snapshot data)**
**NAS File Systems**

When the first NAS Thin Provisioning Volume (TPV) is created in the ETERNUS DX, system volumes ($SYSVOL1, $SYSVOL2, and $SYSVOL3) are automatically created in the same pool where the TPV is created and then the NAS file system is created.

A NAS file system can be used as a shared folder with Windows or UNIX/Linux. For VMware, the NAS file system can be used as a data store to store data such as configuration information and the OS of the virtual machine.

### IMPORTANT

#### During the configuration phase

- The time it takes to create a file system (NAS volume) varies depending on whether system volumes exist. If system volumes do not exist within the ETERNUS DX, creating a file system takes 10 to 15 minutes longer than usual because system volumes are created while creating the file system.

- In ETERNUS Web GUI, the progress of a file system creation may remain at 99%. Although this gives the impression that the process has been stopped, the process is still continuing. The process is completed in about 30 minutes.

- The total capacity of the NAS user volumes, NAS backup volumes, and the system volumes (17GB) must not exceed the maximum pool capacity. TPVs and FTVs for a SAN connection are also included.

For more details about the maximum pool capacity setting, refer to "Set Thin Provisioning" in "ETERNUS Web GUI User’s Guide".

#### During the operation phase

- The procedure for deleting the system volume differs depending on the controller firmware version.
  - For controller firmware versions earlier than V10L51
    Contact your maintenance engineer to delete the system volumes. The ETERNUS DX must be rebooted after the system volumes are deleted.
  - For controller firmware versions V10L51 or later
    1. Delete all the NAS volumes.
    2. Delete all the expanded system volumes.
    3. Delete all the system volumes.

When the system volumes are deleted, the NAS system reboots. When performing a NAS configuration after deleting the system volume, check whether the reboot is complete and the status of the NAS Engine is "Maintenance/0xE000" using ETERNUS CLI.

Deleting all system volumes ($SYSVOL1, $SYSVOL2, and $SYSVOL3) at once is recommended. When system volumes are deleted one by one, delete the next system volume after the system is rebooted.
## System Volumes

A system volume consists of three volumes that has a total capacity of 17GB. Two of the three system volumes are for the Rootfs partition for each controller. The remaining volume is for the file system management partition.

System volume names cannot be changed.

The following table shows the name, capacity, and usage of the system volumes.

**Table 2 System Volumes**

<table>
<thead>
<tr>
<th>Volume name</th>
<th>Capacity</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SYSVOL1</td>
<td>1GB</td>
<td>File system management partition</td>
</tr>
<tr>
<td>$SYSVOL2</td>
<td>8GB</td>
<td>Rootfs partition for CM#0</td>
</tr>
<tr>
<td>$SYSVOL3</td>
<td>8GB</td>
<td>Rootfs partition for CM#1</td>
</tr>
</tbody>
</table>

### Note

**During the design phase**

To use the Eco-mode function for TPPs that include NAS volumes, move the system volumes to a different TPP. The Eco-mode function does not work for a TPP that contains system volumes. System volumes can be moved by using RAID Migration.

**During the configuration phase**

- Copy operation suppression (volume protection) cannot be set for system volumes.
- The status of the controller (CM) is "Maintenance" until system volumes are created. When NAS user volumes and system volumes are created, the status of the controller (CM) changes to "Normal".

## Expanded System Volume

To use the NAS audit log function, create expanded system volumes for each controller in advance. Volume names can be set arbitrarily.

The following table shows the type, capacity, and usage of the expanded system volumes.

**Table 3 Expanded System Volume**

<table>
<thead>
<tr>
<th>Type</th>
<th>Capacity</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>cm0-nas-ex-sysvol</td>
<td>1GB – 4TB</td>
<td>Expanded system volume for CM#0</td>
</tr>
<tr>
<td>cm1-nas-ex-sysvol</td>
<td>1GB – 4TB</td>
<td>Expanded system volume for CM#1</td>
</tr>
</tbody>
</table>

Expanded system volumes are required for saving the NAS audit logs. For the creation procedure, refer to "Audit Log Setup" (page 132).

## System Management Area

Each NAS volume must have a system management area of approximately 300GB. This area is the metadata area that is used by the system for managing file system information.
# Meta Cache

For the NAS file system, information for managing metadata, which is file system information, is deployed in the cache memory of the controller (CM) for each NAS volume to seed up access. This is called meta cache.

Meta cache is deployed in either CM#0 or CM#1 for each NAS volume. Immediately after a NAS volume is created, the meta cache is deployed in both CMs equally.

![Figure 3 Initial Deployment of Meta Cache](image)

If maintenance work is required due to problems such as errors detected in the NAS volume, the meta cache may be unevenly deployed in one controller. The ETERNUS DX supports the function that releases the unbalanced state. Your maintenance engineer may ask you to execute this function during maintenance. For details on the function, refer to “Meta Cache Distribution” (page 57).

# NAS Volume

TPVs that are used as NAS volumes must be created in a TPP virtual pool. Because TPVs support virtualization of volume capacity, a volume can be used more efficiently by using a volume capacity that is larger than the actual physical capacity.

Two types of NAS volumes are available; NAS user volumes used for operation and NAS backup volumes used for backup.

SAN volumes and NAS volumes can exist in the same TPP. Although NAS user volumes and NAS backup volumes can also exist in the same TPP, creating these types of volumes in separate TPPs is recommended to ensure redundancy. For load balancing, it is also recommended to configure a TPP with two or more RAID groups if NAS volumes will be created in this TPP.

When controller firmware version V10L21 or later is used, expansion of the NAS volumes is available. Before a capacity expansion, perform the following actions:

- **NAS volume reconfiguration (format conversion)**
  
  When the capacity of the NAS volume that was created with a controller firmware version earlier than V10L21 is expanded, a NAS volume reconfiguration (format conversion) must be performed prior to a volume capacity expansion. If a volume capacity expansion is performed for the NAS volume without a reconfiguration (format conversion), an error occurs. A NAS volume reconfiguration (format conversion) can be performed with the "Reconfigure NAS Volume" function from ETERNUS Web GUI, or ETERNUS CLI.

- **Stopping access to all the volumes**
  
  While a volume is being expanded, access to the volume may be delayed because the access is temporarily suspended. Stop access to all the volumes while a volume expansion is being performed. If a volume capacity expansion is performed without stopping the access to the volumes that are not expanded, the process may fail (timeout).
During the configuration phase

- Do not format the NAS volume. If it was formatted, delete the NAS volume and create it again.
- Do not configure the QoS setting to NAS volumes.
- Do not perform TPV/FTV capacity optimization (Zero Reclamation) for NAS user volumes, NAS backup volumes, or the system volumes.
- When creating multiple NAS volumes in a Thin Provisioning Pool that is configured with Nearline SAS disks, wait at least 10 minutes after each NAS volume is created before creating the next one.

During the operation phase

- An error occurs when a volume capacity expansion is performed with backup and Snapshot settings already configured. Delete the backup and Snapshot settings before performing a volume capacity expansion. Do not delete the backup volume at this point because the volume is necessary for restoration if the volume capacity expansion fails and data on the drive is corrupted. Delete the backup volume and reset the backup and Snapshot after volume capacity expansion is completed successfully.
- When the NAS volume is being reconfigured (format conversion), do not access the volume or mount the volume to CIFS or NFS from the client. If these operations are performed, an I/O error will occur because the volume is unmounted during the reconfiguration process. For controller firmware versions V10L31 and later, because the file lock state is released for all file systems, execute the NAS volume reconfiguration (format conversion) after stopping operations for all file systems.
- For NAS volumes where a NAS volume reconfiguration (format conversion) was performed or for newly created NAS volumes, do not restore backup data that was acquired before the reconfiguration. Acquire backup data after reconfiguring the NAS volumes.
- If NAS user volumes and NAS backup volumes are mounted from a UNIX/Linux client, do not run the following functions on them.
  - Volume deletion
  - Volume formatting

During the configuration phase

The threshold can be set for TPVs for NAS in the same way as TPVs for SAN.

During the operation phase

A NAS volume reconfiguration (format conversion) takes up to 15 minutes.
### NAS User Volumes

A NAS user volume must have an area of 300GB for the system management area, and an area of 100GB or more for the user area to store user data. Create a TPV with a capacity of 400GB or more for the NAS user volume.

For example, when a 3TB NAS user volume is created, 0.3TB is reserved for the system management area and 2.7TB is reserved for the user data area.

A NAS user volume (TPV) may be up to 128TB. Note that the total TPV capacity must be smaller than the maximum capacity of the TPP. The capacity of a NAS user volume can be expanded after it is created. When capacity expansion is performed using ETERNUS Web GUI, select [Expand TPV] from the [Volume] screen.

**Note**

During the configuration phase

The following operations cannot be performed for NAS user volumes in which a shared folder exists.

- Volume deletion
- Volume formatting

### NAS Backup Volumes

NAS backup volumes are created in TPVs to back up NAS user volumes. One NAS backup volume can be created for a NAS user volume. The maximum number of NAS backup volumes is the same as the NAS user volumes.

NAS backup volumes can be created with ETERNUS CLI or ETERNUS SF AdvancedCopy Manager. For details, refer to "Available Functions for Each Software" (page 176). NAS user volumes can be restored from NAS backup volumes. A backup or restore of NAS user volumes is performed with volume copy using QuickOPC.

To restore data for each file, manually copy the files to restore from the client after mounting the NAS backup volumes.

In addition, NAS backup volumes can be backed up to and restored from remote ETERNUS DX storage systems. ETERNUS SF AdvancedCopy Manager is required for backup/restore.

Note that the NAS backup volume is stored in a different destination from the snapshot.

**Caution**

During the configuration phase

A NAS backup volume must be created with the same capacity as the backup source volume.

During the operation phase

In the ETERNUS DX100 S3 with a controller firmware version earlier than V10L53, do not mount NAS backup volumes.

**Note**

During the operation phase

Before deleting NAS backup volumes, remove client connections from the NAS backup volumes (by unmounting (for NFS) or disconnecting the network drive (for CIFS)) and unmount the NAS backup volumes by using the ETERNUS SF software.
### NAS Snapshot Destination Volumes

To acquire snapshots, volumes to store snapshot control information and Snapshot data. Snap Data Volume (SDV) is a generation management volume used as the copy destination. Snap Data Pool Volume (SDPV) is used for saving snapshot data.

- **SDV**
  A volume that is used to store the snapshot control information. When snapshot settings are performed, an SDV with the same capacity as the NAS user volume is created for the specified number of generations.

- **SDPV**
  A volume that is pooled in an SDP to store snapshot data. Create an SDPV before acquiring snapshots. An SDPV must have enough size to store snapshot. If the SDP size is insufficient, an error occurs for a snapshot.

SDVs and SDPVs cannot be created in a TPP. SDVs are automatically created in the RAID group that is specified when setting snapshot. SDPVs must be created separately. When acquiring 128 generations of snapshots, a RAID group for registering an SDV and a RAID group for registering an SDPV must be prepared separately.

### Block Size

An optimal block size can be set for the file system according to the operation. In addition, file systems with different block sizes can exist together in a single ETERNUS DX.

A block size is a unit for managing files within the ETERNUS DX. Files are stored in blocks that are divided into a fixed size. A small block size minimizes areas used by each file, thereby improving the storage efficiency of a system that creates many small-sized files.

The block size is fixed at 256KB for NAS volumes that are created with controller firmware versions earlier than V10L31. For NAS volumes that are created with controller firmware versions V10L31 or later, the block size can be specified when volumes are created.

The block size setting determines the maximum file size and the maximum volume capacity. The following table shows the maximum file size and the maximum volume capacity for each block size.

<table>
<thead>
<tr>
<th>Firmware version</th>
<th>Block size</th>
<th>Maximum file size</th>
<th>Maximum volume capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>V10L30 or earlier</td>
<td>256KB</td>
<td>32TB</td>
<td>128TB</td>
</tr>
<tr>
<td>V10L31 or earlier</td>
<td>8KB</td>
<td>1TB</td>
<td>4TB</td>
</tr>
<tr>
<td></td>
<td>32KB</td>
<td>4TB</td>
<td>16TB</td>
</tr>
<tr>
<td></td>
<td>256KB</td>
<td>32TB</td>
<td>128TB</td>
</tr>
<tr>
<td>V10L33 or later</td>
<td>8KB</td>
<td>1TB</td>
<td>32TB</td>
</tr>
<tr>
<td></td>
<td>32KB</td>
<td>4TB</td>
<td>128TB</td>
</tr>
<tr>
<td></td>
<td>256KB</td>
<td>32TB</td>
<td>128TB</td>
</tr>
</tbody>
</table>

### Caution

**During the configuration phase**

- Volumes cannot be expanded to a capacity larger than the maximum volume capacity that is determined by the block size.
- The block size of the file system cannot be changed after a NAS volume is created.
File System Specification

- File System Usage and Free Space

Available free space in the file system is shown differently when the file system area is checked from a CIFS client or an NFS client.

The areas described below are displayed as used areas in the file system.

- **root Reserved Area**

  For NFS clients, this is an area that is accessible by administrators if free space is insufficient for general users. In addition, this area is not recognized as an unused area or a used area from the NFS client. Note that the capacity of this area is included in the total capacity.

  For CIFS clients, this is an area that cannot be used by administrators or general users.

  The capacity of root reserved area ranges from 1GB to 1,277GB, which is 1% of the user area that is specified when creating NAS volumes (excluding the system management area).

- **Access Client Reserved Area**

  The reserved area that is secured in advance for the file system to read data efficiently. This area is used to write the user data.

  This area is recognized as a used area from the CIFS client, the NFS client, ETERNUS Web GUI, and ETERNUS CLI.
The capacity of the access client reserved area (approximately 1.5GB to 6GB) depends on the NAS volume size.

**Figure 4 How Free Space Is Recognized**

During the operation phase

- If “Out of NAS Capacity” for the Setup Event Notification function is enabled, an event is notified when all areas including the root reserved area are used.
- The usage status of a NAS volume can be checked via ETERNUS Web GUI or ETERNUS CLI. The used capacity that is displayed includes the capacity of the access client reserved area regardless of the protocol (CIFS, NFS, and CIFS/NFS) that is used for the shared folder. The used capacity and the free capacity do not include the capacity of the root reserved area. The capacity of the root reserved area is included in the total capacity.
Data Encryption

By using Self Encrypting Drives (SED) or the firmware data encryption function, NAS volume data can be encrypted.

Because data encryption is performed using the firmware in the ETERNUS DX controller, the performance is degraded when compared to unencrypted data access.

Because SEDs do not affect system performance, encrypting the data with SEDs is recommended when system performance is prioritized.

For details on data encryption, refer to "Design Guide (Basic)".

Caution

During the design phase

For each ETERNUS DX, select and specify "AES128", "AES256", or "Fujitsu Original Encryption" as the encryption mode for the firmware data encryption function. To specify the encryption mode, refer to the following notes.

- For the ETERNUS DX100 S4/DX100 S3
  Set the encryption mode to "Fujitsu Original Encryption". AES encryption modes cannot be used because setting "AES128" or "AES256" deteriorates the performance of the NAS function.

- For the ETERNUS DX200 S4, the ETERNUS DX500 S4/DX600 S4, the ETERNUS DX200 S3, and the ETERNUS DX500 S3/DX600 S3
  It is highly recommended that the encryption mode is set to "Fujitsu Original Encryption".
2. Designing NAS Operations

This chapter describes user management, access control, and file sharing in a NAS system. This chapter also explains the available NAS functions for the ETERNUS DX.

NAS Server Name (Host Name)

A 12-digit NAS server name is automatically set for the ETERNUS DX according to the following rules:

- **DX<10-digit ETERNUS DX serial number>**

The NAS server name can be changed to any name by using ETERNUS Web GUI or ETERNUS CLI. For the configuration procedures, refer to "NAS Server Name Settings" (page 95).

Because the NAS server name (or NetBIOS name) is not broadcast, when a NAS server name is used for CIFS access, make sure that the name resolution is enabled in the DNS server.

For Active Directory authentication, the NAS Engine of the ETERNUS DX uses the NAS server name as a NetBIOS name.

After the NAS server name (NetBIOS name) is changed, the authentication server must be registered again. If the Active Directory authentication server information has already been registered before the NAS server name (NetBIOS name) is changed, perform the following operation:

### Procedure

1. Delete the configuration information for the Active Directory authentication server before changing the NAS server name.
   - To delete the information, use the "Set Authentication Server" function in ETERNUS Web GUI or the "set nas-ad" command in ETERNUS CLI.

2. Change the NAS server name.
   - To change the information, use the "Change NAS Server Name" function in ETERNUS Web GUI or the "set nas-server" command in ETERNUS CLI.

3. Set the information for the ETERNUS DX and the Active Directory authentication server again.

   **End of procedure**
User Management

This section describes user management for NAS connection with the ETERNUS DX. User management for NAS clients is performed with an authentication server or with local user authentication.

● Windows (CIFS) Environment

When the Active Directory authentication server is used, access can be controlled based on the registered user accounts in the authentication server.

When an authentication server is not used, access using the following methods.

• For controller firmware versions earlier than V10L53
  All users share a fixed user account for access.
• For controller firmware versions V10L53 or later
  Local users/local groups can be created. Access is available on a per local user/local group basis. For details, refer to "Local User Authentication" (page 34).

**Note**

If the controller firmware version is earlier than V10L53 and an authentication server is not used, upgrading the controller firmware to V10L53 or later automatically creates the local user "shareuser$". This user can be operated in the same way as a fixed user account.

● UNIX/Linux (NFS) Environment

When the LDAP authentication server (such as OpenLDAP) is used, access can be controlled based on the registered user accounts in the authentication server. When NFS access is used, the folders that the administrator mounts can be accessed by all users.
Authentication Server

An authentication server can be used to control access to the ETERNUS DX NAS file system. Connect the authentication server to the network in the NAS environment. Prepare the Active Directory authentication server to perform access via Windows or prepare the LDAP authentication server to perform access via UNIX/Linux.

For the character strings that can be specified when configuring the authentication server, depending on the item, the following requirements exist.

- **Domain name, domain administrator's user ID, and password**
  - The number of characters that can be specified is 1 to 255 characters.
  - The types of characters that can be used are alphanumeric characters (US-ASCII code) and symbols between space character (0x20) to "~" (0x7E). Note that "?" (0x3F) and "\" (0x5C) cannot be used.

- **Authentication server**
  - The number of characters that can be specified is 1 to 255 characters.
  - The following types of characters can be used.
    - Alphanumeric characters (US-ASCII code)
      - "A" (0x41) to "Z" (0x5A) and "a" (0x61) to "z" (0x7A)
    - Numerical characters
      - "0" (0x30) to "9" (0x39)
    - Symbols
      - "." (0x2E), ":" (0x3A), and ":" (0x3A)

![Figure 5 Authentication Server](image)

For operations that use the Active Directory authentication server or the LDAP authentication server, a configuration error of the NAS functions that are described in "Available Functions for Each Software" (page 176), a NAS Engine down, or a snapshot failure may occur if communication with the authentication server is unavailable due to a network error.
## Authentication in a CIFS Environment

A login authentication by the Active Directory authentication server (Kerberos authentication method) or the local user authentication setting is required to perform user management of the directories and files with CIFS access.

The ETERNUS DX supports Active Directory's one-way and two-way explicit trust relationships. For example, when the trusting domain is set in the ETERNUS DX, setting the trust relationship of the domains as one-way or two-way gives the trusted domain user access to the ETERNUS DX.

File access control information is stored for each directory or file in a CIFS environment in the same way as in a normal Windows environment.

Access privileges to read and write to shared folders can be assigned for each user or each group.

For Active Directory authentication, specify the user name in the following format:

```
netbios_domain_name\User_name
```

Example: `domain\user1`

### IMPORTANT

**During the design phase**

The time in the ETERNUS DX and the Active Directory authentication server must be synchronized to perform operations with the Active Directory authentication server. Automatic time correction by the Network Time Protocol (NTP) is recommended.

### Caution

**During the design phase**

If the controller firmware version is earlier than V10L61, the ETERNUS DX uses SMB1.0 to communicate with the Active Directory authentication server.

For this reason, disabling SMB1.0 in the Active Directory authentication server causes user authentication failures which in turn make the shared folder inaccessible.

Before disabling SMB1.0 of the Active Directory authentication server, update the ETERNUS DX controller firmware version to V10L61 or later.

### Note

**During the configuration phase**

- For Active Directory authentication, the NAS Engine of the ETERNUS DX uses the ETERNUS DX's host name as a NetBIOS name.
  
  For details on the ETERNUS DX's host name, refer to "NAS Server Name (Host Name)" (page 27).

- Active Directory's two-way, transitive trust relationships are not supported.

- The maximum number of users that can be managed using Active Directory is 100,000.
# Authentication in an NFS Environment

A login authentication by the LDAP authentication server (such as OpenLDAP) is required to perform user management of directories and files with NFS access.

## Caution

### During the design phase
Operations using an LDAP authentication server that is running Active Directory Lightweight Directory Services are not supported.

## Note

### During the configuration phase
- To use the LDAP authentication server, add the administrator to manage subdirectories under the target directory tree in the LDAP authentication server in advance. In addition, set this administrator as the LDAP domain administrator when setting the authentication server from ETERNUS Web GUI or ETERNUS CLI.

  The procedure to set a directory tree administrator varies depending on the software. The examples when using the following products are as follows.

- **When the 389 Directory Server (formerly called as Fedora Directory Server) is used**
  Register the administrator to manage subdirectories under the target directory tree using "ldapadd" command or GUI screen after installing the package in addition to the "Directory Server Manager (account that is specified with Directory Manager DN)" that is input when installing the package.

- **When OpenLDAP is used**
  Because an administrator has already been registered during the package installation, additional settings are not required.

- **When Oracle Unified Directory (OUD) is used**
  Create the administrator to manage subdirectories under the target directory tree in addition to the "Directory Server Manager" that is input when creating the instance. Register the administrator to manage subdirectories under the target directory tree using the "ldapadd" command or GUI screen.

### During the operation phase
The access privilege for the shared folder cannot be changed from an NFS client by executing the "mount" command with an option to assign a Read-Write (rw) access privilege when this shared folder is created with the operation management interface (ETERNUS Web GUI or ETERNUS CLI) so that it supports the NFS protocol and receives a Read (r) access privilege.
### Authentication in Environments where the CIFS Protocol and the NFS Protocol Are Used Concurrently

In environments where the CIFS protocol and the NFS protocol are used concurrently and Active Directory (AD) authentication and LDAP authentication are used, operational design for authentication information (username, group name, and ID) is required.

- **Process of Acquiring the Authentication Information during a Switchover from AD Authentication to LDAP Authentication**
  
  - **CIFS access**
    
    For CIFS access, AD authentication is performed.
    Therefore, attempts to access directories or files from a user not registered in the AD authentication server result in an authentication error.

  ![Figure 6 Process for Acquiring the Authentication Information (CIFS)](image)

  - **NFS access**
    
    For NFS access, confirmation of the access permissions is performed.
    The ETERNUS DX initially accesses the AD authentication server to reference the authentication information.
    If the AD authentication server lacks the authentication information, the LDAP authentication server is accessed.

[diagram of authentication process]
If the authentication information is not registered in the AD authentication server or the LDAP authentication server, the access results in an authentication error.

Figure 7 Process for Acquiring the Authentication Information (NFS)

Policies Related to the Operation Design of the Authentication Information

- For users who use the CIFS protocol and the NFS protocol

  The relevant username and group name need to be set in the AD authentication server and the LDAP authentication server.

  1. Register the user in the AD authentication server
     After the user registration, check the user's Relative ID (RID). RID is a part of the Security ID (SID).
     For a SID value of "S-1-5-21-xxxx-yyyy-zzzz-nnnn", the RID value is indicated by the "nnnn" portion.

  2. Register the user in the LDAP authentication server
     Set the following values to UID and GID.
     The RID value obtained when the user is registered in the AD authentication server + 10,000,000

- For users who use only the NFS protocol

  The relevant username and group name need to be set in the LDAP authentication server.
  In the LDAP authentication server, set a UID and GID value within the following range.
  1,005 to 9,999,999

- For users who use only the CIFS protocol

  No consideration is needed.
Fixed User Account

- **CIFS Environment**
  The following account is used for all users who are not managed with the Active Directory authentication server or with the function that is described in "Local User Authentication" (page 34).

  **User name:** shareuser$

  **Password:** share!

  The fixed user account (shareuser$) cannot be used if users are managed with the Active Directory authentication server.

  For controller firmware versions V10L53 or later, the fixed user account is not available in the initial settings. The fixed user account must be created in the local user authentication setting.

  However, if the controller firmware version is earlier than V10L53 and an authentication server is not used, upgrading the controller firmware to V10L53 or later automatically creates the local user "shareuser$". This user can be operated in the same way as a fixed user account. "shareuser$" can be deleted and recreated. However, the previous password (share!) cannot be specified for the re-creation because the password must contain eight characters or more.

- **NFS Environment**
  If user management with the LDAP authentication server is not performed, or access control with ACL is not performed, all of the users that perform NFS access are allowed access. Only an administrator can perform the mount operation for access.

Local User Authentication

Local user authentication is a function that manages local users/groups who can access the shared folder without using the authentication server and can enable CIFS access on a per created local user/local group basis. Specify the access permission of the shared folder when the shared folder is created. Authentication server and local user authentication cannot be used simultaneously.

**Caution**

**During the configuration phase**

When a shared folder is created using CIFS/NFS and the same access privilege is used between CIFS and NFS, the user name, user ID, group name, and group ID of the client that performs an NFS access must match the user name, user ID, group name, and group ID that are created on the ETERNUS DX.

Local user/local group management (such as creating, changing, and modifying) can be performed from ETERNUS Web GUI or ETERNUS CLI. For local users/local groups, up to 100 can be created for each. However, three local groups are used for the BUILTIN groups.

Local users can belong to one primary group and multiple secondary groups. Only the local user who created the files or directories and local users in the same group can access these files or directories.

Registered local users can be used for the following functions.

- Shared folder owner/group
- CIFS access permission settings for shared folders
- Quota settings on a per local user/local group basis
- Home directories
• Account authentication for FTP connections

● Primary Group

Primary group is the group that is set for the directories and files that were created by the local user. A local user must belong to one of the primary groups. If the primary group is not specified when the local user is created, the local user will belong to "sharegroup$" which is the shared group of all local users.

● Secondary Group

Secondary group is the subgroup for accessing directories and files that were created by the other users. Local users can belong to multiple secondary groups (up to 16 groups) in addition to the primary group. Local users who do not belong to any secondary groups can be created.

During the operation phase

• When operations are migrated from the authentication server to local user authentication, deleting the local user/local group settings and reconfiguring the user on the authentication server side are required.
• BUILTIN groups can be used only for secondary groups.
• BUILTIN groups cannot be deleted. Even if BUILTIN groups exist, authentication server settings can be performed.
• If the controller firmware version is earlier than V10L53 and the fixed user account "shareuser$" is used, upgrading the controller firmware to V10L53 or later automatically creates the local user "shareuser$". This user can be operated in the same way as a fixed user account. For details, refer to "Fixed User Account" (page 34).

For the character strings that can be specified when the local user authentication is configured, the following requirements exist depending on the item.

• Local user names and local group names
  - The number of characters that can be specified is 1 to 32 characters.
  - The following types of characters can be used.
    - Alphanumeric characters and symbols ("-", "_", "$") (US-ASCII code)
    - The first character must be an alphanumeric character or an underscore ("_"). A dollar sign ("$") can only be used for the last character. A local group name consisting of only numbers cannot be set.
  - In addition, local users and local groups using the same name cannot be created. The characters are case-insensitive.
  - Because the following character strings are reserved words, they cannot be specified.
    adm, audio, bin, cdev, cpath, daemon, dialout, dip, disk, everyone, floppy, ftp, games, gopher, halt, kmem, ldap, lock, lp, mail, mailnull, man, mem, nfsnobody, nobody, nscl, nscl, ntp, operator, oprofile, root, rpc, rpcuser, saslad, shutdown, smm, sshd, sync, sys, tape, tcpdump, tty, users, utempter, utmp, uucp, vsa, video, wheel
  - When a local user is used in Windows (CIFS) environments, the local user name must be different from the local group name. If the same name is used for the local user and the local group without case sensitivity, access control may not be set correctly for Windows.

• Password
  - The number of characters that can be specified is 8 to 32 characters.
  - The types of characters that can be used are alphanumeric characters and symbols (US-ASCII code).
Access Control (ACL Function)

A NAS file system reserves extended ACL areas to store permission entries. If the CIFS protocol or the NFSv3 protocol is used, up to 256 access permission entries can be registered for files and directories.

In addition, ACLs that are registered for files and directories can also be referenced. In a CIFS environment, the following well-known SIDs are supported.

- Domain SIDs (S-1-5-21-*)
- Administrators (S-1-5-32-544)
- Users (S-1-5-32-545)
- Backup Operators (S-1-5-32-551)

The folders and files registered with Administrators, Users, and Backup Operators are accessible from the Domain Admins group, the Domain Users group, and the fixed user account (shareuser$), respectively. For local users, access to files and folders is granted by setting the group to which the user belongs in the Administrators group, the Users group, or the Backup Operators group.

Accessing to files or directories is not allowed even if unsupported well-known SIDs are specified for the ACL function. Refer to the following site for the well-known SIDs list.

- Well-known security identifiers in Windows operating systems
  https://support.microsoft.com/en-us/kb/243330

Caution

During the configuration phase

- If there are more ACLs than the maximum number of ACL entries that can be registered for each NAS volume, the access privileges information for the target files or directories may be deleted.
- Do not change the following access control settings for the root folder of the shared folder from the client.
  - Owner
  - Group
  - Access privilege

  If these settings are changed from a client, the clients may become unable to access the shared folder.

Access control settings must be configured for subfolders and files under the shared folder.

During the operation phase

If the ETERNUS DX is used as the backup destination or the data migration destination, and if a file that is set with an ACL of an SID that does not exist in the ETERNUS DX user management (authentication server or local user authentication) is copied to the ETERNUS DX, the copied file will become inaccessible. Do not copy the ACL information of an SID that does not exist in the ETERNUS DX user management.
Access Control in a CIFS Environment

For CIFS access, Windows ACL supported file access management is performed.

Windows' Access Based Enumeration (ABE) is supported. With ABE, directories and files can be hidden to users who do not have access privileges. ABE can be enabled or disabled with ETERNUS Web GUI or ETERNUS CLI.

The supported ABE partly differs in specification from the actual Windows ABE. Directories and files without read access privilege are hidden even if write access privilege or special access privilege is set.

If the same name is used for the local user and the local group without case sensitivity when a local user is registered in ACL, access control may not be set correctly for Windows. When a local user is used in Windows (CIFS) environments, delete either the user ("shareuser$") or the group ("shareuser$") and create a local user and local group using a different name.

### IMPORTANT

**During the configuration phase**

The owner and group settings of a shared folder do not automatically set the access privileges for subfolders and files under that shared folder. For subfolders and files under the shared folder, manually set the appropriate access privileges as necessary.

Access Control in an NFS Environment

For NFS access, the NFS access control supported by each of the NFS versions can be configured in addition to the permissions.

If NSF access control is configured, that configuration has a higher priority than permissions.

POSIX ACL is used for NFSv3 access control.

### Caution

**During the operation phase**

NFS clients using NFSv4 to mount the shared folder cannot execute commands that set or display POSIX ACLs for the shared folder.
Access Control in a Shared CIFS/NFS Environment

When the CIFS protocol and the NFS protocol are used, the access control varies depending on the version of NFS.

The NFS access control varies depending on the NFS version.

For details, refer to "Access Control in an NFS Environment" (page 37).

If the same name is used for the local user and the local group without case sensitivity when a local user is registered in ACL, access control may not be set correctly for Windows. When a local user is used in Windows (CIFS) environments, delete either the user ("shareuser$") or the group ("shareuser$") and create a local user and local group using a different name.

During the operation phase

- Even though advanced security settings are specified with Windows ACL, the ACL security setting for some users or groups may be unintentionally overwritten by an ACL setting that is performed later or may not be enabled when the CIFS protocol and the NFS protocol are used at the same time.

- Even though advanced security settings are specified with Windows ACL, the UNIX POSIX ACL converts them to Read permissions, Write permissions, and Execute permissions and maps these permissions. Accesses from other Windows clients are controlled by privileges mapped to POSIX ACL.

- When adding ACL user from Windows, a security ID (Security ID) may be displayed instead of the name that is specified from other Windows clients. If this occurs, disconnect the network drive and wait for a while. After rebooting the network drive, the specified name is displayed.

CIFS Access Permission Settings

Access permissions can be set for a specific user or group when a CIFS shared folder is created.

The group "everyone" can be specified as a group. Access permissions can be changed for existing CIFS shared folders. The CIFS access permission setting can grant access permissions for users or groups who have access permissions that are granted by the ACL function.

When "everyone" is specified as the group, the privileges that are set for "everyone" are granted to all users. However, users that are granted the "rw" access privilege can read and write data regardless of the privileges that are set for "everyone".

Access permissions for the CIFS shared folders can be changed using ETERNUS Web GUI or ETERNUS CLI. The changed settings are applied to sessions that are established after the change.

If NAS volumes that are backed up in the ETERNUS DX with a controller firmware version earlier than V10L51 are restored to an ETERNUS DX with a controller firmware version V10L51 or later, folder access permissions are granted according to the default settings (where access permissions are not granted to any specific user or group).

During the configuration phase

To use the CIFS access permission setting for access control of a shared folder, either omit the owner and group settings or specify "root" when creating a shared folder. For details on the owner and group settings of the shared folder, refer to "File Sharing" (page 39).
File Sharing

Each client can share files in the NAS file system for the ETERNUS DX. For file sharing, the CIFS protocol is used for Windows and the NFS protocol is used for UNIX/Linux.

**Shared Folder**

To share files, create shared folders in the file system for the ETERNUS DX that support the protocol that is to be used. Shared folders are directories that are created in the root directory of the file system.

Up to 256 shared folders can be created in the ETERNUS DX. When creating multiple file systems, the total number of shared folders in each file system cannot exceed 256.

**Note**

**During the operation phase**

Before deleting all the data in the shared folder with the NAS data deletion function or before deleting the shared folders, remove the client connections (by unmounting for NFS or by disconnecting the network drive for CIFS).

**Access Privileges (Permissions) for Shared Folders**

Each shared folder can be set with a protocol that enables access to it and the range of access that is allowed. For shared folders, "Owner" for the folder and "Group" to which the owner belongs can be specified. A user that receives ownership or a user in a group that receives ownership is granted access privileges (permissions) to the shared folders. Regardless of whether the authentication server (Active Directory or LDAP) is used, if the shared folder is created by omitting the Owner setting and the Group setting, "root" is set as the owner of the shared folder and has full control (rwxrwxrwx).

Hosts that are allowed or denied access to the shared folders can be specified. In an IPv6 environment, global addresses and local addresses can be set with an IP address. Link-local addresses cannot be set with an IP address.

**Caution**

**During the configuration phase**

- If only the owner is specified for the shared folder, the "rwx" access privilege is added for the specified user. For this setting, other users cannot access the shared folder.
- If only the group is specified for the shared folder, the "rwx" access privilege is added for the root user and the specified group. For this setting, other users cannot access the shared folder.
- For shared folders that are accessed with CIFS access, the recommended configuration is to set the owner and group to "root" and then configure the CIFS access permission setting for access control.
  - If the owner and group of the shared folder is "root", access control cannot be performed for the root folder of the shared folder. Therefore, set the access privileges using the CIFS access permission setting.
  - If the owner and group of the CIFS shared folder or CIFS/NFS shared folder is not "root", users who are not the owner or users who do not belong to the group are denied access to the shared folder.
  - Even if the access privilege is set to "everyone" by the CIFS access permission setting or by the access control setting of the CIFS client, if the owner and group of the shared folder is not "root", users who are not the owner or users who do not belong to the group cannot access those shared folders.
During the design phase

- The types of characters that can be used for the owner name and group name are alphanumeric characters (or US-ASCII codes) and symbols from the space character (0x20) to the tilde "~" (0x7E). Note that "?" (0x3F) and "\" (0x5C) cannot be used.
- The types of characters that can be used for CIFS Allowed Hosts, CIFS Denied Hosts, and NFS Allowed Hosts are alphanumeric characters (or US-ASCII codes) and symbols from the space character (0x20) to the tilde "~" (0x7E). Note that "?" (0x3F) and "\" (0x5C) cannot be used.
- The owner and group of a shared folder cannot be assigned with the character strings below because they are reserved words. This applies even if the character strings are registered in the authentication server.

<table>
<thead>
<tr>
<th>Reserved words that cannot be assigned to the owner</th>
<th>Reserved words that cannot be assigned to the group</th>
</tr>
</thead>
<tbody>
<tr>
<td>shareuser$, bin, daemon, adm, lp, sync, shutdown, halt, mail, uucp, operator, games, gopher, ftp, nobody, vsca, rpc, nsck, ntp, saslauth, mailnull, smmsp, rpcuser, nfsnobody, sshd, nsldc, tcpdump, oprofile</td>
<td>shareuser$, bin, daemon, sys, adm, tty, disk, lp, mem, kmem, wheel, mail, uucp, man, games, gopher, video, dip, ftp, lock, audio, nobody, users, utmp, utempter, floppy, vsca, rpc, nsck, cdrom, tape, dialout, ntp, saslauth, mailnull, smmsp, rpcuser, nfsnobody, sshd, ldap, tcpdump, oprofile</td>
</tr>
</tbody>
</table>

**Character Set**

For the ETERNUS DX in a Unified configuration, UTF-8 is used as the character set.

File names and directory names are set with the UTF-8 character set.

During the operation phase

- Specifications for the character set and the length of the file name depends on the OS. File names must be taken into consideration when sharing files.
  - The following table shows the character set and the file name length for Windows and UNIX/Linux.

<table>
<thead>
<tr>
<th>OS</th>
<th>Character set</th>
<th>File name length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>UTF-8 (Unicode)</td>
<td>Up to 255 bytes</td>
</tr>
<tr>
<td>UNIX/Linux</td>
<td>UTF-8</td>
<td>Up to 255 bytes</td>
</tr>
</tbody>
</table>

- Note that the following characters cannot be used for file names in Windows.
  - "(double quotation mark), * (asterisk), / (slash), : (colon), <, >, ?, \, | |
- The maximum length for a UNIX/Linux directory path name is 1,005 bytes.

Although UNIX/Linux allows up to 1,023 bytes for the directory path name, internal processes for the ETERNUS DX uses 18 bytes so the maximum length for path names are reduced to 1,005 bytes.
CIFS Operation

This section describes an operation in which the CIFS protocol is used. In a Windows environment, domain-based operations are supported.

Caution

During the configuration phase

If the controller firmware version of the ETERNUS DX is earlier than V10L61, do not disable SMB1.0 in the Active Directory authentication server. This is because the ETERNUS DX uses SMB1.0 to access the Active Directory authentication server to obtain authentication.

If SMB1.0 is disabled in the Active Directory authentication server, authentication settings cannot be modified or the ETERNUS DX shared folder becomes inaccessible from the CIFS client during domain-based operations.

Switching between SMB1.0/2.0/3.0

For versions of the SMB protocol, SMB3.0 is enabled by default.

To change the version of the SMB protocol, execute the following procedure.

Procedure

1. Specify the protocol version that is to be changed in the "-smb-version" parameter of the ETERNUS CLI "set nas-server" command, and then execute the command.

2. Reestablish a session for the CIFS client that is to be connected.

End of procedure

Note

During the configuration phase

- When the CIFS client is Windows 8.1 or Windows Server 2012 R2, or later, if SMB1.0 is disabled, even if the protocol version is changed to SMB1.0 with the "set nas-server" command, connections cannot be made using SMB1.0.
- If the SMB protocol version was changed to SMB1.0 or SMB2.0 with the encryption function of SMB3.0 still enabled, disable the encryption function when accessing the shared folder.
Alternate Data Stream

The NAS file system in the ETERNUS DX supports the Alternate Data Streams (ADS). Multiple data streams can be assigned to a file. When a file that includes ADS is copied via the CIFS protocol, the ADS information is stored in a different file in the ".streams" folder on the shared folder.

The ADS information cannot be preserved for the following cases.

- If the file is moved or copied to a non-ETERNUS DX file system that does not support ADS.
- If the file, regardless of whether it is in the ETERNUS DX, is moved or copied with protocols other than the CIFS protocol

Note that the access performance may be reduced if ADS information is added to a file. The maximum amount of characters that can be set with the ADS is 64KB.

Because ADS information (or Zone Identifier) is added to files that are downloaded from the Internet, copying these files to the CIFS shared folder may not be possible. In this case, confirm that the downloaded files are safe, remove the file block from the property screen, and then copy the files to the CIFS shared folder.

During the configuration phase

The ADS information cannot be preserved if the following operations are performed.
- Snapshot files are being viewed or restored.
- NAS backup volume files are being viewed.

When NAS backup volumes are restored, the ADS information is preserved only if they are restored to the existing NAS user volumes. If NAS backup volumes are restored to different NAS user volumes, the ADS information cannot be preserved.

During the operation phase

Do not use the ".streams" folder which is directly under the shared folder because it is a folder used for the NAS system.
### Displaying/Hiding Alternate Data Streams

From ETERNUS CLI, the settings can be changed to show or hide the ADS information (*.streams* folder or file). Perform the following procedure to change the settings.

**Procedure**

1. Execute the ETERNUS CLI "set nas-server" command by specifying "yes" or "no" for the "-show-cifs-ads-files" parameter.
2. Reestablish a session for the CIFS client that is to be connected.

**End of procedure**

**Caution**

**During the configuration phase**

If the ADS information is hidden, the *.streams* folder or file cannot be displayed or created in the shared folder.

### Changing the Settings for Anonymous Access

The setting to allow anonymous access for the CIFS access can be changed.

If anonymous access is used, CIFS access from the CIFS client is allowed without specifying the username and password.

Anonymous access is useful for troubleshooting or for test environments but is not recommended for normal operations.

Perform the following procedure to change the settings for anonymous access.

**Procedure**

1. Execute the ETERNUS CLI "set nas-server" command by specifying "yes" or "no" for the "-cifs-restrict-anonymous" parameter.
2. Execute the ETERNUS CLI "show nas-server" command and then check the displayed result for "CIFS restrict anonymous".

**End of procedure**

**Note**

**During the operation phase**

For Windows with a setting that does not permit anonymous access, anonymous access to the ETERNUS DX is not available.
Displaying/Hiding Files and Folders Whose Names Begin with a Dot

Dotfiles (files and folders whose names begin with a dot ".") are set with the "Hidden" attribute when stored with the default settings of the ETERNUS DX. Therefore, these files are invisible with the default settings of Windows Explorer.

For controller firmware versions V10L83 and later, the dotfiles can be shown or hidden with ETERNUS CLI. If the setting is changed to show the dotfiles, they are stored without the "Hidden" attribute. This setting shows the dotfiles even with the default settings of Windows Explorer.

Perform the following procedure to show or hide the dotfiles.

Procedure

1. Execute the ETERNUS CLI "set nas-server" command by specifying "yes" or "no" for the "-show-cifs-dot-file-folder" parameter.

2. Reestablish a session for the CIFS client that is to be connected.

Caution

During the operation phase
- Dotfiles set with the "Hidden" attribute are invisible regardless of whether the dotfiles are shown or hidden.
- To remove the "Hidden" attribute from the dotfiles, change the setting to show the dotfiles with ETERNUS CLI and then change the file attribute from the NAS client.
NFS Operation

This section describes an operation in which the NFS protocol is used.

**Note**

**During the configuration phase**

If a data write needs to be ensured, set "Synchronous I/O" so that the data is reliably written in the ETERNUS DX.

In the case where "Asynchronous I/O" is set, data may not be written immediately in the ETERNUS DX if the NFS client is used for cache or a network error occurs.

**During the operation phase**

For the procedure to mount from the NFS client, refer to "Access from NFS Clients" (page 154).

## Enabling / Disabling NFSv4.0

For the NFS protocol versions, NFSv4.0 is disabled by default.

The following procedure shows the operations for enabling or disabling NFSv4.0.

### Procedure

1. If the NAS volumes of the ETERNUS DX are mounted with NFS mount using the NFS client, unmount the NAS volume.
2. For the ETERNUS CLI "set nas-server" command, specify "enable" or "disable" for the "-nfsv4" parameter and execute.
3. Stop all server access connecting with the SAN environment.
4. Use ETERNUS Web GUI or ETERNUS CLI to reboot the ETERNUS DX.
5. Mount the NAS volumes in the ETERNUS DX from the NFS client.

**End of procedure**

### Caution

**During the configuration phase**

Be sure to reboot the storage system after using this procedure to change "enable" or "disable" for the "-nfsv4" parameter of the "set nas-server" command. If the operation is resumed without rebooting the storage system, access may stop when a failover or a failback is triggered by a controller failure.
## Note

### During the configuration phase

The enabling or disabling of NFSv4.0 can be performed when the controller firmware version is V10L51 or later.

### During the operation phase

After the hot update is complete, even if the controller firmware version is switched to a version that supports NFSv4.0 (V10L51 or later), the currently mounted NFS client will still be using NFSv2 or v3. Operations can continue as is within the usable range of NFSv2 or v3.

## Commands

Different capacity values are shown for the results of the "df" command (shows the usage status of disk drives in UNIX/Linux) and the "du" command (shows the used capacity of disk drives for the directory).

- The "df" command shows the total capacity of used and reserved areas in the file system.
- The "du" command shows the total capacity of the files that are actually used in a directory and all of the sub-directories under it.
Home Directories

A dedicated shared folder (home directory) can be obtained when a CIFS connection is used. The home directory can be accessed with Active Directory authentication or local user authentication. To use a home directory, use ETERNUS Web GUI or ETERNUS CLI to create a shared folder ("homes") for the home directory by selecting "Home Directory". The state of the home directory can be checked from ETERNUS CLI.

**Figure 8 Home Directories**

- **Access Method**
  - `\IP_address_of_the_NAS_interface\User_name`
  - Or
  - `\IP_address_of_the_NAS_interface\homes`
Quota

Quota is a function that limits drive space and the number of files used on a user, group or shared folder basis. The drive capacity can be protected from being used exclusively by a specific user, group, or shared folder by setting the upper limit of the drive space and the number of files available for the user, group, or shared folder. The Quota function allows the scale of the organization and the use of the system to be taken into consideration to realize flexible operations.

The Quota settings can be referred to from the target client.

For CIFS access, the Quota function can be used for each user or shared folder. For NFS access, the Quota function can be used for each user, group, or shared folder.

Figure 9 Quota (for Each User or Group)
Figure 10 Quota (for Each Shared Folder)

Set the upper limit drive usage for each shared folder. An alarm notification is sent to the client currently accessing the drive when the threshold is exceeded.

<table>
<thead>
<tr>
<th>Model</th>
<th>Number of Quota settings (max.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETERNUS DX100 S4/DX100 S3</td>
<td>5,000</td>
</tr>
<tr>
<td>ETERNUS DX200 S4/DX200 S3</td>
<td>10,000</td>
</tr>
<tr>
<td>ETERNUS DX500 S4/DX500 S3</td>
<td>15,000</td>
</tr>
<tr>
<td>ETERNUS DX600 S4/DX600 S3</td>
<td>20,000</td>
</tr>
</tbody>
</table>

Threshold Monitoring of Used Space

When the usage reaches the threshold set for users or groups, a notification is sent to the notification destination (SNMP Trap, e-mail, or Syslog) specified using the [Setup Event Notification] function. There are two types of thresholds: “Limit” and “Warning”. A different value can be specified for each threshold type. Also, ETERNUS SF Storage Cruiser can be used to monitor the used capacity.

- Threshold for the used capacity of drives or the number of files

  There are two threshold stages: Limit and Warning. Specify an arbitrary numeric number (capacity) for the threshold. When the configured value for the Limit threshold is exceeded, writing data and file creation becomes impossible.
Snapshot

Snapshot is a function that automatically backs up volume data at a certain point. Unlike usual backup copies, this function only copies differential data from the source volume data. Therefore, the disk space necessary for backup is reduced.

Acquiring snapshots of the NAS user volume enables file restoration from a snapshot even if a file is deleted by mistake. Data can be restored from a client.

Snapshot is a standard function of the Unified kit. It can be used regardless of whether the Advanced Copy license is registered.

Automatic and Manual are available as acquisition modes.

For necessary settings to acquire snapshots, refer to "Basic Settings for Snapshot" (page 121). For restoration operations, refer to "Snapshot Restoration" (page 129).

Data in the snapshot destination has been assigned Read only (r) for the access permission and can only be referenced from the client.

The following table shows the maximum number of snapshot generations that can be acquired and the maximum number of target volumes.

Table 6 Maximum Number of Generations (per ETERNUS DX or Volume) and Number of Target Volumes for Snapshots

<table>
<thead>
<tr>
<th>Model</th>
<th>Controller firmware version</th>
<th>Target volume number</th>
<th>Maximum number of generations (per ETERNUS DX) (°1)</th>
<th>Maximum number of generations (per volume) (°1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETERNUS DX100 S4</td>
<td>V10L71 or later</td>
<td>2</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>ETERNUS DX200 S4</td>
<td>V10L71 or later</td>
<td>4</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>ETERNUS DX500 S4</td>
<td>V10L81 or later</td>
<td>8</td>
<td>256</td>
<td>128</td>
</tr>
<tr>
<td>ETERNUS DX100 S3</td>
<td>V10L51 or earlier</td>
<td>1</td>
<td>16 (°2)</td>
<td>16 (°2)</td>
</tr>
<tr>
<td></td>
<td>V10L53 or later</td>
<td>1 (°3)</td>
<td>16 (°3)</td>
<td>16 (°3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 (°4)</td>
<td>64 (°4)</td>
<td>64 (°4)</td>
</tr>
<tr>
<td>ETERNUS DX200 S3</td>
<td>V10L31 or earlier</td>
<td>2</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>V10L33 or later</td>
<td>2 (°5)</td>
<td>64</td>
<td>64 (°5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 (°6)</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>ETERNUS DX500 S3</td>
<td>V10L31 or earlier</td>
<td>4</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>V10L33 or later</td>
<td>4</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>ETERNUS DX600 S3</td>
<td>V10L31 or earlier</td>
<td>8</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>V10L33 or later</td>
<td>8</td>
<td>256</td>
<td>128</td>
</tr>
</tbody>
</table>

°1: Maximum number of generations in the ETERNUS DX (or the total number of generations acquired in Automatic mode and the number of generations acquired in Manual mode).

°2: The maximum number of generations when CIFS connections are used is eight.

If nine or more generations of snapshots are acquired for a CIFS operation, the NAS user volumes may become inaccessible.

°3: Values when either of the following conditions is applied.

- When the Memory Extension (ETFMCA / ETMCA-L / ETDMCAU / ETDMCAU-L) is installed
- When the cache memory included in the Unified kit is installed

°4: Values when the Memory Extension (ETFMCC / ETFMCC-L / ETDMCCU / ETDMCCU-L) is installed
**5:** Number of volumes when the Memory Extension is not installed (but cache memory included in the Unified kit is installed).

**6:** Number of volumes when the controller firmware version is V10L33 or later and the Memory Extension is installed.

### NAS Snapshot Destination Volumes

To acquire snapshots, prepare snapshot destination volumes (an SDV and an SDPV). For details on volumes, refer to "**NAS Snapshot Destination Volumes** (page 23).

The following table shows the required capacity for the SDV and the SDPV (guidelines).

**Table 7 Required Capacity of SDV/SDPV (Guideline)**

<table>
<thead>
<tr>
<th>Volume</th>
<th>Required capacity (formula)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDV (*1)</td>
<td>((24 \text{ [MB]} + \text{NAS user volume capacity} \times 0.1 %) \times \text{the number of generations})</td>
</tr>
<tr>
<td>SDPV (SDP)</td>
<td>(\text{The update amount for the time interval to acquire snapshots} \times \text{the number of generations})</td>
</tr>
</tbody>
</table>

*1: The physical capacity required for creating an SDV. The logical capacity (capacity seen from the server) is the same as that of the NAS user volume.

**Figure 11 Snapshot**

- **Required SDP (SDPV) Capacity**
  
  An SDP is shared between the Snapshot and the Advanced Copy (SnapOPC/SnapOPC+) in the SAN or NAS environment. Calculate the required capacity for each respectively.
The total SDPV capacity must be larger than the total amount of data that is saved to the SDV. The total amount of data that is saved to the SDV is the sum of the following data.

- The total data that is saved by the Snapshot function
- The total data that is saved by Advanced Copy operations (SnapOPC+) in the NAS environment
- The total data that is saved by Advanced Copy operations (SnapOPC/SnapOPC+) in the SAN environment

**SDPE Capacity**

Snap Data Pool Element (SDPE) is a unit of pool area to be allocated from an SDPV to an SDV (copy destination area). When data is written to the copy destination, the SDP is divided into small units called SDPE, so that only as much as is required is used.

1GB, 2GB, or 4GB can be specified for an SDPE unit. Specify as small a value as possible, because the usage efficiency of area allocation improves as the SDPE unit becomes smaller.

The maximum SDP capacity differs depending on the specified SDPE unit. When a small value is specified for the SDPE, the maximum SDP capacity will be smaller. Because a storage area exceeding the copy source capacity (logical SDV capacity) that was specified during the SDV creation cannot be supplied, set a large value to the SDPE capacity only when the total data capacity that is to be saved to the SDV exceeds the total SDP capacity that is to be created.

**Number of SDPVs**

Multiple SDPVs with a maximum of 2TB capacity can be created. When SDPVs are created, the total capacity of the SDPVs is pooled as an SDP.

Distribute SDPVs to multiple RAID groups so that the load is not concentrated on a specific drive. In addition, distribute controlling CMs of the RAID groups where the SDPVs are created so that load is balanced.

When SDPVs are concentrated on one RAID group, the time required for restoration increases as the number of snapshot generations to acquire increases.

■ How to Check Snapshot Data

Acquired snapshot data can be verified from the client with the following methods.

**CIFS Client**

Identical to Windows shadow copy, snapshot data can be verified from the client using Explorer. Open the directory or file properties and when the [Previous Versions] tab screen is selected, a list of collected data is displayed.

**NFS Client**

After a shared folder is mounted, snapshot data can be referred to from the ".snap" directory under that shared folder.

Snapshots are saved to directories that are created using the acquisition time stamp as the name under the ".snap" directory in the shared folder.

A directory is created according to the following naming rule.

@GMT—yyyy.mm.dd—hh.mm.ss

"yyyy.mm.dd" indicates year/month/day, "hh.mm.ss" indicates the Greenwich Mean Time (GMT) and the seconds (ss) are rounded off.

For example, when "/mnt/share_dir/" is mounted as the shared folder, the snapshot of file (A) in the shared folder is acquired to the following destination (B).

A. Copy source file
B. Snapshot destination

/mnt/share_dir/.snap/@GMT—2014.06.10—09.13.00/aaa.txt (*2)

*1: "/mnt/share_dir/" is the mount point of the shared folder.

*2: "@GMT—2014.06.10—09.13.00" is the directory where the snapshots acquired at 9:13 AM on June 10, 2014 are saved.

During the operation phase

For some NFS clients, executing the "df" command may display the snapshot directory as a mount point if the following conditions are all satisfied.

- NFS mount the NFS shared folder or the CIFS/NFS shared folder.
- Execute the "df" command in the NFS client immediately after accessing the snapshot directory from the NFS client.

The snapshot directories that are output with the "df" command are automatically mounted by the NFS client. If no access is attempted from the NFS client to the snapshot directory for a certain period of time, the NFS client automatically unmounts the directory. The time to automatically unmount the directory depends on the specifications of the NFS client.

Backup

The ETERNUS DX links ETERNUS SF AdvancedCopy Manager and performs high-speed backups and restorations by using the Advanced Copy function. Each NAS user volume is copied. QuickOPC can be used for local copies. For the remote copies, Remote Equivalent Copy (REC) is available. Copying from the ETERNUS DX to other cabinets uses SAN connections to transfer data.

For details on backup and restoration of NAS volumes, refer to "ETERNUS SF Web Console Manual". For details on backup between multiple storage systems using REC, refer to "ETERNUS SF AdvancedCopy Manager Operation Guide for Copy Control Module".
Packet Trace Acquisition

When trouble occurs on the network, problems can be quickly resolved with an analysis of the network trace information to determine the cause of the trouble. In the packet trace acquisition setting, the maximum size of each file, the number to divide the file by, and the maximum length of each packet can be specified. For details on these settings, refer to "5. Packet Trace Acquisition Settings" (page 138).

After the packet trace acquisition function is used, the trace information for the packets that are transferred via the network port of the ETERNUS DX can be output and extracted. Because the trace information is output in the binary format, general packet analysis software such as WireShark can be used for network investigation.

Figure 12 Packet Trace Acquisition
File Format of Trace Information

The trace information is divided and output to a file in a system volume. In addition, file names are created according to the following naming rule.

`pcap_NASIF_yyyy-mm-dd_hh-mm-ss.pcapN`

- NASIF
  NAS interface number
- `yyyy-mm-dd_hh-mm-ss`
  Date and time (year, month, day, hour, minute, second)
- `N`
  Serial number (assigned in ascending order starting from 0)

`hh-mm-ss` indicates the time that is managed by the clock function in the ETERNUS DX.

In addition to the trace information file, the following files are output.

- `ls_cm0.txt`
- `ls_cm1.txt`

These two files contain the output results that are equal to the output results of the "ls" command that was executed for the trace information file folder.

If the dedicated account is used to log in to FTP, the trace information file can be referenced from the directory (`/pcap`) that stores the packet trace files under the home directory.
Audit Log

Audit logs are audit trail information that record operations that are executed for the ETERNUS DX and the response from the system. This information is required for auditing. The number of files for saving the audit logs can be specified. For details on these settings, refer to "Audit Log Setup" (page 132).

The audit log function enables monitoring of all operations and any unauthorized access that may affect the system.

Only audit logs for CIFS access can be acquired in NAS environments. Audit logs for NFS access cannot be acquired.

For each shared folder that is to be accessed, an audit log file is output to the expanded system volume in the ETERNUS DX. FTP is used to acquire the audit log file that is output.

For details about the audit log messages, refer to "C. Audit Log Messages" (page 184).

File Format of the Audit Log

The audit log information is output to files by shared folder and date in the expanded system volumes. In addition, file names are created according to the following naming rule.

```
audit_shared_folder_name_controller_number.log-yyyyymmdd
```

For example, if the shared folder name is "shareA", the connection destination controller is "CM#0", the acquisition date is "2015/08/20", then the file name is "audit_shareA_0.log-20150820".

However, writing the date in the file name on the day of the audit log collection is not allowed.

When the user account for the audit log FTP is used to log in, the audit log files can be referenced from the directory that stores the audit logs under the home directory.
Meta Cache Distribution

The meta cache distribution function is used to balance the file system management data (or meta cache) that is concentrated in one controller due to problems such as a NAS volume error.

When NAS volumes are created, the meta cache is deployed in the cache memory of the controller for each NAS volume. Meta cache is distributed to either CM#0 or CM#1 for each NAS volume so that the meta cache is balanced in both controllers.

If an error occurs in the NAS volume during an operation, a failover of the meta cache to the other controller is performed. The cache memory capacity in one controller becomes insufficient and the performance may be reduced if the operation continues in this condition.

Figure 14 Meta Cache Distribution

State where the meta cache is distributed to both CMs in a balanced manner (initial deployment)

State where the meta cache is unbalanced due to problems such as errors detected in the NAS volume

Your maintenance engineer may ask you to execute the meta cache distribution function during maintenance. The target volumes for the meta cache distribution function are NAS user volumes and NAS backup volumes. In addition, the meta cache distribution function can be performed automatically and manually. Automatic meta cache distribution is disabled by default.
Caution

During the configuration phase

• The meta cache distribution function can be executed manually or automatically.
  If automatic execution is selected, meta cache distribution is executed automatically on a regular basis (every hour on the half hour) and when a controller is implemented according to the imbalanced state of the meta cache. When the meta cache distribution function is executed, I/O responses may be delayed for several tens of seconds to two minutes.
  Manual execution is recommended if the I/O response delay becomes an issue.
• The meta cache may be distributed to a controller that is different from the initial deployment in the following situations.
  - When the controller or NAS engine is abnormal, or when the controller is implemented after stopping for maintenance.
  - When the ETERNUS DX is rebooted

Note

During the design phase

Accessing NAS file systems via the NAS interface of the controller where the meta cache is deployed may enhance performance. Therefore, when mounting the shared folder, set the IP address of the NAS interface that is in the same CM as the initial meta cache deployment. The initial meta cache deployment and the IP address of the NAS interface can be checked using ETERNUS Web GUI or ETERNUS CLI.

File Lock

Client Resource Deallocation

The Client Resource Deallocation function is used to forcefully release the file that is occupied by the client and check the holding state of the lock.

During a file lock state, when the client machine goes down while accessing the file or a path error occurs between the client and the ETERNUS DX, the lock that was held may remain in the controller of the failover source. If another client issues a lock request when locks are being held, the process remains in a wait state until a file lock can be acquired.

In order to resolve the issue where a client process permanently remains in a wait state, locks held by any client and locks that remain in any controller can be released. In addition, the lock state information can be acquired and displayed.

The following methods show how to release the remaining locks and how to check the lock state.
• Releasing the lock and acquiring information on the lock state through ETERNUS CLI
• Releasing the lock and acquiring information on the lock state through SSH from the operational LAN
Releasing/Displaying the Locks through ETERNUS CLI

The following table shows the specifications of the Client Resource Deallocation function that is available through ETERNUS CLI.

Table 8 Specifications of the Client Resource Deallocation Function (through ETERNUS CLI)

<table>
<thead>
<tr>
<th>Item</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported protocols</td>
<td>CIFS, NFSv3, NFSv4.0</td>
</tr>
<tr>
<td>Lock release unit</td>
<td>The client IP address or the controller (CM) that is specified</td>
</tr>
<tr>
<td>Acquisition unit of the lock state information</td>
<td>The client IP address or the controller (CM) that is specified</td>
</tr>
<tr>
<td>Maximum number of lock releases</td>
<td>100,000</td>
</tr>
</tbody>
</table>

The following procedure shows the operations for displaying the lock state and releasing the lock.

Procedure

1. Log in to ETERNUS CLI using the administrator account.
2. Execute the "show nas-lock" command.
   Confirm that the IP address of the lock release target client is displayed in the output results.
   
   **Note**
   
   During the operation phase
   The IP addresses of the clients where a possible lock is being held are displayed with the "show nas-lock" command.
   Therefore, the IP addresses of the clients where a lock is not being held may also be displayed.
   
3. Execute the "delete nas-lock" command by specifying the IP address of the client that was confirmed in Step 2.
4. Execute the "show nas-lock" command again.
   Confirm that the IP address that was specified in Step 3 is not displayed in the output results.

End of procedure
Releasing/Displaying the Locks through SSH from the Operational LAN

To release the lock through SSH from the operational LAN, PRIMECLUSTER Wizard for NAS, which is an optional product of FUJITSU Software PRIMECLUSTER, must be installed on the client.

Perform the following settings with ETERNUS CLI in preparation for releasing the lock through SSH from the operational LAN.

1. Execute the "set nas-port" command to change the state of the PRIMECLUSTER port (28950) to "OPEN".
2. Execute the "show nas-port" command to check that the state of the PRIMECLUSTER port (28950) is "OPEN".

End of procedure

For details, refer to the manual for PRIMECLUSTER Wizard for NAS.

Caution

During the operation phase

Release the lock through ETERNUS CLI if an error occurs in the ETERNUS DX or in the path to the ETERNUS DX (CA error and CA port error) or a machine down occurs while the client acquires a lock. If the lock is released through ETERNUS CLI after recovering from a failure, even though the lock was released, the lock is restored due to retries from the client and appears as though the lock was not released.

Note

During the operation phase

Releasing locks for each file or lock, and releasing locks with a specified protocol are not supported.
NFS File Lock Takeover Function

- **Takeover Process for the NAS File Lock Information**

  If the IP address for the NAS port is taken over by a different controller due to a failover/failback, the file lock information takeover process that was acquired by the NFS client is performed in the NAS system of the ETERNUS DX.

  The takeover process of the file lock information is performed only when NFSv4.0 is used to mount the volume.

  The takeover process of the file lock information is realized by re-notifying the NAS system of the NFS client's file lock information. Because of that, if the NAS system file is not re-notified from the NFS client due to the I/O load, the network environment, or the NFS client operation, the file lock information is not taken over and the file lock is released.

  While waiting for a re-notification, other than the takeover process, some operations from the NFS client are stopped.

  The grace period for the re-notification after the IP address is taken over is 100 seconds. However, the grace period may be extended to 175 seconds for the following conditions.

  - When a hot update of the controller firmware is performed
  - When a hot preventive maintenance is performed on the CM
  - When the controller is starting up
  - When the VLAN settings are being performed
  - When the NIC-CA has failed
  - When the CA port has failed

  In addition, if the failover/failback is conflicted, the takeover process of the file lock information is performed again.

  The operations in the following table are stopped during the grace period.

  **Table 9 Operations That Are Stopped during a Re-Notification Grace Period of the NFS File Lock Information**

<table>
<thead>
<tr>
<th>Operations</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NFSv3</td>
</tr>
<tr>
<td>LOOKUP</td>
<td>I/O continuation</td>
</tr>
<tr>
<td>READ/WRITE</td>
<td>I/O continuation</td>
</tr>
<tr>
<td>LOCK setting/viewing/releasing</td>
<td>I/O stop</td>
</tr>
</tbody>
</table>

- **Number of Takeovers for the NFS File Locks**

  The maximum number of file locks that can be taken over by the ETERNUS DX when a failover occurs varies depending on the model.

  **Table 10 Maximum Number of File Locks That Can Be Taken Over (per Controller)**

<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum number of file locks that can be taken over (per controller)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETERNUS DX100 S4/DX100 S3</td>
<td>500</td>
</tr>
<tr>
<td>ETERNUS DX200 S4/DX200 S3</td>
<td>1,000</td>
</tr>
<tr>
<td>ETERNUS DX500 S4/DX500 S3</td>
<td>1,000</td>
</tr>
<tr>
<td>ETERNUS DX600 S4/DX600 S3</td>
<td>1,000</td>
</tr>
</tbody>
</table>

  The maximum number of file locks that can be taken over may be significantly reduced depending on the system load and the network environment state.
During the operation phase

- A takeover process of file lock information can be performed if the controller firmware version is V10L51 or later.
- A takeover process of the file lock information is supported only if the OS of the used NFS client has verified the operation and NFSv4.0 is used.
  
  For OSs that have verified the operation, refer to "Confirmed OS" (page 14).
- If the file lock information is not re-notified from the NFS client because of a network path error, the file lock information for the target NFS client will be lost from the NAS system.
- If the lock is released during a failover/failback, the conflicting process may acquire a lock. As a result, multiple processes may unintentionally run simultaneously and the files may become damaged.
- If the NFS client OS is Solaris, the maximum number of file locks that can be taken over is approximately 200 per client. If the number exceeds 200, the lock state may not be taken over.
- For clients that connect with NFS, do not set the firewall when communicating with the ETERNUS DX. Otherwise, the NFS client cannot detect a failover/failback and the file lock information will be lost.
- If the OS of the NFS client is Solaris, disable the IP network multipathing (IPMP). If this is enabled, the NFS client cannot detect a failover/failback and the file lock information will be lost.
- If access to both controllers (CM#0 and CM#1) are disconnected at the same time because of an event such as turning the ETERNUS DX on/off, machine down recovery, or a path disconnection to both controllers (CM#0 and CM#1), the NFS file lock takeover function will not work normally.
- To enable the NFS file lock takeover function, unmount the NFS client, update the controller firmware for both controllers (CM#0 and CM#1) to V10L51 or later, and then perform the NFS mount again.
- When performing operations that include file locks, the operation cannot be guaranteed before a controller firmware update in cold mode or a downgrade of the controller firmware is performed. In this case, first unmount using the NFS client, perform an upgrade or a downgrade of the controller firmware, and then perform an NFS mount via the NFS client again.
- Operations can continue during a hot update of the controller firmware from versions earlier than V10L51 to version V10L51 or later for both controllers (CM#0 and CM#1), however the NFS file lock takeover function will not work normally. Therefore, file locking operations are not guaranteed during a hot update.
- If the "forced nas-fsunmount" command is executed, the controller that is not specified as the unmount target also enters the grace period. As a result, the I/O for the controller that is not specified as the unmount target also stops during the grace period.
- Do not mount the same shared folder in the ETERNUS DX from the same client more than once. The takeover process of the file lock information may not be performed correctly.
Performance Index

This section describes the performance index when configuring a NAS environment. Although the ETERNUS DX has sufficient throughput, the performance degrades when the load is high. Performance requirements (indices for process performance) must be taken into consideration.

The following table provides the performance requirements for the ETERNUS DX.

Table 11 Performance Requirements (during Random Access) for the ETERNUS DX

<table>
<thead>
<tr>
<th>Item</th>
<th>For a system focusing on online response</th>
<th>For a system focusing on batch throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM (CPU) busy ratio</td>
<td>80% or less</td>
<td>90% or less</td>
</tr>
<tr>
<td>Disk busy ratio</td>
<td>60% or less</td>
<td>80% or less</td>
</tr>
<tr>
<td>Response time</td>
<td>20ms or less</td>
<td>No standard value</td>
</tr>
</tbody>
</table>

The performance requirements in Table 11 are based on the items below that are measured with ETERNUS SF Storage Cruiser when the SAN function is used.

- CM (CPU) busy ratio
- CM load (CPU usage) ratio
- Disk busy ratio
- Disk usage busy ratio
- Response time

Read and Write response times for each LUN and RAID groups (ms)

Sparse File Inflation

If I/Os are performed to large capacity sparse files such as thin virtual disks, a type of VMware virtual disks, the files become fragmented and the access performance may be reduced.

The Sparse File Inflation function inflates (or overwrites the entire area with zeros) VMware virtual volumes (vmdk volumes) to prevent a reduction in access performance. When VMware virtual volumes are created, make sure to execute the Sparse File Inflation function before the volumes are used.
During the operation phase

- Do not execute the Sparse File Inflation function for the currently running virtual disks. When an inflation is performed, all areas in the file are overwritten with zeros and all existing data is deleted. The Sparse File Inflation function is used on the assumption that it inflates thin virtual disks that have just been created and do not contain any data.
- Do not perform I/Os for the files where Sparse File Inflation is being performed.
- If the NAS engine terminates with an error such as when the power to the ETERNUS DX is disconnected during an inflation, the inflation process is suspended. After the system is restored from the error, execute the "start nas-file-inflate" command of ETERNUS CLI with the "-overwrite-whole-file" option specified to perform the inflation again.
- When the inflated file is copied, the copied file is fragmented and the performance is reduced. Perform an inflation after copying.
- Files that are to be inflated using the Sparse File Inflation function are not targets for the Quota function. Therefore, the drive usage amount may exceed the limit value.
- Until the command prompt is returned after the "start nas-file-inflate" command is executed, regardless of whether the inflation is complete, the results may not be displayed correctly if the "show nas-file-inflate" command or "show nas-share-progress" command of ETERNUS CLI is executed from a different terminal. After the command prompt is returned, execute the "show nas-file-inflate" command or the "show nas-share-progress" command.
- The "start nas-file-inflate" command may terminate with an error due to a capacity shortage regardless of whether free space is available. This happens when a contiguous large area cannot be secured and a reduction in access performance cannot be prevented. Delete large unnecessary files or add disks.
- When sparse files in the Thin Provisioning NAS volume are inflated, the physical area will be secured for the capacity of the sparse files that are overwritten with zeros. Therefore, when a snapshot of the ETERNUS DX is acquired for the NAS user volume that includes inflated files, the areas that are overwritten with zeros are also detected as differential data.
- To use VMware, refer to the following notes.
  - In the following cases, the inflation status of xxx-flat.vmdk is output. This does not affect the inflation results.
    - xxx.vmdk is specified for the "show nas-file-inflate" command.
    - The "show nas-share-progress" command is executed while xxx.vmdk is being inflated.
  - From the beginning of the inflation, the inflation target file is seen as a thick virtual disk in the datastore browser of VMware vSphere Web Client, but the inflation is not complete. Make sure that the inflation process is complete with the "show nas-file-inflate" command before using the file.
  - When inflated thin virtual disks and the virtual machine that has those thin virtual disks are cloned with VMware functions (such as vMotion), files in the vMotion destination are fragmented and performance is reduced.
  - Do not use the VMware "Inflate" function because files may become fragmented.
During the operation phase

The relative path from the shared folder to the thin virtual disk is "[datastore name]/[VM name]/[VM name].vmdk" for VMware vSphere ESXi 5.5. For VMware vSphere Web Client 6.0, use the following procedure for checking.

The relative path may differ depending on the VMware vSphere version. For details, refer to the manual for VMware vSphere Web Client.

1. Select "Datacenters" that is in the left pain of VMware vSphere Web Client.
2. Select "Datastores".
3. In the "Datastores" field, select the name of the datastore that is to be used by the target virtual machine.
4. Select the "Manage" tab.
5. Select the "Files" tab.
6. Select the name of the target virtual machine.

Check the path to the thin virtual disk.

Path to the thin virtual disk

Example: If "[dx_datastore]vm_on_dx" and "vm_on_dx.vmdk" are displayed, the path is "dx_datastore/vm_on_dx/vm_on_dx.vmdk".

The following procedure shows how to inflate a thin virtual disk of the newly-created virtual machine.

Procedure

1. Create a new virtual machine.
2. Execute the "start nas-file-inflate" command of ETERNUS CLI to start the inflation.

The following example is for when vm/myvm.vmdk that is in shared folder "SHARE#3" is inflated.

```
CLI> start nas-file-inflate -share-name SHARE#3 -path vm/myvm.vmdk
```
3 Execute the "show nas-file-inflate" command of ETERNUS CLI.
When "Full" is displayed for File Allocation Status, the inflation process is complete.

<table>
<thead>
<tr>
<th>Share No.</th>
<th>[3]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share Name</td>
<td>SHARE#3</td>
</tr>
<tr>
<td>File Path</td>
<td>vm/myvm-flat.vmdk</td>
</tr>
<tr>
<td>Provisioned Size(KB)</td>
<td>131584</td>
</tr>
<tr>
<td>File Allocation Status</td>
<td>Full</td>
</tr>
<tr>
<td>Inflate Progress</td>
<td>[-]</td>
</tr>
</tbody>
</table>

4 Install the OS in the virtual machine and start operations.

End of procedure
3. Connection Interface Configuration

Ethernet is used for a NAS interface (NIC-CA). The server and the ETERNUS DX can be connected directly or via a switch.

NAS Interface (NIC-CA)

This section describes the NAS interface specifications. Host interfaces with two different maximum transfer rates (10Gbit/s and 1Gbit/s) are available for Ethernet (NIC-CA).

Disable the Spanning Tree Protocol (STP) function for the switch. If the STP function is enabled, connections with the ETERNUS DX may fail.

- **Operation Mode**
  The Ethernet 10Gbit/s operation mode is 10GBASE-SR. Set "Auto-negotiation" for the transfer rate.
  The Ethernet 1Gbit/s operation mode is 1000BASE-T Full Duplex (FULL) or 100BASE-TX Full Duplex (FULL). The transfer rate can be selected from fixed setting or Auto-negotiation.

- **Internet Protocol**
  IPv4 and IPv6 are supported.

- **VLAN**
  The tag VLAN function is supported. The number of NAS interfaces, including tag VLANs (VLAN ID), that can be set for the whole system in the NAS environment is shown in the table below. Distribute VLAN IDs across the controllers so that VLAN IDs are not concentrated in one controller.

<table>
<thead>
<tr>
<th>Model</th>
<th>Number of available NAS interfaces (per ETERNUS DX)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETERNUS DX100 S4/DX100 S3</td>
<td>40</td>
</tr>
<tr>
<td>ETERNUS DX200 S4/DX200 S3</td>
<td>160</td>
</tr>
<tr>
<td>ETERNUS DX500 S4/DX500 S3</td>
<td>160</td>
</tr>
<tr>
<td>ETERNUS DX600 S4/DX600 S3</td>
<td>160</td>
</tr>
</tbody>
</table>

- **Caution**

  During the configuration phase
  - Since the maximum number of VLAN IDs that can be configured depends on the number of NAS interfaces, the ports that do not use VLAN (with no VLAN ID setting) are also counted as VLAN IDs.
  - Port VLAN is not supported for connections between an ETERNUS DX and a switch.
- **Jumbo Frame**
  Enabling Jumbo Frame increases the amount of data that can be transferred for each Frame. The range that can be set is from 1,280 to 9,000 bytes.

### Note

**During the configuration phase**

The targets are different for specifiable MTUs in the Jumbo Frame and Large MTUs that are supported in SMB3.0.

For Jumbo Frame, the size of the data transmission unit of the Ethernet (frame) is specified.

Large MTU is a data transmission unit that can be delivered through a network when transferring files using the CIFS protocol.

- **Firewall**

  Firewall settings can be configured for each port with the following network protocols.

<table>
<thead>
<tr>
<th>Table 13 NAS Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usage</strong></td>
</tr>
<tr>
<td>NFSv3</td>
</tr>
<tr>
<td>NFSv4.0</td>
</tr>
<tr>
<td>CIFS</td>
</tr>
<tr>
<td>CIFS</td>
</tr>
<tr>
<td>LDAP</td>
</tr>
<tr>
<td>RIP (IPv4)</td>
</tr>
<tr>
<td>RIP (IPv6)</td>
</tr>
<tr>
<td>ICMP</td>
</tr>
<tr>
<td>FTP</td>
</tr>
<tr>
<td>FXP</td>
</tr>
<tr>
<td>Local User Password</td>
</tr>
<tr>
<td>PRIMECLUSTER</td>
</tr>
</tbody>
</table>

*1: The CIFS client uses the same port number.
During the configuration phase

- For the NAS system of the ETERNUS DX, "0528:866c:29ce:4005:3b03:9764:ed89:e3f1/126" is used as an IPv6 address. Therefore, connections with servers and clients with IP addresses within the range of "0528:866c:29ce:4005:3b03:9764:ed89:e3f1/126" are not possible.

- When the NFSv3 protocol is used in a firewall environment, set the firewall so that communication is possible between the NAS interface and the NFS client.

  For communication from the NFS client to the NAS interface, enable ports 2049 / 111 / 28900 / 28901 / 28902 / 28903 (TCP/UDP).

  For communication from the NAS interface to the NFS client, using ports 2049 / 111 (TCP/UDP) or the port mapper to enable communication for the port and protocol that are assigned dynamically to the NFS related daemon is required.

  The ports/protocols that are assigned to the NFS related daemon depend on the settings of the NFS client. Check the settings of the NFS client.
Redundant Method

This section explains a NAS connection and also a configuration with a NAS connection for the ETERNUS DX.

**IMPORTANT**

During the configuration phase
Specify an IP address in a different subnet for each NAS port in the same controller.

Single Path Connection

For a single path connection, only one controller is connected to the NAS network.

If an error occurs on the path of a connected controller, client access cannot be performed. The system must be stopped during the replacement of failed components and controller firmware.

For a single path connection, the failover function cannot be used.

**Figure 15 Single Path Connection (When a NAS Connection Is Used)**

Multipath Connection (Active-Active Connection)

A Multipath connection (Active-Active connection) is a configuration in which two controllers are connected to the same NAS network. System reliability is improved due to the path redundancy.

If a link down occurs in a connected controller, access can be continued by switching to another controller via the failover function.

Even when a controller or NIC-CA fails, operation can continue by giving the information to the normal controller. After a failed component is replaced with a normal component, the connection type returns to the previous settings.

During operation, each client can use the paths of both controllers to access the same volume.

While a client is writing to a file (the file is open), the access permission of the file is set to Read only (r) for requests to open the same file from the other path.
During the configuration phase

- A different IP address on the same subnetwork must be set for the redundant port.
- A configuration with an Active-Standby connection is not supported.

During the operation phase

- During a multipath connection, if a failover or a failback is performed due to a controller failure or a path error, the path that is being accessed becomes temporarily offline and the access path switch occurs. While the access path is being switched, NFS access sessions can continue the current connection, but CIFS access sessions are temporarily disconnected. In addition, even for NFS access, a timeout may occur depending on the retry count setting and the session may be disconnected.
- If paths are switched during CIFS access, wait for a while and try again. Note that access can be immediately resumed by issuing a command (such as dir) that checks drives.
- The failover function for the NAS interface (NIC-CA) does not work if the operation management LAN ports (MNT port/RMT port) have failed.
- An NFS access error or a response failure may occur in the following cases.
  - When the IP address of the NAS port is taken over due to a failover or a failback
  - When a NAS user volume or NAS backup volume is mounted or unmounted

If an error occurs, re-execute the application with the NFS client. If an error or a response failure occurs when re-executing the application, restart the NAS client.

The following table shows the relevant OSs.

<table>
<thead>
<tr>
<th>NFS protocol</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFSv3</td>
<td>Red Hat Enterprise Linux 6</td>
</tr>
<tr>
<td></td>
<td>Solaris 11</td>
</tr>
<tr>
<td></td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td>HP-UX</td>
</tr>
<tr>
<td>NFSv4.0</td>
<td>Red Hat Enterprise Linux 6 (6.7 or later)</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7.0</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7.1</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7.2</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7.3</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7.4</td>
</tr>
<tr>
<td></td>
<td>Solaris 10</td>
</tr>
<tr>
<td></td>
<td>Solaris 11</td>
</tr>
</tbody>
</table>

- If the ETERNUS DX is used as a VMware datastore, the IP address of the NAS port may be taken over due to a failover or a failback, and the following events may occur during a VM snapshot acquisition.
  - Virtual machines are powered off, rebooted, or enter an unresponsive state.
  - VM snapshot acquisitions fail.
  - OS installations to virtual machines fail.

If problems such as these occur, check that a failover or failback is not being performed for the IP address of the ETERNUS DX, and reboot the virtual machine or perform the failed operation again.
**During the operation phase**

If an error occurs on one of the two ports that are set for redundancy by the multipath connection settings and the path cannot be accessed, the IP address is taken over by the other port.

For example, when a controller or NIC-CA error occurs on the CM#0 side (IP address: 192.168.2.1) in the connection configuration shown in Figure 16, the paired ports on the CM#1 side (IP address: 192.168.2.2) takes over the processes for the CM#0 side and receives access to both 192.168.2.1 and 192.168.2.2.

**Estimated Required Time for Failover or Failback**

The time it takes for a failover or a failback varies depending on the events that occurred, the OS used, and the network environment or configuration.

The following table shows the estimated required time.

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Estimated required time</th>
</tr>
</thead>
<tbody>
<tr>
<td>When an error is detected in a NAS port or a path (*1)</td>
<td>Approx. 1 minute</td>
</tr>
<tr>
<td></td>
<td>Approx. 1 minute + 100 or 175 seconds (*2)</td>
</tr>
<tr>
<td>- When an error is detected in a controller or a NIC-CA</td>
<td>Approx. 3 minutes</td>
</tr>
<tr>
<td>- When a NIC-CA is replaced (for the ETERNUS DX500 S4/DX600 S4 and the ETERNUS</td>
<td>Approx. 3 minutes + 100 or 175 seconds (*2)</td>
</tr>
<tr>
<td>DX500 S3/DX600 S3)</td>
<td></td>
</tr>
<tr>
<td>- When a preventive maintenance is performed for a controller</td>
<td>For NFS operations (including CIFS/NFS operations)</td>
</tr>
<tr>
<td>- When components are replaced in a controller</td>
<td>Approx. 3 minutes + 100 or 175 seconds (*2)</td>
</tr>
<tr>
<td>- When a memory expansion is performed for a controller</td>
<td>Approx. 5 to 10 minutes + 100 or 175 seconds (*2) (*3)</td>
</tr>
<tr>
<td>- When a hot update of the controller firmware is performed</td>
<td>Only for CIFS operations</td>
</tr>
<tr>
<td>- When a NIC-CA is replaced (for the ETERNUS DX100 S4/DX200 S4 and the ETERNUS</td>
<td>Approx. 3 minutes</td>
</tr>
<tr>
<td>DX100 S3/DX200 S3)</td>
<td></td>
</tr>
</tbody>
</table>

*1: For NFS operations (including CIFS/NFS operations)
*2: Approx. 5 to 10 minutes + 100 or 175 seconds
*3: Only for CIFS operations
**1:** The estimated time when an error is detected in a NAS port.
   If errors occur in multiple ports, time is required to switch each port after errors are detected.

**2:** Required time including the grace period for NFS operations
   For NFS operations, a grace period is required after a failover or a failback. For details, refer to "NFS File Lock Takeover Function" (page 61).

**3:** Time required for the following cases
   - If the controller firmware version is V10L51 or V10L53
   - If NFSv4.0 is enabled and the controller firmware version is V10L61 or later
   For more details on enabling and disabling NFSv4.0, refer to "Enabling / Disabling NFSv4.0" (page 45).

---

**Note**

If an IPv6 address is used, detection of the access path switch is delayed in the client OS and the access downtime may be longer than the estimated time described in Table 14.

---

**Bonding**

Bonding is a function that creates a single virtual network interface from NAS ports in the ETERNUS DX for communication. By expanding the communication bandwidth, efficient load balancing is realized and performance is improved. In addition, fault tolerance is improved with port duplication. Even if an error occurs in a port or cable with the Bonding setting, communication can be continued with other ports.

Figure 17 Bonding

---

**Note**

During the configuration phase
Bonding cannot be configured by NAS ports in different controllers. Make sure to select NAS ports in the same controller.
Bonding Operation Mode

Six operation modes are available for Bonding. Select the appropriate mode according to the usage. Using Mode 4 is recommended when there are no special requirements.

The following table shows the features of each mode.

### Table 15 Features of the Bonding Operation Mode

<table>
<thead>
<tr>
<th>Mode</th>
<th>Name</th>
<th>Performance improvements (load balancing)</th>
<th>Fault tolerance</th>
<th>Functions required for the switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>balance-rr</td>
<td>○ (transmission) × (reception)</td>
<td>○ (transmission)</td>
<td>Ether Channel</td>
</tr>
<tr>
<td>1</td>
<td>active-backup</td>
<td>× (transmission), ○ (reception)</td>
<td>○ (transmission)</td>
<td>IGMP</td>
</tr>
<tr>
<td>2</td>
<td>balance-xor</td>
<td>○ (*1) (transmission), × (reception)</td>
<td>○ (transmission)</td>
<td>Ether Channel</td>
</tr>
<tr>
<td>4</td>
<td>802.3ad</td>
<td>○ (*1) (transmission), × (reception)</td>
<td>○ (transmission)</td>
<td>LACP (IEEE 802.3ad)</td>
</tr>
<tr>
<td>5</td>
<td>balance-tlb</td>
<td>○ (transmission), × (reception)</td>
<td>○ (transmission)</td>
<td>IGMP</td>
</tr>
<tr>
<td>6</td>
<td>balance-alb</td>
<td>○ (transmission), △ (*2) (reception)</td>
<td>○ (transmission)</td>
<td>IGMP</td>
</tr>
</tbody>
</table>

○: Possible ×: Impossible △: Partially supported —: N/A

*1: With the Exclusive-OR (XOR) operation, packets are transferred using the NAS port that matches the MAC address of the incoming request. Because load balancing methods depend on the XOR operation, communications traffic may be unbalanced.

*2: Load balancing during reception is not performed for ports specified with IPv6 addresses.

- **Mode 0 (balance-rr)**
  Enables performance improvements (load balancing). All NAS ports are used in a rotation (round-robin) for transmitting. Reception depends on the switch setting.
  The switch must have the Ether Channel function. For some switches, Ether Channel is also called "port trunking" or "link aggregation".
  Connect the ETERNUS DX and the switch directly. Note that settings may be required for some switch models. For details, refer to relevant manuals of the switch.

- **Mode 1 (active-backup)**
  Dedicated to the duplication function. One NAS port is used to transfer packets during normal operation. If an error occurs in the active port, a different port is used.
  Connecting a different switch to each port can improve fault tolerance. The switch to be connected must support Internet Group Management Protocol (IGMP).

- **Mode 2 (balance-xor)**
  Enables performance improvements (load balancing). In transmission, data is distributed according to the settings in the connection destination. Reception depends on the switch setting.
  The switch must have the Ether Channel function. For some switches, "Ether Channel" is also called "port trunking" or "link aggregation".
  Connect the ETERNUS DX and the switch directly. Note that settings may be required for some switch models. For details, refer to relevant manuals of the switch.

- **Mode 4 (802.3ad)**
  Enables performance improvements (load balancing). Data is distributed according to the methods compatible with the IEEE 802.3ad Dynamic link aggregation standards. Ports used for receiving and transmitting are determined by multiple information.
Use a switch compatible with IEEE 802.3ad Link Aggregation.

Connect the ETERNUS DX and the switch directly. Note that settings may be required for some switch models. For details, refer to relevant manuals of the switch.

- **Mode 5 (balance-tlb)**
  Enables performance improvements (load balancing). Transmission performs a load balance dynamically according to the speed (load status) of each NAS port. Only one port is used for receiving at any time.

Connecting a different switch to each port can improve fault tolerance. The switch to be connected must support Internet Group Management Protocol (IGMP).

- **Mode 6 (balance-alb)**
  Enables performance improvements (load balancing). In addition to the Mode 5 (balance-tlb) function, load balancing is also performed when receiving data. In reception, data is distributed according to the settings in the connection destination.

Connecting a different switch to each port can improve fault tolerance. The switch to be connected must support Internet Group Management Protocol (IGMP).

### Note

**During the configuration phase**

Set the same transfer rate and transfer mode for interface ports configured in the single Bonding. Combining interface ports with differing transfer rates and transfer modes is not recommended.

### Recovery Requirements After a Link Down State for All Member Ports

Specify "1" for the "linkaggregation collecting minimum count" in the switch setting. If a value other than "1" is set, the operation may not work correctly. For switches other than the Fujitsu SR-X series, this set item may have different names and specifications.

For example, if "1" is specified for the "linkaggregation collecting minimum count" when four ports are used to configure Bonding, the Bonding function remains enabled until all of the four ports become unavailable. When one of the failed ports is restored for communication after all of the ports have failed, the Bonding function is enabled.

The requirements to recover communication using the Bonding function after all ports have failed are shown in the following table. Note that a failback condition is applied when a multipath connection is configured with Bonding.

**Table 16 Recovery Requirements After a Link Down State for All Member Ports**

<table>
<thead>
<tr>
<th>Firmware version</th>
<th>Whether or not the multipath configuration has been configured with Bonding</th>
<th>Bonding mode</th>
<th>Recovery requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>V10L21</td>
<td>No</td>
<td>Other than Mode 4 (802.3ad)</td>
<td>Any one port must be linked up</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mode 4 (802.3ad)</td>
<td>All member ports must be linked up</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Any mode</td>
<td>All member ports must be linked up</td>
</tr>
<tr>
<td>V10L31 or later</td>
<td>No</td>
<td>Any mode</td>
<td>Any one port must be linked up</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Any mode</td>
<td>All member ports must be linked up</td>
</tr>
</tbody>
</table>
Multipath Connection When Using Bonding

To configure a multipath connection, set multipath with master ports with the Bonding setting. For ports configured with a multipath connection, IP addresses in the same subnet must be specified.

The following shows an example of a connection when bundling two NAS interface ports by Bonding, defining two VLANs for the virtual devices, and configuring a multipath (Active-Active connection).

Figure 18 Multipath Connection When Using Bonding
During the operation phase

The following description shows how the failover works when ports are set for redundancy using a multipath connection and configured with two sets of Bonding groups each with two ports.

Configure a multipath using ports with the same port number:
- CM#0 CA#1 Port#0 and CM#1 CA#1 Port#0
- CM#0 CA#1 Port#1 and CM#1 CA#1 Port#1
- CM#0 CA#1 Port#2 and CM#1 CA#1 Port#2
- CM#0 CA#1 Port#3 and CM#1 CA#1 Port#3

Configure a Bonding group using neighboring ports:
- CM#0 CA#1 Port#0 and CM#1 CA#1 Port#1
- CM#0 CA#1 Port#2 and CM#1 CA#1 Port#3
- CM#1 CA#1 Port#0 and CM#1 CA#1 Port#1
- CM#1 CA#1 Port#2 and CM#1 CA#1 Port#3

If each Bonding group connects to a different system (segment) and one of the ports become inaccessible, the other Bonding group port continues the connection.

If Port#0 cannot be accessed, continued access is performed with Port#1 and a failover is not performed.

If the other port also becomes inaccessible, the failover function is executed, and the IP address is taken over by a port of a different controller. In this case, the other Bonding groups (B and D) are not affected by this operation.
Network Path Control

To connect multiple subnetworks to networks in the NAS environment, configure the appropriate path information between the ETERNUS DX and the client. If the settings are not correct, path control does not work and connection fail or data transfer takes long time because the appropriate path is not selected.

If the NAS interface of the ETERNUS DX is accessed from a client in a different network via a gateway device, one of the following settings is recommended.

- Setting a single NAS interface in the controller (CM)
  Set a gateway from the NAS interface settings.
- Setting multiple NAS interfaces in the controller (CM)
  Perform one of the following settings:
  - Set the static route information.
  - Enable the RIP setting (enabled by default).
  - Enable the RIP setting and set the static route information.

Configure a network so that the same NAS interface is used to send and receive traffic from the client. Network configurations that use different NAS interfaces to send and receive traffic (asymmetric routing) are not supported.

Do not set multiple gateways in one controller using the NAS interface settings. If multiple gateways are set in a single controller, the default gateway may change to any one of the gateways due to, for example, a firmware change and the network connection may fail.

Do not specify a gateway, instead use RIP settings and static route information to specify paths even when connecting to different networks through a gateway device.
FTP/FXP

Shared folders can be accessed using the File Transfer Protocol (FTP) and the File eXchange Protocol (FXP).

Up to five shared folders can be published using FTP.

For FXP, data in the shared folder can be transferred between ETERNUS DX storage systems.

For access using FTP and FXP, a user authentication in the authentication servers (Active Directory authentication servers and LDAP authentication servers) or an account that is registered in the local user authentication setting is required.

Figure 19 FTP/FXP

When the user account that is registered in the authentication servers is used for the FTP login, the shared folders that are published in the home directory can be accessed. Files in the folder can be downloaded and can be uploaded to shared folders.
Caution

During the operation phase

- Both active mode and passive mode can be used as the connection mode for FTP and FXP.
- A total of 50 sessions can be accessed with FTP and FXP at the same time.
- Volumes for snapshots and backup volumes cannot be accessed with FTP connections.
- Encrypted communications (FTPS/SFTP/FXSP) are not supported.
- If a failover or failback occurs during an FTP, the connection is disconnected and must be reconnected from the FTP client side.
- In the ETERNUS DX100 S3, if NAS FTP is used at the same time with the I/O of NFS or with the I/O of CIFS, the CPU Busy rate may reach 100% and the FTP session may disconnect.
  If an error message (for example: No control session for command) is displayed on the FTP client side when an FTP session disconnects, perform the I/O via FTP again.
- For NAS FTP, if a large quantity of small files were written (with a PUT operation) continuously (for example: tens of thousands of files with tens of KB were written), FTP may be terminated abnormally according to the OS/FTP tools’ specification on the FTP client side.
  If FTP is terminated abnormally and an error message (for example: Could not bind the data socket: Address already in use) is displayed on the FTP client side, continue process after dividing the number of files.
4. NAS Environment Configuration

This chapter explains how to configure a NAS environment for an ETERNUS DX. The Thin Provisioning function must be enabled in advance because it is used to operate NAS volumes.

This chapter explains general setting operations with ETERNUS Web GUI.

To configure a NAS environment, the following settings are required:

- **Thin Provisioning Pool (TPP) Creation**
  Prepare a pool that is used to create NAS volumes. For details, refer to "Thin Provisioning Pool (TPP) Creation" (page 83).

- **NAS Volume Creation**
  Create TPVs that are used as NAS volumes. For details, refer to "NAS Volume Creation" (page 84).

- **Bonding Settings**
  Create a single virtual network interface from the NAS ports in the ETERNUS DX. For details, refer to "Bonding Settings" (page 86).

- **NAS Interface Settings**
  Create information on the interface for NAS network connection. Configure here when duplicating NAS ports and performing a multipath connection (Active-Active connection). For details, refer to "NAS Interface Settings" (page 89).

- **VLAN Settings**
  Perform the tag VLAN settings. This settings can be performed at the same time as a NAS interface creation. For details, refer to "VLAN Settings" (page 92).

- **Authentication Server Settings**
  Set the authentication server that is used to control access to the NAS environment. For details, refer to "Authentication Server Settings" (page 97). For using local user authentication, refer to "Local User Authentication Settings" (page 100).

- **Local User Authentication Settings**
  Perform a local user authentication setting. For details, refer to "Local User Authentication Settings" (page 100). For using the authentication server, refer to "Authentication Server Settings" (page 97).

- **Shared Folder Creation (CIFS/NFS)**
  Create a shared folder that is used to access NAS user volumes via CIFS/NFS. For details, refer to "Shared Folder Creation (CIFS/NFS)" (page 105).

- **Home Directory Settings**
  If the used protocol is CIFS, a home directory can be used. For details, refer to "Home Directories" (page 110).

- **Quota Settings**
  Perform the settings to limit drive space and the number of files used on a user, group, or shared folder basis. For details, refer to "Quota Settings" (page 115).
● **Snapshot Settings**

Perform the settings to back up volume data at a regular interval according to the day of the week. For details, refer to "Snapshot Settings" (page 121).

● **Audit Log Setup**

Perform the settings to collect the audit logs for the CIFS access. For details, refer to "Audit Log Setup" (page 132).

● **Meta Cache Distribution Settings**

Set the parameters to perform a meta cache distribution. For details, refer to "Meta Cache Distribution Settings" (page 135).

---

**Caution**

**During the configuration phase**

When "Authentication Server Settings" or "Shared Folder Creation" is performed, communication is established between the ETERNUS DX and the authentication server. Make sure that both of the controllers can communicate with the authentication server before setting authentication servers and creating shared holders.

Each controller must satisfy the following three conditions in order for the ETERNUS DX storage systems to communicate with the authentication server.

- IP addresses are assigned to one or more ports in the NAS interface settings.
- NAS ports are ready for communication with (linked up to) the authentication server.
- The multipath is configured with a multipath connection (Active-Active connection).

Note that a configuration with an Active-Standby connection is not supported.

If the above conditions are not satisfied and communication errors occur, satisfy these conditions and perform the settings again.
Thin Provisioning Pool (TPP) Creation

Create a TPP that is used to register NAS volumes. The Thin Provisioning function must be enabled in advance. For more details, refer to "ETERNUS Web GUI User's Guide".

In addition, NAS volumes can be created in an existing pool. The creation procedure is the same as when TPPs are created for a SAN.

The procedure to create a TPP is as follows:

1. Click the [Thin Provisioning] tab on the navigation of the ETERNUS Web GUI screen.
   The [Thin Provisioning Pool] screen appears.

2. In [Action], click [Create].
   The [Create Thin Provisioning Pool] screen appears.

3. In [Name], enter the name of the Thin Provisioning Pool that is to be registered. Then select "Automatic" or "Manual" for "Create Mode".
   When "Automatic" is selected, the settings for "Automatic Setting" are displayed.
   When "Manual" is selected, the settings for "Manual Setting" are displayed.

4. Set the required items and click the [Create] button.

   ![Create Thin Provisioning Pool](image)

   A confirmation screen appears.

5. Click the [OK] button.
   The TPP is registered and the registration completion screen appears.
NAS Volume Creation

Create NAS volumes in the TPP.

**Caution**

**During the configuration phase**

- One file system is created for each NAS volume. A system management area (300GB) is required for each file system. If a sufficient physical area cannot be secured for the system management area, NAS volumes cannot be created. In addition, specify a 100GB or larger user area.

  Take the system management area and the root reserved area into consideration when estimating the NAS volume capacity. For details, refer to "File System Specification" (page 24).

- To create NAS volumes with ETERNUS Web GUI, use the [Volume] screen. NAS volumes cannot be created by selecting [Create Volume] in the [Thin Provisioning Pool] screen.

The procedure to create a NAS volume is as follows:

**Procedure**

1. Click the [Volume] tab on the navigation of the ETERNUS Web GUI screen.
   The [Volume] screen appears.

2. In [Action], click [Create].
   The [Create Volume] screen appears.
3. Set the required items in the [Create Volume] screen and click the [Create] button.

- Type
  Select [NAS Volume].

- Capacity
  Specify a capacity that includes the system management area (300GB). The minimum capacity is 400GB; the system management area and 100GB for the user management area.

- NAS FS Block Size
  Select the file system block size.

A confirmation screen appears.

4. Click the [OK] button.
The volume is created and the registration completion screen appears.

5. Click the [Done] button.
The screen returns to the [Volume] screen.

End of procedure
This section provides the required procedure to configure Bonding.

Create a single virtual network interface from the NAS ports in the ETERNUS DX to use the Bonding function. Up to 15 member ports can be set for a single master port.

The following procedure is an example of setting the Bonding mode to mode6 for CM#0 CA#1 Port#0 as the master port, and CM#0 CA#1 Port#1, CM#0 CA#1 Port#2, and CM#0 CA#1 Port#3 as member ports.

**Procedure**

1. Set the necessary parameters and execute the "set nas-bonding" command of ETERNUS CLI.

   ```
   set nas-bonding -master-port 010 -member-port 011,012,013 -mode 6 -hash-policy L23
   ```

   **-master-port**

   Specify a port that is to become the master port.
During the configuration phase
• The following ports cannot be specified.
  - Non-NAS ports
  - Ports that are set as member ports
  - Ports in which multipathing is configured
• When Bonding is configured to a port for the first time, the NAS interface port setting is deleted from the specified port.
  When the specified port has already been configured with Bonding, the NAS interface port setting is maintained.

-members-port
Optional. Specify a port that is to become a member port. Multiple ports can be specified by separating each port with a comma (,). When adding member ports, specify only the ports that are to be added. Specifying ports that have already been set as member ports of the target master port does not cause an error.

During the configuration phase
• The following ports cannot be specified.
  - Non-NAS ports
  - Ports that are set as master ports
  - Ports that are set as member ports of other master ports
  - Ports in which multipathing is configured
  - Ports that are in a CM that is different from the master port.
  - The NAS interface port setting is deleted from the ports that are specified as member ports.

-mode
Optional. Specify the Bonding mode.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>balance-rr</td>
</tr>
<tr>
<td>1</td>
<td>active-backup</td>
</tr>
<tr>
<td>2</td>
<td>balance-xor</td>
</tr>
<tr>
<td>4</td>
<td>802.3ad</td>
</tr>
<tr>
<td>5</td>
<td>balance-tlb</td>
</tr>
<tr>
<td>6</td>
<td>balance-alb</td>
</tr>
</tbody>
</table>

-hash-policy
Optional. Specify a hash policy. If omitted, a policy equivalent to L2 is set.
### Caution

**During the configuration phase**

The setting is enabled only when 2 (balance-xor) or 4 (802.3ad) is set for -mode. However, if -mode is a value other than 2 or 4, the specification is available but the setting will be ignored.

<table>
<thead>
<tr>
<th>Hash policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2</td>
<td>Layer2 (default)</td>
</tr>
<tr>
<td>L23</td>
<td>Layer2+3</td>
</tr>
<tr>
<td>L34</td>
<td>Layer3+4</td>
</tr>
</tbody>
</table>

---

End of procedure
NAS Interface Settings

Set the connection information for the NAS interface (NIC-CA) and create the NAS network interface. To perform a multipath configuration in order to use the failover function, set which redundant ports are used.

Caution is necessary for configurations when connecting to multiple networks through a gateway. Refer to cautions in "Network Path Control" (page 78).

During the configuration phase

- When a NAS interface is created or changed, the NAS engine in the ETERNUS DX automatically restarts the CIFS access service. CIFS client access may be unavailable for a few tens of seconds. If data cannot be written with the CIFS access, wait for a while and then try again.
  - NFS access is available regardless of whether CIFS access is available or not.
- System volumes must be created in advance to perform the settings for the NAS interface. System volumes are automatically created when the NAS volume is created for the first time. The following configurations cannot be performed if no system volumes ($SYSVOL1, $SYSVOL2, and $SYSVOL3) are created in the ETERNUS DX.
  - NAS interface settings
  - Authentication server settings

Procedure

1. Click the [Connectivity] tab on the navigation of the ETERNUS Web GUI screen, and then click "NAS" – "NAS Interface" in [Category].
   - The [NAS Interface] screen appears.

2. In [Action], click [Create].
   - The [Create NAS Interface] screen appears.
Set the required items in the [Create NAS Interface] screen and click the [Create] button.

- Port
  Select which port to set as the NAS interface.

- RIP Setting
  Set whether to receive the routing information via the Routing Information Protocol (RIP). To receive it, select "Enable".

- Redundant Port
  Select which redundant port to use with the port for the multipath configuration (Active-Active connection). For a redundant port, select a port in the controller that is different from the target port. If a multipath configuration is not used, select "None".

  When configuring redundant ports to perform a multipath connection, follow the procedure below to configure each of the ports that are paired for multipathing.

  (1) When configuring a redundant port for one of the ports, select "None" for "Redundant Port" and specify the IP address for the NAS interface.

  (2) When configuring a redundant port for the other port, select the NAS interface port that was created in Step (1) for "Redundant Port". In addition, specify an IP address that is on the same subnet network but one that is different from the port specified in Step (1).

  The IP addresses that are configured for the paired ports must be the same type (IPv4 addresses or IPv6 addresses).

  **During the configuration phase**
  - Configure redundant ports while the two target ports are linked up.
  - Multipathing cannot be configured with ports in the same controller.

- IP Address
  Set the IP address for the NAS interface.

  To specify an IPv4 address, set "IP Address", "Subnet Mask", and "Gateway".

  To specify an IPv6 address, set "IPv6 Link Local Address", "IPv6 Connect IP Address", "IPv6 Gateway", and "IPv6 Prefix length".
During the configuration phase
For multipath connections (Active-Active connections), set a different IP address on the same subnet-network in each controller port for redundancy.

A confirmation screen appears.

4. Click the [OK] button.
The NAS interface is created and the registration completion screen appears.

5. Click the [Done] button.
The screen returns to the [NAS Interface] screen.

End of procedure
This section provides the necessary procedure to configure VLAN. Use the NAS interface settings function to perform the basic settings to use the VLAN function.

During the configuration phase
- To use VLAN and Bonding at the same time, complete the Bonding setup and then perform VLAN configuration. Bonding configures one virtual network from multiple NAS ports. VLANs must be created in this virtual network.
- Distribute VLAN IDs across the controllers so that VLAN IDs are not concentrated in one controller.
- Do not specify an IP address on the same subnet for each NAS interface (including the VLAN settings) in the same controller.

Do not perform the settings that are shown in the following example.

Example:
- CM#0 CA#0 Port#0
  IP address: 192.168.10.1
  Subnet mask: 255.255.255.0
- CM#0 CA#1 Port#0
  IP address: 192.168.10.2
  Subnet mask: 255.255.255.0

Do not specify the same subnet address with different VLAN IDs in the same controller.

Procedure

1. Set the necessary parameters and execute the "create nas-interface" command of ETERNUS CLI.

   ```
   create nas-interface -port 000 -ip 192.168.0.100 -netmask 255.255.255.0 -gateway 192.168.0.1 -vlan-id 1
   ```

   -port
   Optional. Specify a port to assign the NAS interface. If Bonding is set, specify the master port.

   During the configuration phase
   - Only NAS ports can be specified.
   - For NAS interfaces without a specified VLAN ID, multiple NAS interfaces cannot be assigned to each NAS port.
   - For NAS interfaces with a specified VLAN ID, multiple NAS interfaces with the same VLAN ID cannot be assigned to each NAS port.
Specify a VLAN ID within a range of 0 to 4094. If 0 is specified, VLAN is disabled.

DNS Server Settings

Configure the DNS server used in the NAS environment.
Configure the DNS server before configuring the authentication server.

Caution

During the configuration phase
To use the DNS server in the Active Directory domain, SRV resource records of the DNS server must be set to resolve the NetBIOS domain name from the Active Directory DNS domain name.
If the DNS server setting is incorrect, a connection failure error is displayed when setting the authentication server.

Note

During the configuration phase
• Specify a DNS server that is connected to the NAS environment network.
  Even if a DNS server is specified in the network environment settings for the operation management LAN, it is not used by the NAS environment.
• For NFS operations in environments that use DNS servers, enable forward/reverse lookups for the FQDN of the NFS client and the FQDN of the NAS interface.

Procedure

1. In ETERNUS Web GUI, click the [Connectivity] tab on the navigation, and then click [NAS] — [Environment Settings] in [Category].
   The [Environment Settings] screen appears.
2. In [Action], click [Set DNS Server].
   The [Set DNS Server] screen appears.
Set the required items in the [Set DNS Server] screen and click the [Set] button.

- Primary IP Address
  Enter the primary IP address for the DNS server in IPv4 format.
- Secondary IP Address
  Enter the secondary IP address for the DNS server in IPv4 format.
- IPv6 Primary IP Address
  Enter the primary IP address for the DNS server in IPv6 format.
  IPv6 addresses that can be entered are global addresses or unique local addresses.
- IPv6 Secondary IP Address
  Enter the secondary IP address for the DNS server in IPv6 format.
  IPv6 addresses that can be entered are global addresses or unique local addresses.

A confirmation screen appears.

4 Click the [OK] button.
The DNS server is set and the registration completion screen appears.

5 Click the [Done] button.
The screen returns to the [Environment Settings] screen.

End of procedure
**NAS Server Name Settings**

Set the name that will be used when changing the NAS server name (host name) for the ETERNUS DX that is used in the NAS environment. The default NAS server name can also be used. For details on the default NAS server name, refer to "NAS Server Name (Host Name)" (page 27).

For Active Directory authentication, the NAS Engine of the ETERNUS DX uses the NAS server name as a NetBIOS name.

**Note**

**During the configuration phase**

Specifying the NAS server name has the following requirements.
- The number of characters that can be specified is 1 to 15 characters.
- The following types of characters can be used.
  - Alphanumeric characters (US-ASCII code)  
    "A" (0x41) to "Z" (0x5A) and "a" (0x61) to "z" (0x7A)
  - Numerical characters  
    "0" (0x30) to "9" (0x39)
  - "." (hyphen) (0x2D)
    The "." cannot be used as the first and/or the last character of the NAS server name.
- Do not use special characters (symbols) except for a hyphen. If these characters are used, the process of creating shared folders will result in an error.

**Procedure**

1. In ETERNUS Web GUI, click the [Connectivity] tab on the navigation, and then click [NAS] – [Environment Settings] in [Category].
   The [Environment Settings] screen appears.

2. In [Action], click [Change NAS Server Name].
   The [Change NAS Server Name] screen appears.
3. Set the required items in the [Change NAS Server Name] screen and click the [Change] button.

![Change NAS Server Name](image)

A confirmation screen appears.

4. Click the [OK] button.
The NAS server name is changed and the registration completion screen appears.

5. Click the [Done] button.
The screen returns to the [Environment Settings] screen.

---

End of procedure
Set the Active Directory authentication servers and the LDAP authentication servers that are used in the NAS environment. The maximum number of authentication servers that can be set for each server type is three.

If the Active Directory authentication server is configured, user management of the directories and files are possible, but the fixed user account (shareuser$) cannot be used. Note that the local user settings and the local group settings must be deleted when local user authentication is used. For details, refer to "Local User Authentication" (page 34).

By setting the LDAP authentication servers, user management of directories and files can be performed for access via the NFS protocol.

**Caution**

During the configuration phase

- The setting must be performed when the NAS interface is in an Active-Active connection state.
  - If the authentication servers are set while the NAS interface is in an Active-Standby connection state or a failover state, an error occurs.
- System volumes and the NAS interface must be created in advance to perform the settings for the authentication servers. System volumes are automatically created when the NAS volume is created for the first time. The following configurations cannot be performed if no system volumes ($SYSVOL1, $SYSVOL2, and $SYSVOL3) are created in the ETERNUS DX.
  - NAS interface settings
  - Authentication server settings
- To set authentication servers, specify each server with an IP address or an FQDN. Note that a DNS server is required for name resolution when using an FQDN to specify the authentication server. Configure the DNS server before configuring the authentication server.
- The DNS server function is required to use the domain name for operations with Active Directory authentication. For that reason, when using an Active Directory authentication server, always configure the DNS server. If the DNS server is not set up, the Active Directory server is temporarily set as the DNS server.
- Perform an operation setting of the user management in the authentication server or in the local user authentication before creating shared folders in the ETERNUS DX.
- If an LDAP authentication server is not being used, delete the LDAP authentication server from the authentication server settings.
- When using Active Directory authentication, make sure to configure the following DNS settings.
  - Enable forward/reverse lookups for the host name FQDN of the Active Directory server
    - Configuration example:
      Configure the DNS setting to enable the name resolutions of "adserver.example.com" and "example.com" for the following case.
      - Host name of the Active Directory server: adserver
      - Domain name of the Active Directory server: example.com
    - Enable forward/reverse lookups for the host name FQDN of the Windows client
During the configuration phase

- Before setting up the authentication server, connect both of the controllers to the authentication server to make communication between them ready.
- Active Directory's two-way, transitive trust relationships are not supported.

Procedure

1. In ETERNUS Web GUI, click the [Connectivity] tab on the navigation, and then click [NAS] — [Environment Settings] in [Category]. The [Environment Settings] screen appears.


3. Set the required items in the [Set Authentication Server] screen and click the [Set] button.

Set the items of the "Active Directory Authentication Settings" or "LDAP Authentication Settings" according to the authentication servers that are to be used.
During the configuration phase

• To set a new authentication server, setting the domain name, the domain administrator, and the authentication server is required.

• In "LDAP Authentication Settings", specifying both "Domain Name" and "Domain Administrator" is required. Set the dc attribute as "Domain Name", and the cn attribute as "Domain Administrator" for the bind DN that is used for LDAP authentication.

  Configuration example:
  If bind DN is "cn=Manager,dc=test,dc=local", then set "Domain Name" as "test.local" and "Domain Administrator" as "Manager".

• Specify each LDAP authentication server with an IP address to set up the authentication server if a DNS server is not used.

• For details on the characters that can be specified, refer to "Authentication Server" (page 29).

- Domain Name
  Specify the domain name of the authentication server.

- Domain Administrator
  Specify the administrator name of the authentication server.

- Change Password
  To change the password of an authentication server administrator, select the checkbox.

- Domain Administrator's Password
  Input the password for the authentication server administrator.
  When inputting the Domain Administrator's Password, select the Change Password checkbox and then input the same password in the confirmation field.

- Authentication Server (1) – (3)
  Input an IPv4 address, an IPv6 address, or an FQDN for the authentication server.
  A confirmation screen appears.

4 Click the [OK] button.
  The authentication server is set and the registration completion screen appears.

5 Click the [Done] button.
  The screen returns to the [Environment Settings] screen.

| Caution |
Local User Authentication Settings

To perform a user management without using the authentication server, perform a local user authentication setting. If the local user authentication is used with CIFS, the local user settings are enabled after CIFS is re-connected.

The following procedure is used to set the local user authentication.

Local Group Creation

Create a local group to which the local user belongs.

Procedure

1. In ETERNUS Web GUI, click the [Connectivity] tab on the navigation, and then click [NAS] - [Environment Settings] in [Category].
   The [Environment Settings] screen appears.
2. Click the [Local Group] tab in [Environment Settings] and then click [Add Local Group] in [Action].
   The [Add Local Group] screen appears.
3. Set the required items in the [Add Local Group] screen and click the [Add] button.

- Name
  Specify the local group name.
- Group ID
  Specify the group ID. Specify a group ID with a value between 500 and 999. The group ID is optional. If omitted, the ID is automatically assigned.
  A confirmation screen appears.
4. NAS Environment Configuration  
Local User Authentication Settings

4. Click the [OK] button.  
The local group is added and the registration completion screen appears.

5. Click the [Done] button.  
The screen returns to the [Environment Settings] screen.

End of procedure

Local User Creation

Create a local user.

Procedure

1. In ETERNUS Web GUI, click the [Connectivity] tab on the navigation, and then click [NAS] - [Environment Settings] in [Category].  
The [Environment Settings] screen appears.

2. Click the [Local User] tab in [Environment Settings] and then click [Add Local User] in [Action].  
The [Add Local User] screen appears.

3. Set the required items in the [Add Local User] screen, select the local groups to which the user belongs, and click the [Add] button.

![Add Local User Screen]

- **Name**  
  Specify the local user name.

- **User ID**  
  Specify the local user ID. Specify a user ID with a value between 500 and 999. Specify 450 for the user ID when using the same user name (shareuser$) as the fixed user account.  
The user ID is optional. If omitted, the ID is automatically assigned.

- **Password**  
  Enter a password for the local user to gain access. Specify a password in the range of 8 to 32 characters.
4. NAS Environment Configuration

Local User Authentication Settings

- Confirm Password
  Enter the password for confirmation.
  A confirmation screen appears.

4. Click the [OK] button.
   The local user is added and the registration completion screen appears.

5. Click the [Done] button.
   The screen returns to the [Environment Settings] screen.

End of procedure
Changing the Local User Password

Besides using the management LAN, users can change their local user password from the user LAN (NIC-CA). Local user passwords can be changed from ETERNUS Web GUI or ETERNUS CLI. Note that the local user password can only be changed from the Master CM.

Caution

During the operation phase
- Do not perform local user/local group operations from the management LAN and password change operations from the user LAN at the same time.
- Multiple local users cannot change their passwords at the same time. Password change operations that are executed at a later time result in an error.

The following procedure is used to change the local user password. This section describes the procedure for when ETERNUS CLI is used.

Procedure

1. Execute the "set nas-port" command of ETERNUS CLI from the management LAN to specify "open" for the firewall setting of the port used to change the password for local user authentication (30022) that is in the NIC-CA port.

   The following example is for when the firewall setting for the port used to change the password for local user authentication of CM#0 CA#0 Port#0 is set to "open".

   ```
   set nas-port -port 000 -local-user-password open
   ```

2. Using the local user account of the password change target, connect to the port for changing the local user authentication password (30022) using SSH from the NIC-CA port for which the firewall is set to "open".

   The following example is for when the password of user (testusr_uid_599) is changed via the NIC-CA port (172.16.0.70). The specification method may differ depending on the client OS.

   ```
   ssh testusr_uid_599@172.16.0.70 -p 30022
   ```

3. Enter the changed password and the password for confirmation.

   ```
   New password: ←Enter the changed password.
   Retype new password: ←Re-enter the changed password (for confirmation).
   ```

   Completed.

   Press any key to logout: ←Press any key to log out.

End of procedure
Authentication Method Change

The following procedures are used to change the authentication method.

■ When Changing the Authentication Method from Local User Authentication to an Authentication Server

Authentication server and local user authentication cannot be used simultaneously.

Note that when changing the authentication method from the local user authentication to an authentication server, ACL will be affected.

■ When Changing the Authentication Method from an Authentication Server to Local User Authentication

Authentication server and local user authentication cannot be used simultaneously.

Note that when changing the authentication method from an authentication server to the local user authentication, ACL will be affected.

■ When Changing the Authentication Method from the Fixed User Account (shareuser$) to Local User Authentication

The following procedure is used to change the authentication method from the fixed user account (shareuser$) that was used with firmware version V10L51 or earlier to local user authentication.

1. Create a local user/local group.
   For details, refer to "Local User Authentication Settings" (page 100).

2. Use a local user account to copy the files that were created using the fixed user account (shareuser$) to another shared folder.

3. When access is controlled in CIFS environments, delete either the user ("shareuser$") or the group ("shareuser$").

4. For operations in CIFS environments, set the security ID using the "set nas-server" command of ETERNUS CLI.

   ```
   set nas-server -server-sid S-1-5-21-x-x-x
   ```

   To check the security ID that is to be specified for ",server-sid", execute the following command in PowerShell CLI via the CIFS client. Specify the file name that was created by the local user.

   ```
   get-acl <Name_of_any_file_in_the_shared_folder> | fl
   ```

   The security ID that is to be specified using ETERNUS CLI is S-1-5-21-x-x-x (where x is a numerical value from 0 to 4294967295) that is displayed for "Owner" and "Group" in the result.

Procedure

1. Create a local user/local group.
   For details, refer to "Local User Authentication Settings" (page 100).

2. Use a local user account to copy the files that were created using the fixed user account (shareuser$) to another shared folder.

3. When access is controlled in CIFS environments, delete either the user ("shareuser$") or the group ("shareuser$").

4. For operations in CIFS environments, set the security ID using the "set nas-server" command of ETERNUS CLI.

   ```
   set nas-server -server-sid S-1-5-21-x-x-x
   ```

   To check the security ID that is to be specified for "server-sid", execute the following command in PowerShell CLI via the CIFS client. Specify the file name that was created by the local user.

   ```
   get-acl <Name_of_any_file_in_the_shared_folder> | fl
   ```

   The security ID that is to be specified using ETERNUS CLI is S-1-5-21-x-x-x (where x is a numerical value from 0 to 4294967295) that is displayed for "Owner" and "Group" in the result.

End of procedure
Shared Folder Creation (CIFS/NFS)

Create folders that can be shared among users. Access protocols can be set for each shared folder. To limit accessible hosts, set hosts that are allowed or denied access. In addition, "Owner" and "Group" can be specified for each shared folder.

When the used protocol is "CIFS" or "CIFS/NFS", the Opportunistic locking function (or Oplocks) can be specified. File data can be cached in the CIFS client by enabling this function.

If enabled, notifications to the ETERNUS DX can be reduced during file operations using the CIFS client. As a result, the performance can be improved due to less network traffic.

If the used protocol is CIFS, a home directory can be used. For details about how to use home directories, refer to "Home Directories" (page 110).

**Caution**

**During the configuration phase**
- If an Alternate Data Stream (ADS) is used, do not enable the Oplocks settings.
- If a shared folder is created with the same name as a user when home directories are used, the created shared folder is used as the home directory of the user and the shared folder for home directories ("homes") is not used. The shared folder can be accessed in the same manner as home directories and can be accessed by other users who have access privileges.
- Disabling Oplocks is recommended when multiple users perform an operation on the same file. If multiple users perform an operation on the same file when Oplocks is enabled, synchronizing the cache with the ETERNUS DX fails and the data may become corrupted depending on the network conditions.

**During the operation phase**

Do not create a folder or a file named ".streams" in the shared folder.
During the configuration phase

- Shared folder names have conditions on the unavailable characters (reserved words and prohibited characters) and a limit on the number of characters (up to 76 characters) available.
  - The following strings cannot be used regardless of case.
    . .. .snap global homes printers ipc$.streams
  - The following characters cannot be used.
    - Symbols
      "" (0x5C), "/" (0x2F), ":" (0x3A), ":*" (0x2A), ":?" (0x3F), ":" (0x22), ":<>" (0x3C), ":=" (0x3D), ":,;" (0x2C), ":[]" (0x5B), ":" (0x7C), ":%" (0x25)
    - Spaces (0x20)
  - The character string "$bak" cannot be used alone or as a suffix.
  - The character string "@GMT" cannot be used alone or as a prefix. The characters are case-insensitive.
- Japanese character sets with non-ASCII characters (UTF-8) can be used for the shared folder names.
  However, if the client OS does not support Japanese, the shared folder names may be garbled in the management software, or operations using the shared folder may fail with an error. When specifying, check if Japanese is supported by each client OS. If Japanese is not supported, do not use Japanese character sets.
- Do not mount CIFS shared folders using the NFSv4.0 protocol. If a mount is performed, creating a shared folder with the same name as the target shared folder may fail. If a shared folder with the same name cannot be created, creating a shared folder with a different name makes creating a shared folder with the same name possible.
- The same name as an existing shared folder cannot be used in the ETERNUS DX. An error occurs if a shared folder with the same name as an existing shared folder is set.
- When a new shared folder is created, "Yes (Writable)" is enabled and Oplocks is set to "Disable (Do not use)". To change these settings, use the Modify Shared Folder function.
- If CIFS is used for the protocol and local user authentication for the access permission, specify the local user or local group that is to be allowed access with [CIFS Permissions].

Procedure

1. Click the [Connectivity] tab on the navigation of the ETERNUS Web GUI screen, and then click "NAS" in [Category].
   The [NAS] screen appears.
2. In [Action], click [Create Shared Folder].
   The [Create Shared Folder] screen appears.
Set the required items in the [Create Shared Folder] screen and click the [Create] button.

- **Usage**
  Set the usage of the shared folder. Specify "File Sharing".

- **Shared Folder Name**
  Set the shared folder name.

- **Protocol**
  Set the protocol that is used for the shared folder.
  When using the shared folder with Windows, select "CIFS". To use the shared folder in UNIX/Linux, select "NFS". If the shared folder is used with both Windows and UNIX/Linux, select "CIFS/NFS".

- **Owner**
  Set the owner name for the shared folder.
  Specify the user name of the domain to which the ETERNUS DX belongs.
  If the ETERNUS DX does not belong to the domain, specify "root". If omitted, "root" is specified.

- **Group**
  Set the group name for the shared folder.
  Specify the group name of the domain to which the ETERNUS DX belongs.
  If the ETERNUS DX does not belong to the domain, specify "root". If omitted, "root" is specified.

- **SMB Encryption of Data Access**
  Specify whether encryption is performed with an SMB3.0 protocol base.

- **Access Based Enumeration**
  Specify whether directories/files are hidden to users who do not have read access privilege for the directories/files.

- **CIFS Allowed Hosts**
  For CIFS, hosts that are allowed access to the shared folder can be set.
  If only CIFS Allowed Hosts are specified, all other hosts are denied access.

- **CIFS Denied Hosts**
  For CIFS, hosts that are denied access to the shared folder can be set.

- **NFS Allowed Hosts**
  For NFS, hosts that are allowed access to the shared folder can be set.
Specify hosts that are allowed access (mount operation). If the NFS Allowed Hosts are specified, all other hosts are denied access.

### Caution

#### During the configuration phase
- CIFS Allowed Hosts, CIFS Denied Hosts, and NFS Allowed Hosts cannot be specified with IPv6 link-local addresses.
  - If IPv6 link-local addresses are used for CIFS Allowed Hosts, all CIFS access is denied.
  - If IPv6 link-local addresses are used for NFS Allowed Hosts, all NFS access is denied.
- When the IPv6 format is used, use IPv6 global addresses. When the IPv6 format is not used, use IPv4 addresses (global or local addresses).
- The setting values of CIFS Allowed Hosts and CIFS Denied Hosts affect the access control over hosts as shown below. Some combinations of the setting values for CIFS Allowed Hosts and CIFS Denied Hosts may allow access from unintended hosts.
  - The CIFS Allowed Hosts setting has a higher priority than the CIFS Denied Hosts setting. If the same subnet or the same IP address is specified in both of the settings, CIFS client access is allowed from the relevant network.
  - CIFS client access is allowed from networks that are not specified in either setting.
  - If neither setting is configured, access is allowed from any host.
  - If CIFS Allowed Hosts or CIFS Denied Hosts is configured or changed, the setting is enabled after the hosts are reconnected.
- For details on the characters that can be specified for CIFS Allowed Hosts, CIFS Denied Hosts and NFS Allowed Hosts, refer to "Authentication Server" (page 29).

#### During the operation phase
Do not change the following access control settings for the root folder of the shared folder from the client.
- Owner
- Group
- Access privilege
- If these settings are changed from a client, the clients may become unable to access the shared folder.
During the configuration phase

- There are conditions for the characters that can be used in the shared folder name. For details, refer to "File Sharing" (page 39).

- Use the following format to specify CIFS Allowed Hosts, CIFS Denied Hosts, or NFS Allowed Hosts with IPv6 addresses.
  - IPv6 address specification
    A setting example is shown below.
    2001:333:333:33::
    ::1
  - IPv6 address range specification
    Use the "IPv6 address/prefix length" format. A setting example is shown below.
    2001:333:333:33::/64

- When the [SMB Encryption of Data Access] setting is changed, the session currently connected to the target shared folders is disconnected. However, if the target folders are shared with CIFS clients, the session is not disconnected until the sharing is stopped. The SMB Encryption setting takes effect after the session is re-established.

- When configuring SMB Encryption in shared folders, SMB2.1 or earlier clients cannot access the shared folders. A confirmation screen appears when attempting to access the shared folders. However, even though authentication information is entered, access is denied.

- When the [Access Based Enumeration] setting is changed, the session currently connected to the target shared folders is disconnected.
  The Access Based Enumeration (ABE function) setting takes effect after the session is re-established.

A confirmation screen appears.

4 Click the [OK] button.
   The shared folder is created and the registration completion screen appears.

5 Click the [Done] button.
   The screen returns to the [NAS] screen.
If the used protocol is CIFS, a home directory can be used. A home directory is available by selecting “Home Directory” to create a shared folder for the home directory ("homes") when shared folders are created.

**Caution**

**During the configuration phase**

- The same parameters that are set in the shared folder can be set for the shared folder used for the home directory, but the following parameters are fixed.
  - Shared Folder Name (fixed to "homes")
  - Protocol (fixed to "CIFS")
  - Writable (fixed to "rw")
  - ABE function (fixed to "disable")
  - CIFS access permission settings (N/A)
  - NFS Allowed Hosts (N/A)

- User names that are used to access the home directory have a condition that they can only contain alphanumeric characters and symbols (\*, _, and $) (or US-ASCII code).

  If a user name with characters other than these characters is specified, the home directory cannot be used.

  If a user name with characters other than these characters is specified to access "\IP_address_of_the_NAS_interface", the user name may appear correctly but the home directory is not accessible.

**During the operation phase**

- Deleting of Active Directory users and deleting of local users are not operated together with the deletion of the home directory. Local users and home directories must be deleted separately.

- The specified home directory cannot be completely deleted for the following cases. After disconnecting the CIFS connection that is being used, delete the home directory again.
  - A file is being created in the home directory

- To confirm that the home directory of the specified user has been successfully deleted, execute the following command with ETERNUS CLI and make sure the user’s home directory does not exist.

  ```
  show nas-share-progress -mode nas-home-directory-deletion
  ```

After confirming that the home directory which is currently being deleted does not exist, execute the "show nas-home-directory" command of ETERNUS CLI and check the list of home directories. Since the home directories may not be completely deleted if the NAS engine fails during the deletion process, delete the home directory again.
During the operation phase

- Home directories cannot be accessed with FTP connections.
- Use the Delete Shared Folder function by specifying "homes" to delete the shared folders for the home directories.
- Use the Clear NAS Data function by specifying "homes" to delete the home directories for all users.
- Use the "delete nas-home-directory" command of ETERNUS CLI to delete the home directory of each user.

Procedure

1. Click the [Connectivity] tab on the navigation of the ETERNUS Web GUI screen, and then click "NAS" in [Category].
   The [NAS] screen appears.

2. In [Action], click [Create Shared Folder].
   The [Create Shared Folder] screen appears.

3. Set the required items in the [Create Shared Folder] screen and click the [Create] button.

   - Usage
     Set the usage of the shared folder. Specify "Home Directory".
   - Shared Folder Name
     Set the shared folder name. "homes" is fixed.
   - Protocol
     Set the protocol that is used for the shared folder. "CIFS" is fixed.
   - Owner
     Set the owner name for the shared folder.
     Specify the user name of the domain to which the ETERNUS DX belongs.
     Owner specification is relevant only when backups or restores are performed ("8. Backup/Restore Settings" (page 156)).
The owner is a user that can access the shared folders ("$homes" or "homes$bak") that become available when backups that include home directories are restored or mounted.

If omitted, "root" is specified.

• Group
  Set the group name for the shared folder.
  Specify the group name of the domain to which the ETERNUS DX belongs.
  Group specification is relevant only when backups or restores are performed ("8. Backup/Restore Settings" (page 156)).
  The group can access the shared folders ("$homes" or "homes$bak") that become available when backups which include home directories are restored or mounted.
  Note that BUILTIN groups cannot be specified.
  If omitted, "root" is specified.

• SMB Encryption of Data Access
  Specify whether encryption is performed with an SMB3.0 protocol base.

• Access Based Enumeration
  Specify whether directories/files are hidden to users who do not have read access privilege for the directories/files. "Disable" is fixed.

• CIFS Allowed Hosts
  Hosts that are allowed access to the home directory can be specified.
  If only CIFS Allowed Hosts are specified, all other hosts are denied access.

• CIFS Denied Hosts
  Hosts that are denied access to the home directory can be specified.

• NFS Allowed Hosts
  Specification is not necessary.
  Refer to Step 3 in "Shared Folder Creation (CIFS/NFS)" (page 105) for notes when setting each item.

A confirmation screen appears.

4 Click the [OK] button.
  The home directory is created and the registration completion screen appears.

5 Click the [Done] button.
  The screen returns to the [NAS] screen.

End of procedure
FTP/FXP Settings

This section provides the required procedures to configure the FTP function and the FXP function.

**Caution**

**During the operation phase**
- The creation date and time information of the files that are obtained using FTP/FXP are displayed in the Greenwich Mean Time (GMT).
- FTP commands STAT and SYST are not supported.

FTP Setting

Use ETERNUS CLI to perform the setup to use FTP. The configuration procedure for FTP is shown below.

**Procedure**

1. Set the necessary parameters and execute the "set nas-ftp" command of ETERNUS CLI to set up the shared folder that is to be published via FTP.
   
   The following example is for when the shared folder #1 is published via FTP.
   
   ```
   set nas-ftp -share-number 1
   ```

   **-share-number**
   
   Specify the shared folder that is to be published via FTP using the shared folder number.
   
   The shared folder can also be published by specifying with "-share-name" instead of "-share-number".

2. Set the necessary parameters and execute the "set nas-port" command of ETERNUS CLI to change the firewall settings for the FTP connection to "open" ("close" as default).
   
   The following example is for when the firewall setting for the FTP connection of CM#0 CA#0 Port#0 is changed to "open".
   
   ```
   set nas-port -port 000 -ftp open
   ```

   **-ftp**
   
   Specify whether to enable or disable the firewall setting of the FTP connection. To disable this function, specify "open" here.
3. From the NIC-CA port, log in to the ETERNUS DX via FTP using the account that is registered in the authentication server or the account that is registered in the local user authentication setting. The shared folders that are published in the home directory for FTP can be accessed.

End of procedure

FXP Setting

Use ETERNUS CLI to perform the setup to use FXP.

Caution

During the configuration phase
When performing an FXP connection, make sure that the firewall settings of the FXP connection and the FTP connection are both set to "open".

The configuration procedure for FXP is shown below.

Procedure

1. Set the necessary parameters and execute the "set nas-ftp" command of ETERNUS CLI to set up the shared folder that is to be published via FTP.
   The following example is for when the shared folder #1 is published via FTP.
   ```
   set nas-ftp -share-number 1
   ```
   `-share-number`
   Specify the shared folder that is to be published via FTP using the shared folder number.
   The shared folder can also be published by specifying with "-share-name" instead of "-share-number".

2. Set the necessary parameters and execute the "set nas-server" command of ETERNUS CLI to enable the FXP function (disabled as default).
   ```
   set nas-server -fxp enable
   ```
   `-fxp`
   Specify whether to enable or disable the FXP function. To enable this function, specify "enable" here.

3. Set the necessary parameters and execute the "set nas-port" command to set the firewall setting for the FTP connection and the FXP connection to "open" ("close" as default).
   The following example is for when the firewall setting for the FTP connection and FXP connection of CM#0 CA#0 Port#0 is set to "open".
   ```
   set nas-port -port 000 -ftp open -fxp open
   ```
4. NAS Environment Configuration
Quota Settings

Specify whether to enable or disable the firewall setting of the FTP connection. To disable this function, specify "open" here.

Specify whether to enable or disable the firewall setting of the FXP connection. To disable this function, specify "open" here.

From the NIC-CA port, log in to the ETERNUS DX via FTP using the account that was registered in the authentication server. After an FTP login, the directory that is exclusive for FTP publishing is the home directory. Between each ETERNUS DX, a data transfer is performed between the published shared folders.

End of procedure

Quota Settings

This section provides the required procedure to set a quota.

The following basic settings are required to use the Quota function.

- A quota for each user or group is set for users or groups that are registered in the authentication server. Register users or groups in the authentication server in advance.

- The types of available quotas vary depending on the controller firmware versions. A quota can be used for each user or group when the controller firmware version is V10L21 or later, and a quota can be used for each shared folder when the controller firmware version is V10L51 or later. When a TPV that was created with the controller firmware version earlier than the supported versions (for every quota) is used, a format conversion must be performed from ETERNUS CLI before the quota setting.

The format conversion procedure is as follows.

1. Use the "reconfigure nas-fs" command to execute a NAS volume reconfiguration.

2. Use the "forced nas-fsunmount" command to unmount the target NAS volume for both controllers.

3. Use the "start nas-fsck" command in "repair mode" to execute a format conversion of the file system.

4. Use the "forced nas-fsmount" command to remount.

- The Quota function sets one or both types of thresholds ("Warning" and "Limit") for the used drive space or for the number of files.
  - When the warning threshold is exceeded
    Since this is a predictive notification, writing to the target NAS user volume is not prohibited.
  - When the limit threshold is exceeded
    Writing to the target NAS user volume is prohibited.

- For a single quota setting information (or each row of the quota target list), a total of four thresholds can be set for the used drive space ("Warning" and "Limit") and the number of files ("Warning" and "Limit"). However, setting "0" to all four thresholds (which includes setting the used drive space to "Not Specified") is not allowed. At least one threshold must have a valid value.
- Add the quota setting information to multiple users, groups and shared folders. Regardless of the environment that is to be used, the maximum number of quota setting information that can be added in a single operation (by clicking the [Add] button on the lower part of the screen) is 100.

- The following events can be notified with the method that is set in advance using the Setup Event Notification function. For more details, refer to "ETERNUS Web GUI User's Guide".
  - The used drive space or the number of files has exceeded the threshold
  - The used drive space or the number of files has returned to within the threshold

**Caution**

**During the configuration phase**

- Quotas cannot be set for snapshots and backup volumes.
- Do not set a Quota for the administrator (root).
- Backing up the file system after setting or deleting a Quota is recommended.
- Even when usable drive space has been specified for each user, group, or shared folder, the drive space can be used over the limit but within the range of the "disk usage limit value + 2GB". However, files that are to be inflated using the Sparse File Inflation function are not targets for the Quota function. Therefore, the drive usage amount may exceed the limit value.

  The number of files cannot exceed the specified threshold.
During the configuration phase

- Specifying the user name and group name has the following requirements.
  - The number of characters that can be specified is 1 to 255 characters.
  - The types of characters that can be used are alphanumeric characters (US-ASCII code) and symbols between space character (0x20) to “~” (0x7E). Note that “?” (0x3F) and “\” (0x5C) cannot be used.

- For CIFS access users, set the limit of the drive capacity that is used to be less than the drive capacity. If a value larger than the drive capacity is specified, correct capacity cannot be referred from the Windows client.

- Set the warning value and the limit value equal to or less than the drive capacity. Areas such as the management area that prevents user data from being written cannot be used. For details, refer to "File System Specification" (page 24).

- When setting a Quota for the user who performs CIFS access using the Active Directory authentication, create a shared folder by specifying CIFS as the protocol to use and set a Quota.

- The Quota process time is increased in proportion to the number of Quota settings. In addition, the response time of the authentication server is affected by the Quota process time. Therefore, the response time for the authentication server must be taken into consideration when designing the system.

- The types of available quotas vary depending on the controller firmware versions. A quota can be used for each user or group when the controller firmware version is V10L21 or later, and a quota can be used for each shared folder when the controller firmware version is V10L51 or later. When a TPV that was created with the controller firmware version earlier than the supported versions (for every quota) is used, a format conversion must be performed from ETERNUS CLI before the quota setting.

  Furthermore, if a quota is set for a TPV that was created with a controller firmware version earlier than the supported versions (for every quota) without a format conversion, an error occurs. For more details on the format conversion, refer to "Quota Settings" (page 115).

During the operation phase

- If Quota settings are deleted when the authentication server is inaccessible, inconsistencies may occur in the Quota information. When inconsistencies occur (such as Quota restrictions being applied to users without a Quota setting), restore the Quota information by executing the "start nas-fsck" command from ETERNUS CLI.

- If the capacity of the drive that is used reaches the limit, writing or creating files for the relevant drive is stopped. The status screen for ETERNUS Web GUI or ETERNUS CLI indicates the limit status, but an error message or event notification that indicates that the limit has been exceeded is not reported at this point. A notification is reported when a file operation has failed because the limit has been exceeded.

- Events are notified at 10 min intervals when a threshold is exceeded or when a Warning is released lowering the threshold.

- When the limit value of the quota setting is reached during a file operation, that file operation fails (or causes an error). However, if a sync option is not specified when an NFS mount is performed from an NFS client, the error is not notified.
The procedure to perform a quota management is shown below.

**Procedure**

1. Click the [Connectivity] tab on the navigation screen in ETERNUS Web GUI, and then click [NAS] - [Quota Management] in [Category].

![Quota Management Screen](image1)

2. In [Action], click [Add Quota Setting].
   The [Add Quota Setting] screen appears.

![Add Quota Setting Screen](image2)

3. Select a NAS user volume to add the quota setting information.
4. NAS Environment Configuration

Quota Settings

Add the quota setting information to the quota target.

(1) Click the [Add] button on the bottom right of the quota target.

The [Add Quota Target] screen appears.

(2) Set the required items and click the [OK] button.

- Type
  Select a quota target.
  - User
    Select this item when the target is a user.
  - Group
    Select this item when the target is a group.
  - Share
    Select this item when the target is a shared folder.

- Name
  Enter the target user name, group name, or shared folder name.
  The character string that can be specified has the following requirements.
  - The types of characters that can be used are alphanumeric characters and symbols (0x20 to 0x7E in ASCII [US-ASCII]). Note that "?" (0x3F) and "\" (0x5C) cannot be used.
  - The number of characters that can be specified is 1 to 255 characters.

- Drive Space
  Enter the warning value for the drive usage in the quota target. The input requirements are as follows.
  - Warning (0 to 128TB)
    If "0" is entered or no values are specified, "Not Specified" (unlimited) is registered in the ETERNUS DX.
    Enter the limit value for the drive usage in the quota target.
- Limit (0 to 128TB)
  If "0" is entered or no values are specified, "Not Specified" (unlimited) is registered in the ETERNUS DX.
- File Count
  Enter the warning value for the number of files in the quota target.
  - Warning (0 to 134217723)
    If "0" is entered, "Not Specified" (unlimited) is registered in the ETERNUS DX.
    Enter the limit value for the number of files in the quota target.
  - Limit (0 to 134217723)
    If "0" is entered, "Not Specified" (unlimited) is registered in the ETERNUS DX.

**Caution**

**During the configuration phase**
If both the warning and limit values are specified, the limit value must be larger than the warning value.

(3) To set multiple quota settings for the selected NAS user volume, repeat Step (1) through Step (2).

5 Click the [Add] button.
The quota setting is performed and a registration completion screen appears.

6 Click the [Done] button.
The screen returns to the [Quota Management] screen.

---

End of procedure
Snapshot Settings

This section provides an explanation of the necessary settings for snapshots, and how to acquire and restore snapshots.

Basic Settings for Snapshot

Perform the basic settings to use the Snapshot function. The following settings are necessary.

• Setting the necessary area for Snapshot
  Prepare a RAID group where Snapshot control information is to be saved and a Snapshot destination volume (SDPV). An existing RAID group can be used.
  Use a RAID group that has sufficient space for the number of generations. SDPVs are used as pool volumes.
  Take the area for the snapshot generations and the amount of updates between generations into consideration when configuring the area necessary for Snapshots.

• Settings related to the snapshot copy operations
  Specify the copy table size. The value that is set here is also used for the Advanced Copy functions.

• Settings for the Snapshot function
  Perform the necessary settings for a snapshot acquisition. Specify the number of snapshot generations to acquire, data destination RAID group, and an acquisition schedule.

When starting the Snapshot operation after completing the basic settings, snapshots are automatically acquired according to the specified schedule.

Caution

During the configuration phase

• Operating a snapshot acquired while a file is opened with write authority may not be possible after a restoration. Make sure to acquire snapshots while files are not in use. When acquiring snapshots multiple times a day, make sure to acquire snapshots during non-business hours at least one generation per day.

• If the SDP capacity runs out while the Snapshot function is in operation, the snapshot may fail. To receive an alert before the SDP capacity runs out, enabling the SDP Usage Rate Over (Lv1, Lv2, and Lv3) settings of the event notification is recommended.

During the operation phase

• The Snapshot function only backs up differential data. A separate full backup is recommended since there is no function to restore the whole volume if an error occurs in a NAS user volume.

• The Snapshot function shares resources with the Advanced Copy functions. Therefore, the number of copy sessions, the amount of copy table used, and the amount of volume used for copy operations all affect each other. If resources are not sufficient, snapshot acquisition may fail.

• When the copy source data is updated, an SDP is allocated for the differential data. Note that the snapshots of all generations cannot be referred to if free space in the SDP runs out. If an error occurs due to insufficient free space in the SDP, delete the snapshot settings and reconfigure.
During the configuration phase

- A snapshot cannot be acquired without a mounted NAS user volume.
- If the NAS user volume of the snapshot acquisition target is encrypted, encryption must be enabled when creating a SDPV.
- When snapshots are acquired up to the specified number of generations, older snapshots are automatically deleted in chronological order and new snapshots are acquired. Therefore, set the schedule taking into consideration how many generations may be required for restoration.

During the operation phase

- The Snapshot function must be stopped before performing a backup or restoration.
- When an old snapshot is deleted while the CIFS/NFS client is continuously accessing that snapshot, the acquisition of new snapshots may fail. The session of the CIFS client that accessed the old snapshot may be temporarily disconnected. If an access error is detected, reconnect again.
- If the ETERNUS DX is in a high-load state, snapshots may be acquired behind the specified time or the acquisition may fail.
- The ".snap" directory is a special directory for snapshot references.

Although the ".snap" directory exists from the time the NAS volume is created, it cannot be displayed using commands such as "ls" and "find", and performing directory operations on the ".snap" directory itself cause errors. To access data under the ".snap" directory, move to the ".snap" directory using the "cd" command or specify a direct path.

A directory or a file named ".snap" cannot be created in the shared folder.

If a directory or a file named ".snap" is created in the shared folder using controller firmware versions earlier than V10L31, it will become inaccessible after the controller firmware is upgraded to V10L31 or later.

Example Schedule Settings for Snapshots

The following example explains a case when a backup is acquired every day of the week using the Snapshot generation copy in order to manage generation data.

Example Schedule Settings for Snapshots

![Example Schedule Settings for Snapshots](image)
● ETERNUS DX Environment

The explanation in this section is provided on the assumption that the following system environment is used.

In this example, a volume where control information for seven Snapshot generations is saved (generation management volume) and a volume where snapshots are saved (snapshot destination volume) are registered in a single RAID group.

The capacity of the operation volume (NAS user volume) is 1TB, the update amount per snapshot is 50GB, and a snapshot destination volume (350GB) for saving seven generations is prepared. For snapshot destination volume capacity guidelines, refer to "Snapshot" (page 50).

Figure 22 Example of Creating Operation Volume and NAS Snapshot Destination Volume

*1: SDV is the volume where control information is saved when the Snapshot is executed.

*2: SDPV is the volume where snapshot data is saved.
Preparations for Acquiring Snapshots

Perform preparations that are necessary for acquiring snapshots.

- **RAID Group Creation**
  
  Create a Snapshot destination RAID group that is different from the TPP where the NAS user volume has been registered.
  
  When a RAID group for storing snapshots is specified, a generation management volume (SDV) proportional to the required number of generations is automatically created. The logical capacity for the SDV is the same as the NAS user volume. 0.1% of the logical volume capacity is required for the SDV physical capacity. For details, refer to Table 7.

  ![Figure 23 RAID Group Creation](image)

- **Snapshot Destination Volume (SDPV) Creation**
  
  Create a Snapshot destination volume (SDPV) in the RAID group for saving snapshots.

  ![Figure 24 Snapshot Destination Volume (SDPV) Creation](image)

- **Note**

  During the configuration phase
  
  Up to 128 volumes can be created in a RAID group. When acquiring snapshots for 128 generations, create an SDPV and SDV in different RAID groups.

  For procedures on how to create RAID groups and how to create SDPVs, refer to "Configuration Guide (Basic)".

- **Advanced Copy Settings**

  On the controller cache memory, set the copy table size used by the firmware. This copy table is used as an area for the copy progress management when the Snapshot function is executed.

  The copy table size settings are shared with the Advanced Copy functions. For setup procedures, refer to "Configuration Guide (Basic)".
For details on the calculation method, refer to the "Modify Copy Table Size" section in "ETERNUS Web GUI User's Guide". This section describes how to calculate the recommended values based on the copy requirements, the total copy capacity, and the number of sessions. For Snapshots, perform the calculations as shown below.

- **Copy requirements**
  Same requirements as SnapOPC+ without OPC restoration

- **Total copy capacity**
  Total capacity of NAS volumes in which Snapshot is set

- **Number of sessions**
  Total number of Snapshot generations to which the schedule is set
Settings for the Snapshot Function

Perform detailed settings to acquire snapshots. Set the target NAS user volume, number of snapshot generations, destination RAID group, and schedule.

Procedure

1. Click the [Volume] tab on the navigation of the ETERNUS Web GUI screen, and then click "Snapshot" in [Category].
   The [Snapshot] screen appears.

2. Select the target volume to acquire snapshots and click "Set Snapshot" in [Action].
   The [Set Snapshot] screen appears.

3. Set the required items and click the [Set] button.

   • Number of Generations
     Specify the number of snapshot generations to save.
   
   • Mode
     - Automatic
       Snapshots are acquired automatically according to the schedule that is set from ETERNUS Web GUI or ETERNUS CLI.
     - Manual
       Snapshots are acquired at any time from VMware vSphere Web Client. This acquisition mode is exclusive to VMware vSphere Web Client.
       For more details, refer to "ETERNUS vCenter Plug-in User's Guide".

   • Day of the Week
     Select the day of the week to acquire snapshots (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday). When acquiring a snapshot every day, select all.

   • Time Interval
     Specify the time interval to acquire the snapshot (Every Hour, 2, 3, 4, 6, 8, 12, 24).
4. NAS Environment Configuration
Snapshot Settings

- Select RAID Group
  Specify the RAID group where the SDV is to be created.
  A confirmation screen appears.

4. Click the [OK] button.
   The snapshot settings are performed and the registration completion screen appears.

5. Click the [Done] button.
   The screen returns to the [Snapshot] screen.

End of procedure
Stopping/Resuming Snapshot

This section explains the operations to stop and resume the Snapshot function.

To stop acquiring snapshots, perform the "Stop Snapshot" operation. To resume acquiring snapshots, perform the "Start Snapshot" operation.

**Note**

**During the configuration phase**
- After the snapshot settings are performed, snapshot acquisition automatically starts.
- Even when the Snapshot function is stopped, the existing snapshots and settings are not deleted.

**During the operation phase**
Stop and restart the Snapshot a few minutes before the specified time to acquire the Snapshot. If "Stop Snapshot" is performed during a snapshot acquisition, any ongoing acquisition continues but the scheduled acquisitions that follow are not performed. In addition, if the Snapshot function is restarted after the scheduled acquisition time, a Snapshot is not acquired for that acquisition time.

**Procedure**

1. Click the [Volume] tab on the navigation of the ETERNUS Web GUI screen, and then click "Snapshot" in [Category].
   The [Snapshot] screen appears.
2. Select a NAS volume that is displayed on the list and click "Stop Snapshot" or "Start Snapshot" in [Action].
   A confirmation screen appears.
3. Click the [OK] button.
   The Snapshot acquisition stops or resumes.

End of procedure
Snapshot Restoration

Snapshot data can be referred to from the shared folder. The reference method is different between a CIFS client and an NFS client.

The restoration point is the time when the snapshot is acquired.

Figure 25 Snapshot Restoration

```
[root@uni157-7 aaa]# ls
bbb.txt
```
## Restoration from the CIFS Client

A directory or file is restored from the acquired snapshot. Selecting a directory restores all the data in the directory.

### Procedure

1. Start Windows Explorer, right-click the target directory or file for data restoration, and select "Properties" from the displayed menu.
   The property screen appears.

2. Select the [Previous Versions] tab on the property screen.
   The [Previous Versions] tab screen is displayed and the acquired snapshots are displayed.
3 Select the target data at the restoration point and click the [Restore] button. The confirmation message is displayed.

4 Click the [Restore] button. Data is restored.

End of procedure

- Restoration from the NFS Client
  When using an NFS client, use the "cp" command to copy the required data for restoration.
Audit Log Setup

This section explains the audit log setting.
Use ETERNUS CLI to perform a setup for the audit log collection.
For details about the audit log messages, refer to "C. Audit Log Messages" (page 184).

Caution

During the configuration phase
- The expanded system volume that is to be the output destination for the audit logs must be created in advance.
- FTP is used to collect audit log files from the ETERNUS DX. Check that the firewall setting for the FTP connection of the NAS interface port is "open". This setting is "close" as default. For the procedure to modify the firewall settings, refer to "FTP Setting" (page 113).
- To perform an FTP, use the account that is used to log in to the audit log FTP.

Note

During the operation phase
The date file is created everyday between 3:00 AM and 5:00 AM and the audit log for about the last day's worth is output.
If the power of the ETERNUS DX is off at the time the date file is to be created, the date file is created within two hours after turning on the power of the ETERNUS DX. However, if the power of the ETERNUS DX is turned on after 9:00 PM, the date file will be created between 3:00 AM to 5:00 AM the next day.

The procedure for collecting an audit log is explained below.

Procedure

1. Set the necessary parameters and execute the "create volume" command of ETERNUS CLI to create expanded system volumes.
   The following example is for when a 1GB expanded system volume for CM#0 is created in Thin Provisioning Pool #1 by specifying CM0EXSYS for the name.

   ```bash
   create volume -name CM0EXSYS -pool-number 1 -type cm0-nas-ex-sysvol -size 1gb
   ```

   - **-name**
     Specify the volume name of the expanded system volumes.

   - **-pool-number**
     Specify the Thin Provisioning Pool that is to be the creation destination of the expanded system volumes using the pool number.
     Expanded system volumes can be created by specifying a shared folder name with "-pool-name" instead of "-pool-number".
Specify the volume type.

Specify the volume size of the expanded system volumes that are to be created. The size can be specified in the range of 1GB – 4TB.

**Note**

**During the configuration phase**

- If an expanded system volume with a large size is created using Nearline SAS disks, a timeout error may occur for the ETERNUS CLI command.
  
  From the time the command is executed until the timeout error occurs (or a duration of approximately 20 minutes), other ETERNUS CLI commands cannot be used because the command response is not returned.
  
  If the command input is available after a timeout error, execute the "show volumes -type tpv" command and check the NAS System Volume Format Status of the expanded system volume.
  
  - If "Creating filesystem" is displayed, the expanded system volume is being created.
    
    Wait for a while and re-execute the "show volumes -type tpv" command to check.
  
  - If "Complete" is displayed, the expanded system volume creation is complete. Proceed to the next step.
    
    Generally, if a 4TB expanded system volume is created when the I/O load is low, it takes about 40 minutes to complete the creation.
  
  - When 100,000 files are accessed every day, secure a capacity of about 50GB as a one month standard.

---

2 Set the necessary parameters and execute the "set nas-audit" command of ETERNUS CLI to enable the audit log function for each ETERNUS DX (disabled as default).

The following example enables the audit log function by specifying a generation of 60 days for saving the audit log file.

```bash
set nas-audit -mode enable -rotate-count 60
```

- **-mode**
  
  Specify whether to enable or disable the audit log function for the target ETERNUS DX. To enable this function, specify "enable" here.

- **-rotate-count**
  
  Optional. Specify the number of generations for saving the rotated audit log files.
  
  If omitted, this parameter is set to 30.

3 Set the necessary parameters and execute the "set nas-share" command of ETERNUS CLI to enable the audit log function for each shared folder.

The following example is for when the audit log function is enabled for the shared folder name SHARE1.

```bash
set nas-share -share-name SHARE1 -audit-log enable
```

- **-share-name**
  
  Specify the shared folder name.
Audit Log Setup

4. NAS Environment Configuration

- audit-log
  Specify whether to enable or disable the audit log function for the shared folder. To enable the audit log, specify "enable" here.

4 Execute the "create nas-engine-user" command of ETERNUS CLI to create a user account that is used to log in to the audit log FTP.

The following example is for when user name USER1 is specified and a user account that is used to log in to the audit log FTP is created. After the command is executed, an input prompt is displayed. Specify a password in the range of 8 to 32 characters.

```bash
create nas-engine-user -type audit -name USER1
```

- type
  Specify the user type. Specify "audit" here to create a user account for the audit log FTP.

- name
  Specify the user name.
  The character string that can be specified for the user name has the following requirements.
  - The number of characters that can be specified is 1 to 19 characters.
  - The following types of characters can be used.
    - Alphanumeric characters (US-ASCII code)
    - Numerical characters
  - The following reserved words cannot be specified.
    adm, audio, bin, cdrom, cgroup, daemon, dialout, dip, disk, floppy, ftp, games, gopher, halt, kmem, ldap, lock, lp, mail, mailnull, man, mem, nfsnobody, nobody, nsclcd, ntp, operator, oprofile, root, rpc, rpcuser, saslauth, shareuser$, shutdown, smmsp, sshd, sync, sys, tape, tcpdump, tty, users, utempter, umtp, uucp, vcsa, video, wheel
  - Different user account names must be used for the audit log FTP and the investigation log FTP.
  - The user name that is registered in the authentication server cannot be used.
  - The characters are case-insensitive for Active Directory authentication servers.

5 Execute the "show nas-audit-log-information" command of ETERNUS CLI to check the amount of audit logs that are output for each shared folder.

```bash
show nas-audit-log-information -share-number 1
```

6 From the NIC-CA port, log in to the FTP using the account that was created in Step 4 to collect the audit log file.

When the user account for the audit log FTP is used for the login, the directory that is exclusive for audit logs is the home directory.

7 Analyze the audit log files that are collected.

8 After the analysis, the "clear nas-audit-log" command of ETERNUS CLI can be executed to delete unnecessary audit log files.

The following example is for when the audit logs of shared folder #1 are deleted.

```bash
clear nas-audit-log -share-number 1
```
Specify the shared folder that contains the audit log files that are to be deleted. Specify "-all", when all the audit logs are targets.

**-share-number**

Specify the target shared folder using the shared folder number.

Unnecessary audit log files can also be deleted by specifying the shared folder with "-share-name" instead of "-share-number".

---

### Caution

**During the operation phase**

- The target files during an audit log collection cannot be deleted even if the shared folder that is enabled for the audit log collection is specified as a deletion target.
- When a shared folder is deleted, the audit logs for this shared folder are deleted.

---

## Meta Cache Distribution Settings

This section describes the settings when a meta cache distribution is performed. Automatic meta cache distribution is disabled by default.

### Manual Execution of Meta Cache Distribution

If the file system management data in the target NAS user volumes and NAS backup volumes are still in the initial distribution state, even if meta cache distribution is executed, the meta cache will not be moved. The current distribution state of the file system management data can be confirmed from ETERNUS Web GUI or ETERNUS CLI.

---

### Caution

**During the operation phase**

During a meta cache distribution, operations for the target volume may be delayed for several minutes.

---

This section describes the procedure to perform a manual meta cache distribution.
**Procedure**

1. In ETERNUS Web GUI, click the [Connectivity] tab on the navigation and then click "Meta Cache Distribution" under "NAS" in [Category]. The [Meta Cache Distribution] screen appears.

2. Select the target volume and click [Initialize Distribution] in [Action]. A confirmation screen appears.

3. Click the [OK] button. Meta cache distribution is executed and a completion screen appears.


---

**Automatic Execution of Meta Cache Distribution**

By enabling the automatic execution of this function, a check is performed on whether or not a relocation is necessary for all the NAS user volumes and NAS backup volumes when the NAS engine starts up and every hour on the half hour, and a meta cache distribution is performed if required.
During the operation phase

- During a meta cache distribution, operations for the target volume may be delayed for several minutes.
- When the following functions and automatic meta cache distribution are executed at the same time, the first process is executed until completion and then the next process is performed. If the process that was executed first does not complete even after about 5 minutes, an error occurs.
  - Volume capacity expansion
  - Snapshot acquisition (manual and automatic)
  - NAS volume backup

This section describes the procedure to perform an automatic meta cache distribution.

### Procedure

1. In ETERNUS Web GUI, click the [Connectivity] tab on the navigation and then click "Meta Cache Distribution" under "NAS" in [Category].


2. Click [Enable Automatic Distribution] in [Action].

   A confirmation screen appears.

3. Click the [OK] button.

   Automatic meta cache distribution is set to "Enable" and a completion screen appears.

4. Click the [Done] button.


   **End of procedure**
This chapter provides the required procedure to acquire packet traces. The output trace information is saved in a system volume. To prevent a capacity shortage in the system volume, set an upper limit for the file size that is to be output in advance so that the file capacity does not exceed the free space in the destination system volume. After analyzing the trace information, delete any unnecessary trace information files in the ETERNUS DX.

### Caution

**During the configuration phase**
- Packet trace acquisitions place load on the system and may reduce the performance of NAS I/Os. Disabling the packet trace function during normal operation and enabling it to investigate errors is recommended.
- FTP is used to retrieve the trace information file from the ETERNUS DX. Check that the firewall setting for the FTP connection of the NAS interface port is "open". This setting is "close" as default. For the procedure to modify the firewall settings, refer to "FTP Setting" (page 113).
- When performing an FTP, use the FTP login account used for investigating logs. Although this account is created with an expiration date, the account is disabled even before the expiration date if the ETERNUS DX is turned off, the firmware is updated, or the controller is replaced.
- To acquire packet traces, the recommended timing is when the CM (CPU) busy ratio of the current operation is half the performance index or less. For details on the performance index, refer to "Performance Index" (page 63).

**During the operation phase**
- The creation date and time information of the files that are obtained using FTP are displayed in the Greenwich Mean Time (GMT).
- The output file is divided and created in the order of rotation. When the number of files exceeds the limit, information is output to the first file that was created and files are overwritten in chronological order from the oldest file.
- Packet trace acquisition is stopped when the ETERNUS DX is rebooted. This does not restart automatically. In addition, the packet trace acquisition may stop if the network setting is changed or an error occurs in the network port.

Use ETERNUS CLI to configure packet trace acquisitions. The procedure for acquiring packet traces is provided below.

### Procedure

1. Check the free space in the system volume. Specify the packet trace size that can be output so that the size does not exceed the free space.
Execute the "show nas-pcap" command of ETERNUS CLI.

```
CLI> show nas-pcap
<CM#0 Packet Capture Information>
Free Space (MB)  [6000]
NAS Interface No [-]

<CM#1 Packet Capture Information>
Free Space (MB)  [6000]
NAS Interface No [-]
```

For the free space, check the value that is displayed in "Free Space".

2 Set the necessary parameters and execute the "start nas-pcap" command of ETERNUS CLI to output packet traces.

Specify the maximum size of each file, the number to divide the file by, and the maximum length of each packet.

Specify the maximum output size of a packet trace within the size that was specified in Step 1.

The following example is for when a packet trace acquisition is started by specifying NAS interface #1, a maximum size of 100MB for each file, 10 as the number to divide the files by, and a maximum length of 192 bytes for each packet.

```
start nas-pcap -nas-if-number 1 -file-size 100 -file-count 10 -packet-length 192
```

- **nas-if-number**
  Specify the NAS interface number of the target packet trace that is to be acquired.

- **file-size**
  Optional. Specify the maximum size of the output file in the range of 50 to 1024MB. If omitted, this parameter is set to 100MB.

- **file-count**
  Specify the maximum number to divide the output file by in the range of 2 to 10. If omitted, this parameter is set to 10.

- **packet-length**
  Optional. Specify the maximum data length of the packet to be output in the range of 1 to 9014 bytes. If omitted, this parameter is set to 192 bytes.

3 Execute the "show nas-pcap" command of ETERNUS CLI to check if a packet trace is running.

```
CLI> show nas-pcap
<CM#0 Packet Capture Information>
Free Space (MB)  [5000]
NAS Interface No  [0,2,4]

<CM#1 Packet Capture Information>
Free Space (MB)  [5000]
NAS Interface No  [1]
```

If the packet trace is running, the NAS interface port number is displayed in "NAS Interface No".

4 Reproduce the situation when the trouble occurred.
5. Packet Trace Acquisition Settings

5. Execute the "stop nas-pcap" command of ETERNUS CLI to stop the packet trace output.

```sh
stop nas-pcap
```

6. Execute the "create nas-engine-user" command of ETERNUS CLI to create a user account that is used to log in to the investigation log FTP.

When the user account for the investigation log FTP is used for the login, the directory that is exclusive for the investigation logs is the home directory.

The following example is for when user name USER1 is specified and a user account that is used to log in the investigation log FTP is created with an expiration period of five hours. After the command is executed, an input prompt is displayed. Specify a password in the range of 8 to 32 characters.

```sh
create nas-engine-user -type dump -name USER1 -expiry 5
```

- **-type**
  - Specify the user type. Specify "dump" here to create a user account for the investigation log FTP.

- **-name**
  - Specify the user name.

  The character string that can be specified for the user name has the following requirements.
  - The number of characters that can be specified is 1 to 19 characters.
  - The following types of characters can be used.
    - Alphanumeric characters (US-ASCII code)
    - Numerical characters
  - The following reserved words cannot be specified.
    adm, audio, bin, cdrom, cgred, daemon, dialout, dip, disk, floppy, ftp, games, gopher, halt, kmem, ldap, lock, lp, mail, mailnull, man, mem, nfnobody, nobody, nsd, nsld, ntp, operator, oprofile, root, rpc, rpcuser, saslauth, shareuser$, shutdown, smmsp, sshd, sync, sys, tape, tcpdump, tty, users, utempter, utmp, uucp, vsca, video, wheel
  - Different user account names must be used for the audit log FTP and the investigation log FTP.
  - The user name that is registered in the authentication server cannot be used.
  - The characters are case-insensitive for Active Directory authentication servers.

- **-expiry**
  - Specify the expiration date of the password.

7. From the NIC-CA port, log in to FTP using the account that was created in Step 6 to acquire the packet trace file.

  Specify "binary mode" as the transfer mode on the client side.

8. Analyze the acquired trace information file using software such as WireShark.
After the analysis, execute the "clear nas-pcap" command of ETERNUS CLI to delete any unnecessary packet trace files.

```
clear nas-pcap
```

End of procedure
6. System Status Check

Check the status of the ETERNUS DX with ETERNUS Web GUI, ETERNUS CLI or the ETERNUS SF software.

If the file system capacity is checked immediately after the NAS volume is created, some capacity is recognized as being a used area even when no file writing has been performed.

The file system capacity can be checked with the following methods:

- **For CIFS client**
  Display the properties in Windows.

- **For NFS client**
  Mount the file system via UNIX/Linux and then execute the "df" command.

- **For ETERNUS Web GUI**
  Display the [NAS] screen of the [Connectivity] category.

- **For ETERNUS CLI**
  Execute the "show nas-df" command.

Checking the Shared Folders

- **ETERNUS Web GUI**

  ETERNUS Web GUI can be used to list and check the status of NAS shared folders.
  
  The status of the created shared folders can be viewed in the [NAS] screen. Check if the shared folders are operating normally.
**ETERNUS CLI**

ETERNUS CLI can be used to check the status of the NAS shared folders in detail.

An example of ETERNUS CLI command execution is shown below.

```
CLI> show nas-share -volume-number 3
<NAS Share Information>
Share No. [0]
Share Name [NAS-SHARE#0]
Volume No. [3]
Volume Name [NAS-VOL#0]
Share [Active]
Service [NFS]
NFS Export Path [/mnt/nas/nv3/data/NAS-SHARE#0]
Access [READ-WRITE]
Oplocks [-]
SMB Encryption [-]
ABE [-]
Owner [root]
Group [root]
Allow CIFS Hosts [-]
Deny CIFS Hosts [-]
Allow NFS Hosts []
CIFS Access Users(r) [-]
CIFS Access Users(rw) [-]
CIFS Access Groups(r) [-]
CIFS Access Groups(rw) [-]
Audit Log [-]

<NAS Share Information>
Share No. [1]
Share Name [NAS-SHARE#1]
Volume No. [3]
Volume Name [NAS-VOL#0]
Share [Active]
Service [NFS-CIFS]
NFS Export Path [/mnt/nas/nv3/data/NAS-SHARE#1]
Access [READ-WRITE]
Oplocks [Disable]
SMB Encryption [Disable]
ABE [Disable]
Owner [root]
Group [root]
Allow CIFS Hosts []
Deny CIFS Hosts []
Allow NFS Hosts []
CIFS Access Users(r) []
CIFS Access Users(rw) []
CIFS Access Groups(r) []
CIFS Access Groups(rw) []
Audit Log [Disable]
```
Checking the Home Directories

ETERNUS CLI

The list of home directories can be checked from ETERNUS CLI.
An example of ETERNUS CLI command execution is shown below.

```bash
CLI> show nas-home-directory
domainA\userA
domainA\userAA
domainA\userAAA
domainB\userA
domainB\userB
userA
userB
BASICuserABC
```
ETERNUS Web GUI

The status of the NAS interface settings can be checked in a list from the ETERNUS Web the GUI screen. The statuses of the NAS interface setting, Bonding and VLAN that were created by the customers are displayed in the [NAS Interface] screen. Check whether the NAS interface setting is set correctly.
ETERNUS CLI

The state of the NAS interface settings can be checked in a list from ETERNUS CLI.
An example of ETERNUS CLI command execution is shown below.

```
cli> show nas-interface
<NAS Interface Information>
NAS Interface No.  [0]
Port              [CM#0 CA#1 Port#0]
VLAN ID           [-]
RIP                [enable]
IP Address        [192.168.1.10]
Subnet Mask       [255.255.255.0]
Gateway IP Address [192.168.1.1]
Link Local Address [-]
Connect IP Address [-]
IPv6 Gateway IP Address [-]

<NAS Interface Information>
NAS Interface No.  [1]
Port              [CM#1 CA#1 Port#0]
VLAN ID           [-]
RIP                [enable]
IP Address        [192.168.1.11]
Subnet Mask       [255.255.255.0]
Gateway IP Address [192.168.1.1]
Link Local Address [-]
Connect IP Address [-]
IPv6 Gateway IP Address [-]

cli> show nas-bonding
<Bonding Information>
Master Port        [CM#0 CA#1 Port#0]
Member Port        [CM#0 CA#1 Port#1]
Bonding Mode       [balance-alb]
Hash Policy        [Layer2]

<Bonding Information>
Master Port        [CM#1 CA#1 Port#0]
Member Port        [CM#1 CA#1 Port#1]
Bonding Mode       [balance-alb]
Hash Policy        [Layer2]

cli> show nas-multipath
CM#0 CA#1 Port#0 <-> CM#1 CA#1 Port#0 (Normal)
```
ETERNUS Web GUI

The state of the environment settings can be checked in a list from the ETERNUS Web GUI screen. The status of the server settings, the authentication server settings, and the local user settings that the customer set is displayed in the [Environment Settings] screen. Check whether the server settings are set correctly.
The state of the NAS environment settings can be checked in a list from ETERNUS CLI. An example of ETERNUS CLI command execution is shown below.

<table>
<thead>
<tr>
<th>CLI&gt; show nas-server</th>
<th>Server Name</th>
<th>[DX4611402002]</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI&gt; show nas-dns</td>
<td>Primary(IPv4)</td>
<td>[192.168.1.101]</td>
</tr>
<tr>
<td>CLI&gt; show nas-ad</td>
<td>Server1</td>
<td>[192.168.1.102]</td>
</tr>
<tr>
<td>CLI&gt; show nas-ldap</td>
<td>Server1</td>
<td>[192.168.1.103]</td>
</tr>
<tr>
<td>CLI&gt; show nas-local-user</td>
<td>ID  Name</td>
<td>Primary Secondary</td>
</tr>
<tr>
<td></td>
<td>--------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>450 shareuser$</td>
<td>451 -</td>
</tr>
<tr>
<td></td>
<td>500 User00</td>
<td>500 501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516</td>
</tr>
<tr>
<td></td>
<td>501 User01</td>
<td>500 501,509</td>
</tr>
<tr>
<td></td>
<td>502 User02</td>
<td>510 511,512,513,514,515,516,517,518,519,520,521,522,523,1002,1003,1004</td>
</tr>
<tr>
<td></td>
<td>999 user99</td>
<td>599 666,777</td>
</tr>
</tbody>
</table>
Checking the Quota Management

■ ETERNUS Web GUI

The state of the Quota management settings can be checked in a list from the ETERNUS Web GUI screen. The status of the Quota that the customer set is displayed in the [Quota Management] screen. Check whether the Quota settings are set correctly.
ETERNUS CLI

The state of the Quota management can be checked in a list from the ETERNUS CLI screen. An example of ETERNUS CLI command execution is shown below.

```
CLI> show nas-quota
<Quota Setting Information>
Quota No. [0]
State [Normal]
Volume No. [3]
Volume Name. [nasvol0]
User [Administrator]
Used Disk Space(KB) [1638400]
Limit Disk Space(KB) [0]
Warning Disk Space(KB) [0]
Numbers of files [289]
File Limit [10000000]
File Warning [1000000]

<Quota Setting Information>
Quota No. [1]
State [Normal]
Volume No. [3]
Volume Name. [nasvol0]
User [user1001]
Used Disk Space(KB) [108134400]
Limit Disk Space(KB) [0]
Warning Disk Space(KB) [0]
Numbers of files [400641]
File Limit [10000000]
File Warning [1000000]
```
Checking the Snapshots

**ETERNUS Web GUI**

A list of snapshot setting states can be checked from the ETERNUS Web GUI screen. The setup information for the volumes that were set with Snapshot is displayed on the [Volume] screen. Confirm that the snapshots have been successfully acquired.
ETERNUS CLI

A list of snapshot setting states can be checked from ETERNUS CLI.
The setup information for the volumes that were set with Snapshot is displayed. Confirm that the snapshots have been successfully acquired.

An example of ETERNUS CLI command execution is shown below.

```
CLI> show nas-snapshot
Snapshot Setting Information
Volume Number       [4]
Volume Name         [NAS_VOL#0]
Snapshot Status     [Normal]
Schedule            [Active]
Mode                [Auto]
Day                 [Daily]
Time                [0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23]
Generation Count    [8]
Snapshot Volume Information
RAID Group Number   [1]
RAID Group Name     [RG#1]
Volume No. Name Snapshot Date Status
----------------- -------- ------- -----
10 NAS_VOL#0$snap_2 2016-03-03 16:00 Normal
  9 NAS_VOL#0$snap_1 2016-03-03 15:00 Normal
  8 NAS_VOL#0$snap_0 2016-03-03 14:00 Normal
 11 NAS_VOL#0$snap_3 - -
 12 NAS_VOL#0$snap_4 - -
 13 NAS_VOL#0$snap_5 - -
 14 NAS_VOL#0$snap_6 - -
```

Checking the Backup Information

The state of the backup information can be checked from the ETERNUS SF Web Console screen. A check cannot be performed from ETERNUS Web GUI or ETERNUS CLI.

ETERNUS SF Storage Cruiser

For more details, refer to "ETERNUS SF Storage Cruiser Operation Guide".
7. How to Access from Clients

Access from CIFS Clients

To gain access via Windows, assign a network drive and set file sharing to the shared folder.
To assign a network drive, enter the following string in the address bar.
\IP_address_of_the_NAS_interface\Shared_folder_name

The authentication process during access varies depending on whether an authentication server or local user authentication is set.

- When Active Directory authentication is used
  Enter the user name and password that are registered in the Active Directory authentication server. Specify the user name in the following format:
  netbios_domain_name\User_name
  Example: domain\user1
  Authentication is not required for a client that previously accessed the Active Directory authentication server.

- When local user authentication is used
  Enter the user name and password that are registered as a local user. Note that an authentication is not required when the same user name and password are used for both the ETERNUS DX and the CIFS client.

- When authentication is not used
  Enter "shareuser$" for the user name and "share!" for the password.
  For controller firmware versions V10L53 and later, "shareuser$" can be deleted and recreated. However, the previous password (share!) cannot be specified for the re-creation because the password must contain eight characters or more.

Caution

During the operation phase
If the I/O load is increased and CIFS is used for connections between the Windows 10 client and the CIFS shared folder or the CIFS/NFS shared folder where SMB Encryption is enabled, there are cases in which the shared folder may become disconnected. For that case, reconnect the shared folder.
If the connection to the shared folder is disconnected again even after reconnecting, review the amount of I/O from the Windows 10 client to the shared folder.
Access from NFS Clients

To perform access via UNIX/Linux, mount to the shared folder. Log in to UNIX/Linux and execute the "su" command to switch the user to the administrator. Mount the shared folder by executing the "mount" command to allow access and then log in to UNIX/Linux via LDAP authentication. Writing to or reading from the shared folder becomes available.

During the operation phase

- When mounting from an NFS client, if the "mount" command is executed without specifying the "rsize" option or the "wsize" option, the buffer size that is applied during Read/Write operations is set. The setting value varies depending on the models.

<table>
<thead>
<tr>
<th>Model</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETERNUS DX100 S4/DX100 S3</td>
<td>512KB</td>
</tr>
<tr>
<td>ETERNUS DX200 S4/DX200 S3</td>
<td>1MB</td>
</tr>
<tr>
<td>ETERNUS DX500 S4/DX500 S3</td>
<td>1MB</td>
</tr>
<tr>
<td>ETERNUS DX600 S4/DX600 S3</td>
<td>1MB</td>
</tr>
</tbody>
</table>

In this case, data with the same size as the buffer is resent to environments where access from remote sites is retransmitted frequently. When mounting from an NFS client, specify the "rsize" option or the "wsize" option as required to reduce the buffer size.

The buffer size setting may be different depending on the NFS client. For details, check the specifications of the NFS client.

- If NFSv4.0 is enabled and version specification is omitted when mounting from the client, the following clients are connected with NFSv4.0.
  - Red Hat Enterprise Linux 6 or later
  - Solaris 10 or later

Log in to UNIX/Linux enables access to the shared folders when LDAP authentication is not used. Specify the following character strings when executing the "mount" command.

Note that the <Path_of_the_shared_folder> can be specified with one of the following methods.

- /mnt/nas/nv<Volume_number>/data/<Shared_folder_name>
- The <NFS Export Path> that can be checked with the "show nas-share" command of ETERNUS CLI.

For a display example of the "show nas-share" command, refer to the execution example of the ETERNUS CLI command in "Checking the Shared Folders" (page 142).
For Solaris

- When the controller firmware version is V10L51 or later, executing the following command performs a mount with NFSv4.0.

```
mount -F nfs <IP_address_of_the_NAS_interface>:<Path_of_the_shared_folder> <Mount_destination_directory>
```

- Executing the following command performs a mount with NFSv3.

```
mount -F nfs -o vers=3 <NAS_server_name>:<Path_of_the_shared_folder> <Mount_destination_directory>
```

- Executing the following command performs a mount with NFSv4.0.

```
mount -F nfs -o vers=4 <IP_address_of_the_NAS_interface>:<Path_of_the_shared_folder> <Mount_destination_directory>
```

For Linux

- When the controller firmware version is V10L51 or later, executing the following command performs a mount with NFSv4.0.

```
mount -t nfs <IP_address_of_the_NAS_interface>:<Path_of_the_shared_folder> <Mount_destination_directory>
```

- Executing the following command performs a mount with NFSv3.

```
mount -t nfs -o nfsvers=3 <IP_address_of_the_NAS_interface>:<Path_of_the_shared_folder> <Mount_destination_directory>
```

- Executing the following command performs a mount with NFSv4.0.

```
mount -t nfs4 <IP_address_of_the_NAS_interface>:<Path_of_the_shared_folder> <Mount_destination_directory>
```

For details on the function to automatically perform mounting at the startup of the UNIX/Linux OS, refer to the manuals of the relevant OS.
8. **Backup/Restore Settings**

This chapter provides the settings required to back up NAS volumes and the procedures to back up and restore NAS volumes.
ETERNUS SF AdvancedCopy Manager is required for using the backup/restore function.
A configuration for the backup/restore function cannot be performed from ETERNUS Web GUI or ETERNUS CLI.

**Backup Settings**

For more details, refer to "ETERNUS SF Web Console Guide".

**Backup**

For more details, refer to "ETERNUS SF Web Console Guide".

**Restoration**

For more details, refer to "ETERNUS SF Web Console Guide".
9. Backup Software Settings

Use backup software to back up or restore files using the ETERNUS DX as a backup device. Data is transferred to the NAS user volume in the ETERNUS DX through the NAS network.

This chapter describes the necessary settings and notes for backup software that can be used in NAS environments for the ETERNUS DX.

**Caution**

**During the operation phase**

When restoring NAS user volumes, restore them to existing NAS user volumes or to newly created NAS user volumes without deleting the existing ones.

**Note**

**During the configuration phase**

For details on how to set up and operate backup software, refer to the manual for the backup software.

**Notes When Using Arcserve Backup**

When Active Directory authentication is being performed, the user who is using Arcserve Backup must belong to the "Domain Admins" group.

When local user authentication is being performed, the user who is using Arcserve Backup must belong to "BUILTIN\Administrators" or "BUILTIN\Backup Operators".

If the controller firmware version is earlier than V10L53 and "shareuser$" is used, Arcserve Backup can be used with "shareuser$".
Notes When Using NetVault SmartDisk

In Red Hat Enterprise Linux environments, to back up data to a shared folder that was created for NFS shared environments using NetVault SmartDisk, perform either of the following settings.

- To set "no_root_squash" to all backup hosts that use the shared folder, specify "root" for "Owner" and "Group" of the shared folder.
  
  For ETERNUS CLI, if "Owner" and "Group" are omitted, "root" is specified.

- To set "no_root_squash" to a specific backup host, use the "create nas-share" command or the "set nas-share" command of ETERNUS CLI to specify the "no_root_squash" option for the backup host.
  
  This is available for controller firmware versions V10L53 and later.

  For more details, refer to "ETERNUS CLI User's Guide".

Notes When Using NetWorker

In Red Hat Enterprise Linux environments or in Solaris OS environments, to back up data to a shared folder that was created for NFS shared environments using NetWorker, perform either of the following settings.

- To set "no_root_squash" to all backup hosts that use the shared folder, specify "root" for "Owner" and "Group" of the shared folder.
  
  For ETERNUS CLI, if "Owner" and "Group" are omitted, "root" is specified.

- To set "no_root_squash" to a specific backup host, use the "create nas-share" command or the "set nas-share" command of ETERNUS CLI to specify the "no_root_squash" option for the backup host.
  
  This is available for controller firmware versions V10L53 and later.

  For more details, refer to "ETERNUS CLI User's Guide".
Notes When Using NetBackup

In Red Hat Enterprise Linux environments or in Solaris OS environments, to back up data to a shared folder that was created for NFS shared environments using NetBackup, perform either of the following settings.

- To set "no_root_squash" to all backup hosts that use the shared folder, specify "root" for "Owner" and "Group" of the shared folder.
  
  For ETERNUS CLI, if "Owner" and "Group" are omitted, "root" is specified.

- To set "no_root_squash" to a specific backup host, use the "create nas-share" command or the "set nas-share" command of ETERNUS CLI to specify the "no_root_squash" option for the backup host.
  
  This is available for controller firmware versions V10L53 and later.

  For more details, refer to "ETERNUS CLI User's Guide".

The ETERNUS DX is not displayed for "network" in the left frame of the NetBackup [Backup, Archive, and Restore] backup screen because of the specifications of the ETERNUS DX. Therefore, folders and files in the CIFS shared environments of the ETERNUS DX cannot be backed up. Perform manual backups or scheduled backups using a policy.

In Windows environments, when data is restored to a shared folder that was created for CIFS shared environments using NetBackup, the audit information is not restored.

Notes When Using ETERNUS SF TSM

In Windows environments, to back up data from a shared folder that was created for CIFS shared environments using ETERNUS SF TSM, set "skipntpermissions yes" in the "dsm.opt" file.

When backups are performed from CIFS shared environments, the audit information is not backed up.
10. Troubleshooting

This chapter explains how to troubleshoot the errors that occur during a NAS environment system configuration or system operation.

Configuration Errors

If the problem persists, contact your maintenance engineer according to "Required Information for Inquiries" (page 170).

Table 17 Configuration Errors

<table>
<thead>
<tr>
<th>No.</th>
<th>Symptom</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An error message &quot;ED198 (Process is timeout.)&quot; or &quot;ED710 (NAS internal error.)&quot; is output when the &quot;set nas-ad&quot; command or the &quot;create nas-share&quot; command is executed.</td>
<td>A network error occurred creating an environment where communication is temporarily not possible.</td>
<td>Execute the command again.</td>
</tr>
<tr>
<td>2</td>
<td>An error message &quot;ED710 (NAS internal error.)&quot; is output when the &quot;create nas-volume&quot; command is executed.</td>
<td>The free space in the Thin Provisioning Pool (TPP) is insufficient.</td>
<td>If the free capacity in the TPP is insufficient, delete the created NAS volumes, secure 417GB or more free capacity, and then execute the &quot;create nas-volume&quot; command to create NAS volumes.</td>
</tr>
<tr>
<td>No.</td>
<td>Symptom</td>
<td>Cause</td>
<td>Resolution</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>-------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| 3   | An error message “ED727 (Domain join error.)” is output when the “create nas-share” command or the “set nas-ad” command is executed. | • The Active Directory authentication server setting is incorrect.  
• No Active Directory servers are registered in the DNS.  
• The NAS interface setting is incorrect.  
• If Active Directory was previously set using an existing domain within the same domain tree as the specified domain, the Active Directory setting may fail due to a Windows restriction ([https://technet.microsoft.com/en-us/library/dn535779(v=ws.11).aspx](https://technet.microsoft.com/en-us/library/dn535779(v=ws.11).aspx)) that the machine with an overlapping Service Principal Name (SPN) for Active Directory cannot exist in the same forest. | • If the IP address for the Active Directory server is incorrectly set  
• If an error message is output after executing the “set nas-ad” command, set the correct IP address, and then re-execute the command.  
• If an error message is output after executing the “create nas-share” command, set the correct IP address, execute the “set nas-ad” command, and then re-execute the “create nas-share” command.  
• If the domain name of the Active Directory server is incorrectly set  
• If an error message is output after executing the “set nas-ad” command, set the correct domain name, and then re-execute the command.  
• If an error message is output after executing the “create nas-share” command, set the correct domain name, execute the “set nas-ad” command, and then re-execute the “create nas-share” command.  
• If a user that holds authority over the Active Directory was not specified as the domain administrator for the Active Directory using the “set nas-ad” command or if that user’s password is incorrect  
• If an error message is output after executing the “set nas-ad” command, specify the correct user, and then re-execute the command.  
• If an error message is output after executing the “create nas-share” command, specify the correct user, execute the “set nas-ad” command, and then re-execute the “create nas-share” command.  
• If Active Directory servers are not registered in the DNS, configure the DNS so the FQDN can be resolved for the Active Directory, and then re-execute the command.  
• If the NAS interface setting is wrong, correctly set the value. Make sure that the NAS interface is in an Active-Active connection state, and then re-execute the command. |
<table>
<thead>
<tr>
<th>No.</th>
<th>Symptom</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| 3   | An error message "ED727 (Domain join error.)" is output when the "create nas-share" command or the "set nas-ad" command is executed. | • The Active Directory authentication server setting is incorrect.  
• No Active Directory servers are registered in the DNS.  
• The NAS interface setting is incorrect.  
• If Active Directory was previously set using an existing domain within the same domain tree as the specified domain, the Active Directory setting may fail due to a Windows restriction (https://technet.microsoft.com/en-us/library/dn535779(v=ws.11).aspx) that the machine with an overlapping Service Principal Name (SPN) for Active Directory cannot exist in the same forest. | • When checking the Directory Service of the application and the service log from the event viewer of the specified Active Directory server in environments that use a domain tree configuration for Active Directory and the following message is output.  

```
Error XX/XX/20XX XX:XX:XX XX ActiveDirectory_DomainService 2974 Global Catalog
-------------------------------
The attribute value provided is not unique in the forest or partition. Attribute: servicePrincipalName Value=HOST/SERVER
CN=SERVER,CN=Computers,DC=child,DC=DXS3 TE3T3,DC=LOCAL Winerror: 8647
See http://go.microsoft.com/fwlink/?LinkID=279782 for more details on this policy.
-------------------------------
```

Perform one of the following procedures.  
• Use an Active Directory domain (such as a parent domain and a child domain) that is different from the specified Active Directory domain to delete the computer account with the NAS server name of the ETERNUS DX.  
For information on how to delete the computer accounts, refer to the following URL.  
• Change the NAS server name from ETERNUS Web GUI or ETERNUS CLI of the ETERNUS DX. |
| 4   | An error message "ED728 (Server connection error.)" is output when the "create nas-share" command, the "set nas-ad" command, or the "set nas-ldap" command is executed. | • A network error has occurred.  
• The NAS interface setting is incorrect. | • If an unknown error occurs on the network and communication is not possible, communication with the Active Directory authentication server may temporarily become unavailable. Wait for a while and then execute the command again.  
• If the NAS interface setting is wrong, correctly set the value. Make sure that the NAS interface is in an Active-Active connection state, and then re-execute the command. |
<p>| 5   | An error message &quot;ED729 (Clock skew too great.)&quot; is output when the &quot;create nas-share&quot; command or the &quot;set nas-ad&quot; command is executed. | The time for the Active Directory authentication server and the time specified in the ETERNUS DX differ by five minutes or more. | The time synchronization setting is incorrect and the time of the Active Directory authentication server and the time specified in the ETERNUS DX may differ by five minutes or more. Synchronize the time and then execute the command again. |
| 6   | An error message &quot;ED72A (Improper user or group.)&quot; is output when the &quot;create nas-share&quot; command is executed. | The user name or the group name is incorrect. | A user name or group name that cannot be used may have been specified. Specify a correct user name or group name, and then re-execute the command. |
| 7   | An error message &quot;ED72B (User or group does not exists.)&quot; is output when the &quot;create nas-share&quot; command is executed. | The user name or the group name is incorrect. | The specified user name or group name does not exist. Specify a correct user name or group name, and then re-execute the command. |</p>
<table>
<thead>
<tr>
<th>No.</th>
<th>Symptom</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>An error message &quot;ED72C (Improper allow host address.)&quot; is output when the &quot;create nas-share&quot; command, the &quot;set nas-share&quot; command, or the &quot;delete nas-share&quot; command is executed.</td>
<td>- The allowed host setting is incorrect. &lt;br&gt;- The allowed host setting for the existing shared folder is incorrect. &lt;br&gt;- The name resolution of the FQDN is disabled.</td>
<td>The host name or the FQDN specified for the allowed host may be incorrect. Specify the correct allowed host, and then re-execute the command. In addition, check whether communication with the DNS server is normal and whether the allowed host setting for the existing shared folder is normal, and then check whether the name resolution of the FQDN is enabled.</td>
</tr>
<tr>
<td>9</td>
<td>An error message &quot;ED72B (User or group does not exists.)&quot; is output when the &quot;set nas-share&quot; command is executed.</td>
<td>- For controller firmware versions earlier than V10L53 &lt;br&gt;- For controller firmware versions V10L53 or later</td>
<td>- If the ETERNUS DX does not belong to the domain, specify &quot;root&quot; for the owner and group settings. &lt;br&gt;- To set values other than &quot;root&quot; for the owner and group settings, configure the authentication server and register the ETERNUS DX to the domain. &lt;br&gt;- If the ETERNUS DX does not belong to the domain, specify &quot;root&quot; for the owner and group settings. &lt;br&gt;- To set values other than &quot;root&quot; for the owner and group settings, configure the authentication server and register the ETERNUS DX to the domain. &lt;br&gt;Otherwise, use the local user authentication to register the specified user name or group name before the &quot;set nas-share&quot; command is executed.</td>
</tr>
<tr>
<td>10</td>
<td>An error message &quot;ED72D (Authority error.)&quot; is output when the &quot;set nas-ldap&quot; command is executed.</td>
<td>- The setting for the LDAP domain administrative user is incorrect. &lt;br&gt;- The NAS interface setting is incorrect.</td>
<td>A user with LDAP domain administrator authority was not specified or that user's password is incorrect. Specify the correct user account and then re-execute the command. &lt;br&gt;- If the NAS interface setting is wrong, correctly set the value. Make sure that the NAS interface is in an Active-Active connection state, and then re-execute the command.</td>
</tr>
<tr>
<td>11</td>
<td>The message &quot;ED198 (Process is timeout.)&quot; is output when a CIFS or CIFS/NFS shared folder is created on a newly created NAS volume after configuring the authentication server.</td>
<td>Communication with the authentication server may become unavailable.</td>
<td>Release and reset the authentication server setting, and then re-create the shared folder.</td>
</tr>
<tr>
<td>12</td>
<td>A &quot;0xD1C1 (An error occurred in the CM)&quot; error is responded during a NAS configuration.</td>
<td>During a NAS configuration, the state of controller or the NAS Engine has become Error.</td>
<td>If there is a &quot;0xD1C1 (An error occurred in the CM)&quot; error response during the NAS configuration, request your maintenance engineer for a controller maintenance or NAS Engine maintenance.</td>
</tr>
<tr>
<td>13</td>
<td>An error message &quot;ED198 (Process is timeout.)&quot; is output when a NAS volume is created.</td>
<td>A timeout occurred because the load was concentrated on the target RAID group.</td>
<td>If multiple NAS volumes are created consecutively when a TPP is configured with a RAID group, the load is concentrated on the RAID group and a process may fail with an &quot;ED198 (Process is timeout.)&quot; error. &lt;br&gt;If a failure occurs, after waiting approximately 30 minutes, delete the failed NAS volume, and create a NAS volume again.</td>
</tr>
<tr>
<td>14</td>
<td>The CIFS shared folders cannot be accessed or the files cannot be handled from the host (client) when a DNS server is used.</td>
<td>A lookup for the target host is not possible with the IP address because host information is not registered on the DNS server.</td>
<td>Register host information to the DNS server and make sure that a reverse lookup is possible for the target host with the IP address.</td>
</tr>
</tbody>
</table>
### Operation Errors

#### Table 18 Operation Errors

<table>
<thead>
<tr>
<th>No.</th>
<th>Symptom</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| 1   | An error message "ED733 (The files or folders exist in this shared folder. Please delete it first.)" is output when a shared folder is deleted. | • There is a client that is connected to the shared folder.  
• Data exists in the shared folder. | • Remove client connections (by unmounting [for NFS] or by disconnecting the network drive [for CIFS]).  
• Before deleting the shared folder, delete all the data in the shared folder.  
• If the error message is still output after deleting all the data in the shared folder, hidden files and system files that are not displayed due to the default setting on the client may have remained in the shared folder. Change the setting on the client side so that these files are displayed and make sure that there is no data remaining. |
| 2   | When a directory or file is created or deleted from an NFS client, one of the following errors occurs in the client application.  
• EEXIST error occurs during creation  
• ENOENT error occurs during deletion | If the following events occur while a directory or file is being created or deleted from an NFS client, an EEXIST error or an ENOENT error may occur depending on the client application.  
• Switching of the controller for access by the failover function  
• Rebooting and stopping the ETERNUS DX  
For the NFS protocol, if events such as switching, rebooting, and stopping of the operation node occur in the NFS server, data consistency must be ensured on the NFS client side. For that reason, if the NFS server stops before the processed data is reflected in the ETERNUS DX, the NFS client detects the error and judges if a data resend is necessary to prevent data inconsistency. | Check the operation that was being performed to the directory or file when the error occurred and confirm that the creation or deletion process on the file system is complete.  
If the directory/file on the file system is not created/deleted, create/delete the directory/file again after the ETERNUS DX becomes available once the controller failover or the startup sequence finishes. |
| 3   | When a client that is accessing with the NFSv4.0 protocol executes the "ls -l" command, "nobody" is output for the user name and group name. | • The NFSv4 domain in the NFS client differs from the one in the ETERNUS DX.  
• The cache information of the NFS client user is not updated. | • If the domains of the NFS client and the ETERNUS DX differ, set them with the same NFSv4 domain.  
• If the cache information of the NFS client user is not updated, clear the user cache information from the NFS client. |
<p>| 4   | A timeout error occurred while a NAS volume reconfiguration (format conversion) was being performed. | A controller failure or throughput reduction due to high CPU usage caused an operational failure. | Reboot the ETERNUS DX. After the startup is complete, execute the NAS volume reconfiguration (format conversion) again. |</p>
<table>
<thead>
<tr>
<th>No.</th>
<th>Symptom</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| 5   | When a NAS volume reconfiguration (format conversion) is performed with firmware version V10L51 or later, the NAS FS Version does not become "4". | The NAS volume reconfiguration (format conversion) was interrupted.  
• An error occurred while the NAS volume reconfiguration (format conversion) was being performed.  
• The power has been cut (such as from a power failure) during the process. | Execute the "show volumes -mode detail" command from ETERNUS CLI to check the NAS FS Version of the target volume, and perform the following procedures. If the problem persists, contact your maintenance engineer.  
• If the NAS FS Version shown is "4":  
  The process has successfully been completed. No action is needed.  
• If the NAS FS Version shown is ".":  
  Restore the NAS volumes from backups. After a restoration is complete, execute a NAS volume reconfiguration (format conversion) again.  
  Make sure to execute a NAS volume restoration and a NAS volume reconfiguration (or format conversion) again for the target volume. If the NAS volume reconfiguration (format conversion) was interrupted, the NAS FS Version of NAS volumes other than the target volume may be also shown as ".".  
  However, when the target volume for the NAS volume reconfiguration (format conversion) returns to a normal state, the NAS FS Version of NAS volumes other than the target volume are also shown correctly.  
  • If the NAS FS Version shown is a number other than "4":  
    Execute the NAS volume reconfiguration (format conversion) again. |
| 6   | The volume capacity expansion was interrupted.                         | • An error occurred while the volume capacity expansion was being performed.  
• The power has been cut (such as from a power failure) during the process. | If the volume capacity expansion was interrupted due to an error or a power-supply disconnection (power failure, etc.) during the process, resolve the problem and start the volume capacity expansion again.  
After the process is complete, execute the "show nas-df" command from ETERNUS CLI to confirm that the volume capacity expansion has succeeded. |
| 7   | After a NAS volume is restored, CIFS shared folders cannot be accessed. | The authentication server settings or the owner (Owner) and group (Group) of the shared folder has changed. | Set the authentication server settings, and/or the owner (Owner) and the group (Group) of the shared folder and access the folder again. |
| 8   | After a maintenance of the controller or after the ETERNUS DX is started, the started controller cannot be accessed with CIFS. | Proper communication with the authentication server is unavailable. | Release the authentication server settings and then perform a reconfiguration. |
| 9   | CIFS access may fail.                                                  | • The access load exceeds the network bandwidth.  
• The network bandwidth is insufficient. | • CIFS access may fail if the access load exceeds the network bandwidth. Check if the network bandwidth is sufficient for the amount of access.  
• If the network bandwidth is insufficient, review the environment or limit access according to the load on the network bandwidth. |
<table>
<thead>
<tr>
<th>No.</th>
<th>Symptom</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| 10  | The CIFS client and the NFS client cannot access a file. | During a file lock, an error occurred such as the client machine going down or a network error. | When using a controller firmware version V10L33 or later, execute the "delete nas-lock" command from ETERNUS CLI to release the lock state. For details, refer to "Client Resource Deallocation" (page 58).  
When using a controller firmware version earlier than V10L33 and if an error occurs such as the client machine going down or a network error while the file is locked, the locking status is maintained and both the CIFS client and the NFS client cannot access the file.  
Perform the following procedures:  
* If this error occurs during CIFS access, wait until the lock state is automatically released (which takes approximately two hours). After the lock state is released, access the file.  
* If this error occurs during NFS access, the lock state is not automatically released.  
Execute the "forced nas-fsunmount" command and the "forced nas-fsmount" command to perform a remount of the NAS volumes.  
In addition, when performing a mount and remount, refer to the following notes:  
  - Unmounting a NAS volume clears the CIFS and NFS server management information stored in the ETERNUS DX. To prevent inconsistency of management information between the client and ETERNUS DX, unmount the NAS volume on the ETERNUS DX after unmounting the NAS volume on the client with the CIFS or NFS protocol.  
  - Because the file lock state is released for all file systems, remount the NAS volume after stopping operations for all file systems. |
| 11  | CIFS / NFS / RIP / ICMP access is not available. | The firewall setting for the port is "close". | Execute the "set nas-port" command from ETERNUS CLI to change the firewall setting for the port to "open". |
| 12  | Bonding is not performed or the communication at the port that is configured for Bonding is disconnected. | A value larger than "1" is set for "link aggregation collecting minimum count" in the switch setting.  
  - The STP function is enabled for the switch port that is connected with the ETERNUS DX.  
  - The switch that supports EtherChannel is used for mode 0 or mode 2. In addition, the switch is connected to the ETERNUS DX through another switch.  
  - The switch that is compliant with IEEE802.3ad is used for mode 4. In addition, the switch is connected to the ETERNUS DX through another switch.  
  - For cascade connected switches (for a multistage configuration) between hosts and ETERNUS DX storage systems, there is an error in a setting between a host and the switch that is directly connected to the ETERNUS DX. | If a value larger than "1" is set for "link aggregation collecting minimum count" in the switch setting, communication may be disconnected even though a communication path is available. Specify "1" for the link aggregation collecting minimum count.  
If the STP function is enabled for the switch port that is connected with the ETERNUS DX, connection with the ETERNUS DX may fail. Disable the STP function in the switch port. In addition, disable RSTP/ MSTP.  
For mode 0 or mode 2, use the switch that supports EtherChannel and do not connect the switch to the ETERNUS DX via another switch.  
For mode 4, use the switch that is compliant with IEEE802.3ad and do not connect the switch to the ETERNUS DX via another switch.  
If a switch is connected between hosts and ETERNUS DX storage systems with cascade connections (multistage configuration), confirm that there are no problems in the settings between the host and the switch that is directly connected to the ETERNUS DX.  
The guaranteed range of the Bonding setting is up to the switch of the first stage that is connected directly to the ETERNUS DX. |
<table>
<thead>
<tr>
<th>No.</th>
<th>Symptom</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| 13  | A snapshot was acquired, however the acquired snapshot is not displayed in [Properties] - [Previous Versions] on the CIFS client.                                                                     | • There are no differences between the acquired snapshot and the current file.  
• Cache is enabled on the Windows client.                                                                 | Perform one of the following procedures.  
• Procedure 1  
  Overwrite the target file to update it.  
If the target file is identical to the snapshot, the acquired snapshot may not appear in [Previous Versions].  
• Procedure 2  
  Disable the cache in the Windows client.                                                                 |
| 14  | In an environment where both NFS and CIFS are used, an error message related to the authentication server is output when the "create nas-share" command or the "set nas-share" command is executed. | An error occurred while processing the command.                                                                                                                   | An Active Directory authentication error in the CIFS shared folder settings or an LDAP authentication error in the NFS shared folder settings may have occurred.  
Check the status of the Active Directory authentication server or the LDAP authentication server according to the content of the error message. |
| 15  | The snapshots have not been successfully acquired at the configured time.                                                                                                                                   | • The required resources for acquiring snapshots are not sufficient.  
• An error has occurred in the controller or the NAS Engine.                                                                                                    | • If required resources for acquiring snapshots are not sufficient, snapshot acquisitions fail.  
Check the status of the following items.  
- Is the copy table size sufficient?  
- Is the required SDP (SDPV) space sufficient?  
• If the controller or the NAS Engine fails during a snapshot acquisition, the snapshot acquisition may fail.  
Check whether any errors occurred in the ETERNUS DX when the snapshot acquisition failed. |
| 16  | Mounting the NAS backup volumes has failed.                                                                                                                                                               | A mount was performed for the NAS backup volume when no CIFS shared folders exist.                                                                           | Create at least one CIFS shared folder and then mount the NAS backup volume again.                                                                          |
| 17  | An NFS client becomes unable to recognize some of the directories and files in a snapshot that has been acquired, or recognize the reference directory for a snapshot (.snap@GMT-yyyymmdd hhmmss). This symptom does not occur with CIFS clients. | Old cache information of the directory information may remain in the NFS client and prevent it from recognizing some parts of the snapshot.  
Depending on the timing, this symptom may occur if the following events occur while the NFS client references the snapshot destination.  
• Snapshot acquisition  
• ETERNUS DX reboot  
• Controller restart due to a controller error or controller implementation during maintenance | After this symptom occurs, it can be resolved when a snapshot is acquired. This is because the snapshot acquisition updates the directory information.  
If this symptom has to be resolved at any time, remount the shared folder that contains the snapshot for which this symptom occurs from the NFS client. |
<p>| 18  | An error message &quot;EBEC5 (All of quota setting failed. Specified user or group may not exist.)&quot; is output when a trusted domain user is specified for a quota setting for the NAS volume. | A trusted domain user is not recognized by the ETERNUS DX.                                                                                                      | After logging in to the shared folder as a trusted domain user, perform a quota setting again.                                                              |
| 19  | When Active Directory authentication is set, the trusted domain user cannot access the directories/files under the shared folder.                                                                 | If the number of configured trusted domains is 421 or more for the cumulative total, access to the directories/files that are created by the trusted domain user may become unavailable. | Contact your maintenance engineer.                                                                                                                         |</p>
<table>
<thead>
<tr>
<th>No.</th>
<th>Symptom</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| 20  | After the ACL settings of the root directory for the shared folder are changed, the shared folder cannot be accessed. | If Active Directory authentication is set, if a user other than root is set for the owner of the shared folder and root is set for the group, some of the ACL settings may be lost after the ACL settings are changed by a user other than owner. | With the privileges of the user specified as the owner of the shared folder, undo the changes that were made with the client to the access privileges and the properties of the root directory. To allow access from clients that are not the owner of the shared folder and are not in the group of the shared folder, change the owner and the group of the shared folder to "root" and then take one of the following actions.  
• Set the access restrictions using the CIFS access permission setting.  
• Create subfolders under the shared folder and set the appropriate access privileges from the client. |
| 21  | When a quota for the NAS volume is referenced, the trusted domain user information is displayed as "Unknown". | A trusted domain user is not recognized by the ETERNUS DX. | Log in to the shared folder using a trusted domain user. |
| 22  | An error message "ED710 (An internal error.)" is output when a mount is performed for a CIFS shared folder with NFSv4.0 and the relevant shared folder is deleted, the resource for NFS remains and shared folders with the same names cannot be created. | If an NFS shared folder with the different name is created, creating a shared folder with the same name becomes possible. | |
| 23  | After the "set nas-share" command or the "delete nas-share" command is executed and an error occurs, the specified shared folder cannot be accessed. | While the "set nas-share" command or the "delete nas-share" command is running, the controller is switched by the failover function. | After the failover process of the controller is complete, execute the "set nas-share" command or the "delete nas-share" command again. |
| 24  | After the "set nas-ad" command is executed and an error occurs, the shared folder cannot be accessed. | While the "set nas-ad" command is running, the controller is switched by the failover function. | After the failover process of the controller is complete, execute the "set nas-ad" command again. |
| 25  | An error message "ED739 (One or more clients have connected to this shared folder. Please disconnect it first.)" is output when a shared folder is deleted, or an error message "ED748 (The user cannot be deleted because it is currently being used to access to a shared folder.)" is output when a local user is deleted. | The NAS file in the target CIFS shared folder is locked or the NAS file is locked by the target local user.  
The file may remain locked if the network is disconnected with the client or if the client is rebooted. | Release the lock of the target NAS file with the "delete nas-lock" command. |
| 26  | The following error message is output when a NAS volume is deleted.  
• For ETERNUS CLI  
  ED710 (An internal error occurs in the NAS system)  
• For ETERNUS Web GUI  
  An error detected in NAS Engine. Specified volumes cannot be deleted. | The ETERNUS DX failed to delete the NAS volume. | Perform one of the following operations.  
• Reboot the ETERNUS DX. After the reboot is complete, execute the NAS volume deletion again.  
• Restore one NAS system volume at a time for both CMs. After the restoration is complete, execute the NAS volume deletion again.  
For details on the restoration of the NAS system volume, refer to "NAS Function Restoration" in "ETERNUS CLI User's Guide" or "Recover NAS System Volume" in "ETERNUS Web GUI User's Guide".  
A failover or failback of the controller is performed when the NAS system volume is restored. For details, refer to "Multipath Connection (Active-Active Connection)" (page 70). |
<table>
<thead>
<tr>
<th>No.</th>
<th>Symptom</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>After the local user setting is changed, the new setting is not applied (for example, access with groups is not possible after the change).</td>
<td>To apply the changed local user settings in a CIFS environment, the CIFS session must be reconnected by the target local user. However, if file lock information remains, the changed setting may not be applied just by reconnecting.</td>
<td>Execute the &quot;delete nas-lock&quot; command to delete the information of the file that is locked by that target local user and then reconnect the CIFS session.</td>
</tr>
<tr>
<td>28</td>
<td>NAS Engine down occurred while operating the ETERNUS DX with the LDAP authentication server that is specified for the authentication server setting.</td>
<td>The specified LDAP authentication server is not available or is in a state where a connection cannot be made.</td>
<td>Specify the available LDAP authentication server again in the authentication server setting or delete the unused LDAP authentication server setting.</td>
</tr>
<tr>
<td>29</td>
<td>&quot;ED721 (Invalid operation.)&quot; is output when the &quot;forced nas-fsmount&quot; command is executed.</td>
<td>A volume is being checked or restored with the &quot;start nas-fsck&quot; command.</td>
<td>After using the &quot;show nas-fsck&quot; command to confirm that there are no volumes being checked or restored, try again.</td>
</tr>
<tr>
<td>30</td>
<td>Error message &quot;ED198 (Process is timeout.)&quot; is output when multiple shared folders are deleted.</td>
<td>Due to temporary load, the deletion process timed out.</td>
<td>Reduce the number of shared folders to delete to 128 or less, and try again.</td>
</tr>
<tr>
<td>31</td>
<td>Files cannot be copied to the CIFS shared folder.</td>
<td>The ADS information (or Zone Identifier) is added to files that are downloaded from the Internet.</td>
<td>Confirm that the downloaded files are safe and remove the file block from the property screen.</td>
</tr>
</tbody>
</table>
Required Information for Inquiries

Before contacting your maintenance engineer when trouble occurs, prepare the information that is shown below. For details on the maintenance service, refer to "Maintenance Service" in "Operation Guide (Basic)".

● The Model Name and the Serial Number of the ETERNUS DX

This information can be checked by using a device ID label, ETERNUS Web GUI, or ETERNUS CLI.

Device ID label

![Device ID label diagram]

ETERNUS Web GUI screen

![ETERNUS Web GUI screen diagram]

ETERNUS CLI ("show enclosure-status" command)

Output example of the ETERNUS DX100 S3

```
CLI> show enclosure-status
Enclosure View
Storage System Name                   [ETERNUS DX100 S3]
Model Upgrade Status                 [Not Upgraded]
Model Name                           [ETXXXXX]
Serial Number                        [XXXXXXXX]
```

● Details About the Trouble, Any Actions Taken, and the Results of These Actions

● The Devices That Are Connected to the ETERNUS DX

  - The models of the server and network devices
  - The power synchronized unit model
  - The UPS model

● Log/Dump Information of the ETERNUS DX

When your maintenance engineer asks for the log/dump information of the ETERNUS DX, in addition to obtaining the required log/dump information using the log/dump collection function of ETERNUS Web GUI, obtain the investigation logs by FTP.

  - For details on obtaining the log/dump information, refer to "ETERNUS Web GUI User's Guide".
To obtain the investigation logs by FTP, obtain the log/dump information with ETERNUS Web GUI, create a user account that is used to log in to the investigation log FTP, and obtain the logs under the following directories of both controllers by FTP.

/naslog/*
/pdfs/*

For the creation procedure of the user account that is used to log in to the investigation log FTP, refer to "5. Packet Trace Acquisition Settings" (page 138).
# A. Function Specification List

## NAS Volume Specifications

The following table shows the maximum capacity and the maximum number of TPPs and NAS TPVs (NAS volumes) that can be created in the ETERNUS DX.

### For the ETERNUS DX100 S4/DX200 S4 and the ETERNUS DX500 S4/DX600 S4

Table 19 Maximum Number of TPPs/NAS TPVs (NAS Volumes) That Can Be Created (For the ETERNUS DX100 S4/DX200 S4 and the ETERNUS DX500 S4/DX600 S4)

<table>
<thead>
<tr>
<th>Item</th>
<th>ETERNUS DX100 S4</th>
<th>ETERNUS DX200 S4</th>
<th>ETERNUS DX500 S4</th>
<th>ETERNUS DX600 S4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum TPP capacity (*1)</td>
<td>2,048TB</td>
<td>2,048TB</td>
<td>3,072TB</td>
<td>8,192TB</td>
</tr>
<tr>
<td>NAS TPV (NAS volume)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum number of NAS user volumes</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Maximum number of NAS backup volumes</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Maximum capacity of NAS volume (per volume)</td>
<td>128TB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum capacity of NAS volume (per ETERNUS DX)</td>
<td>256TB</td>
<td>512TB</td>
<td>512TB</td>
<td>1,024TB</td>
</tr>
</tbody>
</table>

*1: The maximum pool capacity is the capacity that combines the FTSP capacity and the TPP capacity in the ETERNUS DX. A TPP is composed of NAS user volumes, NAS backup volumes, SAN TPVs, and system volumes. An FTSP is composed of FTVs.
For the ETERNUS DX100 S3/DX200 S3 and the ETERNUS DX500 S3/DX600 S3

Table 20 Maximum Number of TPPs/NAS TPVs (NAS Volumes) That Can Be Created (For the ETERNUS DX100 S3/DX200 S3 and the ETERNUS DX500 S3/DX600 S3)

<table>
<thead>
<tr>
<th>Item</th>
<th>Model</th>
<th>ETERNUS DX100 S3</th>
<th>ETERNUS DX200 S3</th>
<th>ETERNUS DX500 S3</th>
<th>ETERNUS DX600 S3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum TPP capacity (*1)</td>
<td></td>
<td>2,048TB</td>
<td>2,048TB</td>
<td>3,072TB</td>
<td>8,192TB</td>
</tr>
<tr>
<td>NAS TPV (NAS volume)</td>
<td>Maximum number of NAS user volumes</td>
<td>1 (*2)</td>
<td>2 (*3)</td>
<td>2 (*4)</td>
<td>4 (*5)</td>
</tr>
<tr>
<td></td>
<td>Maximum number of NAS backup volumes</td>
<td>1 (*2)</td>
<td>2 (*3)</td>
<td>2 (*4)</td>
<td>4 (*5)</td>
</tr>
<tr>
<td></td>
<td>Maximum capacity of NAS volume (per volume)</td>
<td>128TB</td>
<td>128TB (*2)</td>
<td>256TB (*3)</td>
<td>512TB (*4)</td>
</tr>
<tr>
<td></td>
<td>Maximum capacity of NAS volume (per ETERNUS DX)</td>
<td>128TB (*2)</td>
<td>256TB (*3)</td>
<td>256TB (*4)</td>
<td>512TB (*5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>512TB</td>
<td>1,024TB</td>
</tr>
</tbody>
</table>

*1: The maximum pool capacity is the capacity that combines the FTSP capacity and the TPP capacity in the ETERNUS DX. A TPP is composed of NAS user volumes, NAS backup volumes, SAN TPVs, and system volumes. An FTSP is composed of FTVs.

*2: Values if any of the following conditions are applied.
- For controller firmware versions earlier than V10L53
- When the Memory Extension (ETFMCA / ETFMCA-L / ETDMCAU / ETDMCAU-L) is installed
- When the cache memory included in the Unified kit is installed

*3: Values when the Memory Extension (ETFMCC / ETFMCC-L / ETDMCCU / ETDMCCU-L) is installed for controller firmware version V10L53 or later.

*4: Values when the Memory Extension is not installed (but cache memory included in the Unified kit is installed).

*5: Values when the controller firmware version is V10L33 or later and the Memory Extension is installed.
## File System Specifications

The following table shows the maximum values of the file system specifications.

<table>
<thead>
<tr>
<th>Item</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity of the file system (NAS volume)</td>
<td>128TB</td>
</tr>
<tr>
<td>Capacity of the user data area</td>
<td>130,772GB = 128TB — 300GB</td>
</tr>
</tbody>
</table>
| Number of file systems (per ETERNUS DX) | 2 (ETERNUS DX100 S4)  
| | 4 (ETERNUS DX200 S4)  
| | 4 (ETERNUS DX500 S4)  
| | 8 (ETERNUS DX600 S4)  
| | 1 (*1) (ETERNUS DX100 S3)  
| | 2 (*2) (ETERNUS DX200 S3)  
| | 2 (*3) (ETERNUS DX500 S3)  
| | 4 (*4) (ETERNUS DX600 S3)  |
| Number of shared folders (per ETERNUS DX) (*5) | 256  
| | 5 (*6) |
| Number of files or directories (per file system) | 128,000,000 (*7) |
| Number of directories (per directory) (*8) | 32,000 |
| Number of files that can be opened concurrently (per ETERNUS DX) (*9) | 4,700 (ETERNUS DX100 S4)  
| | 49,700 (ETERNUS DX200 S4)  
| | 49,700 (ETERNUS DX500 S4)  
| | 49,700 (ETERNUS DX600 S4)  
| | 4,700 (ETERNUS DX100 S3)  
| | 49,700 (ETERNUS DX200 S3)  
| | 49,700 (ETERNUS DX500 S3)  
| | 49,700 (ETERNUS DX600 S3)  |
| Number of allowed host lists (per ETERNUS DX) | 5,120 characters |
| Supported protocols | CIFS (SMB 1.0, 2.0, 2.1, 3.0, 3.0.2, and 3.1.1), NFSv2, v3, v4.0, and FTP/FXP |
| Number of entries in the Access Control List (ACL) for each file | CIFS 256 (*10)  
| | NFSv2 256 (*10)  
| | NFSv3 256 (*10)  |
| Number of FTP/FXP sessions (per ETERNUS DX) | 50 |
| Supported file types | Normal files, directories, and symbolic links (*11) |

*1: Number of file systems when either of the following conditions is applied.

- For controller firmware versions earlier than V10L53
- When the Memory Extension (ETFMCA / ETFMCA-L / ETDMCAU / ETDMCAU-L) is installed
- When the cache memory included in the Unified kit is installed
Number of file systems when the Memory Extension (ETFMCC / ETFMCC-L / ETDMCCU / ETDMCCU-L) is installed for controller firmware version V10L53 or later.

Number of file systems when the Memory Extension is not installed (but cache memory included in the Unified kit is installed).

Number of file systems when the Memory Extension is installed for controller firmware version V10L33 or later.

Total number of directories in an ETERNUS DX that can be created in a root directory of the file system.

Number of shared folders for FTP/FXP.

Total number of directories and files. The maximum number of directories and files that is shown in this table may not be possible in some environments.

The maximum number of subdirectories that can be created in a directory. To create more than 32,000 subdirectories, some measures must be taken such as distributing the subdirectories into multiple directories.

The maximum total number of files that can be concurrently opened using CIFS and NFS.

If more than the maximum number of files are concurrently open, a client application may return an I/O error when it writes to a file.

The maximum number of files that can be operated does not change even when multiple clients operate files at the same time.

If the number of ACL entries in the NAS volume (file system) has reached the limit, the value above may be smaller than 256.

The total number of ACL entries that can be recorded per NAS volume is as follows:

CIFS-ACL: 6,539,968,512 (6,237 \times 1,024^2)

POSIX ACL: 46,187,675,648 (44,048 \times 1,024^2)

Hard links support normal files only.
Available Functions for Each Software

ETERNUS Web GUI, ETERNUS CLI, or ETERNUS SF software can be used to configure a NAS environment as well as perform operation management settings. The operations that can be performed depend on the software that is being used.

The following table shows the available functions for each software.

Table 22 Available Functions for Operation Management Interfaces

<table>
<thead>
<tr>
<th>Function</th>
<th>ETERNUS Web GUI</th>
<th>ETERNUS CLI</th>
<th>ETERNUS SF Storage Cruiser (Web Console) (*1)</th>
<th>ETERNUS SF Advanced-Copy Manager (Web Console) (*1)</th>
<th>ETERNUS SF Express (Web Console) (*1)</th>
<th>ETERNUS SF (CLI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS Interface (NIC-CA)</td>
<td>Status display</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Jumbo Frame</td>
<td>Setting</td>
<td>×</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Display</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>SMB Encryption</td>
<td>Setting</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Display</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Access Based Enumeration (ABE)</td>
<td>Setting</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Display</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Large MTU</td>
<td>Setting</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Display</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Transfer rate/mode</td>
<td>Setting</td>
<td>×</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Display</td>
<td>×</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Volume</td>
<td>Creation</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Display</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Expansion</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>NAS interface</td>
<td>Creation</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Deletion</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Change</td>
<td>△</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>List display</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Detail display</td>
<td>×</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Authentication server</td>
<td>Setting</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Local user authentication</td>
<td>Setting</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>DNS server</td>
<td>Setting</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Changing the NAS server name (NetBIOS setting)</td>
<td>Setting</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Bonding</td>
<td>Setting</td>
<td>×</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Display</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Function</td>
<td>ETERNUS Web GUI</td>
<td>ETERNUS CLI</td>
<td>ETERNUS SF Storage Cruiser (Web Console) (*1)</td>
<td>ETERNUS SF Advanced Copy Manager (Web Console) (*1)</td>
<td>ETERNUS SF Express (Web Console) (*1)</td>
<td>ETERNUS SF (CLI)</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------</td>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>VLAN Setting</td>
<td>×</td>
<td>○</td>
<td>○</td>
<td>×</td>
<td>○</td>
<td>×</td>
</tr>
<tr>
<td>Display</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>×</td>
<td>○</td>
<td>☑</td>
</tr>
<tr>
<td>Quota Setting</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>×</td>
<td>○</td>
<td>×</td>
</tr>
<tr>
<td>Display</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>×</td>
<td>○</td>
<td>X</td>
</tr>
<tr>
<td>Snapshot Setting</td>
<td>○</td>
<td>○</td>
<td>○ (wizard)</td>
<td>×</td>
<td>○ (wizard)</td>
<td>X</td>
</tr>
<tr>
<td>Shared folder Creation</td>
<td>○</td>
<td>○</td>
<td>○ (wizard)</td>
<td>×</td>
<td>○ (wizard)</td>
<td>X</td>
</tr>
<tr>
<td>List display</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>×</td>
<td>○</td>
<td>X</td>
</tr>
<tr>
<td>Detail display</td>
<td>×</td>
<td>○</td>
<td>○</td>
<td>×</td>
<td>○</td>
<td>X</td>
</tr>
<tr>
<td>Change</td>
<td>△</td>
<td>○</td>
<td>○</td>
<td>×</td>
<td>○</td>
<td>X</td>
</tr>
<tr>
<td>Audit log Setting</td>
<td>×</td>
<td>○</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Display</td>
<td>×</td>
<td>○</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>X</td>
</tr>
<tr>
<td>Packet trace Setting</td>
<td>×</td>
<td>○</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>X</td>
</tr>
<tr>
<td>Display</td>
<td>×</td>
<td>○</td>
<td>×</td>
<td>×</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Backup/restore Volume creation</td>
<td>×</td>
<td>○</td>
<td>–</td>
<td>○</td>
<td>–</td>
<td>×</td>
</tr>
<tr>
<td>Backup</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>○</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td>Restoration</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>○</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td>Backup destination mount</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>○</td>
<td>–</td>
<td>×</td>
</tr>
<tr>
<td>Backup destination unmount</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>○</td>
<td>–</td>
<td>×</td>
</tr>
<tr>
<td>Backup/Restoration between ETERNUS DX storage systems</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>○</td>
<td>–</td>
<td>×</td>
</tr>
<tr>
<td>Backup</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>○</td>
<td>–</td>
<td>×</td>
</tr>
<tr>
<td>Restoration</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>×</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>Resuming operations in the DR destination</td>
<td>×</td>
<td>×</td>
<td>–</td>
<td>×</td>
<td>–</td>
<td>X</td>
</tr>
</tbody>
</table>

| O: Supported | ×: Not supported | Δ: Partially supported | -: N/A |

*1: For details on the available functions, refer to the manuals for each software.
*2: NAS user volumes are the target volumes.
*3: Displayed only for master ports/member ports.
B. Snapshot Configurable NAS Volume Capacity (Guideline)

This appendix provides the possible NAS volume capacities (guidelines) for snapshot acquisitions. The maximum copy capacity varies depending on the copy table size and resolution settings, and the number of snapshot generations.

- When a Backup Is Performed Using QuickOPC with OPC Restoration

The values in the table are calculated based on the requirements when the following copies are set for the NAS user volume.

- Snapshot
  Same requirements as SnapOPC+ without OPC restoration

- Backup
  Requirements when one QuickOPC session is set for the backup of the NAS user volume and when an OPC restoration is performed from the copy destination to the copy source for restoring this QuickOPC

Figure 26 Operational Configuration (When a Backup Is Performed Using QuickOPC with OPC Restoration)

To set snapshot, calculate the available NAS volume capacity according to the customer's operating environment and adjust the settings so as not to exceed the upper limit.

For details on how to calculate the copy table size, refer to the "Modify Copy Table Size" section in "ETERNUS Web GUI User's Guide". This section describes how to calculate the recommended values based on the copy requirements, the total copy capacity, and the number of sessions. For Snapshots, perform the calculations as shown below.

- Copy requirements
  Same requirements as SnapOPC+ without OPC restoration

- Total copy capacity
  Total capacity of NAS volumes in which Snapshot is set
**B. Snapshot Configurable NAS Volume Capacity (Guideline)**

- **Number of sessions**

  Total number of Snapshot generations to which the schedule is set

  **Table 23 Guidelines for Snapshot Configurable NAS Volume Capacity (When QuickOPC Is Used)**

<table>
<thead>
<tr>
<th>ETERNUS DX</th>
<th>Number of snapshot generations</th>
<th>Resolution</th>
<th>x1</th>
<th>x2</th>
<th>x4</th>
<th>x8</th>
<th>x16</th>
<th>x32</th>
<th>x64</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETERNUS DX100 S4 (Copy table size: 512MB)</td>
<td>16</td>
<td>1,819 (1.8)</td>
<td>3,639 (3.6)</td>
<td>7,279 (7.1)</td>
<td>14,559 (14.2)</td>
<td>29,119 (28.4)</td>
<td>58,238 (56.9)</td>
<td>116,476 (113.7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>963.3 (0.9)</td>
<td>1,926.5 (1.9)</td>
<td>3,853.1 (3.8)</td>
<td>7,706.1 (7.5)</td>
<td>15,412.2 (15.1)</td>
<td>30,824.5 (30.1)</td>
<td>61,648.9 (60.2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>496 (0.5)</td>
<td>992 (1.0)</td>
<td>1,983.9 (1.9)</td>
<td>3,967.9 (3.9)</td>
<td>7,935.8 (7.7)</td>
<td>15,871.5 (15.5)</td>
<td>31,743 (31.0)</td>
<td></td>
</tr>
<tr>
<td>ETERNUS DX200 S4 (Copy table size: 512MB)</td>
<td>16</td>
<td>1,819 (1.8)</td>
<td>3,639 (3.6)</td>
<td>7,279 (7.1)</td>
<td>14,559 (14.2)</td>
<td>29,119 (28.4)</td>
<td>58,238 (56.9)</td>
<td>116,476 (113.7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>963 (0.9)</td>
<td>1,926 (1.9)</td>
<td>3,853 (3.8)</td>
<td>7,706 (7.5)</td>
<td>15,412 (15.1)</td>
<td>30,824 (30.1)</td>
<td>61,648 (60.2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>495 (0.5)</td>
<td>991 (1.0)</td>
<td>1,983 (1.9)</td>
<td>3,967 (3.9)</td>
<td>7,935 (7.7)</td>
<td>15,871 (15.5)</td>
<td>31,743 (31.0)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>251 (0.2)</td>
<td>503 (0.5)</td>
<td>1,006 (1.0)</td>
<td>2,012 (2.0)</td>
<td>4,024 (3.9)</td>
<td>8,049 (7.9)</td>
<td>16,099 (15.7)</td>
<td></td>
</tr>
<tr>
<td>ETERNUS DX500 S4 (Copy table size: 1,024MB (1Tb))</td>
<td>16</td>
<td>3,640 (3.6)</td>
<td>7,280 (7.1)</td>
<td>14,561 (14.2)</td>
<td>29,123 (28.4)</td>
<td>58,246 (56.9)</td>
<td>116,492 (113.8)</td>
<td>232,984 (227.5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>927 (1.9)</td>
<td>3,854 (3.8)</td>
<td>7,708 (7.5)</td>
<td>15,416 (15.1)</td>
<td>30,832 (30.1)</td>
<td>61,664 (60.2)</td>
<td>123,329 (120.4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>992 (1.0)</td>
<td>1,984 (1.9)</td>
<td>3,969 (3.9)</td>
<td>7,939 (7.8)</td>
<td>15,879 (15.5)</td>
<td>31,759 (31.0)</td>
<td>63,518 (62.0)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>503 (0.5)</td>
<td>1,007 (1.0)</td>
<td>2,014 (2.0)</td>
<td>4,028 (3.9)</td>
<td>8,057 (7.9)</td>
<td>16,115 (15.7)</td>
<td>32,231 (31.5)</td>
<td></td>
</tr>
<tr>
<td>ETERNUS DX600 S4 (Copy table size: 4,096MB (4GB))</td>
<td>16</td>
<td>14,563 (14.2)</td>
<td>29,126 (28.4)</td>
<td>58,252 (56.9)</td>
<td>116,504 (113.8)</td>
<td>233,008 (227.5)</td>
<td>466,017 (455.1)</td>
<td>932,035 (910.2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>7,099 (7.5)</td>
<td>15,419 (15.1)</td>
<td>30,838 (30.1)</td>
<td>61,676 (60.2)</td>
<td>123,353 (120.5)</td>
<td>246,707 (240.9)</td>
<td>493,415 (481.9)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>3,971 (3.9)</td>
<td>7,942 (7.8)</td>
<td>15,885 (15.5)</td>
<td>31,771 (31.0)</td>
<td>63,542 (62.1)</td>
<td>127,084 (124.1)</td>
<td>254,168 (248.2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>2,015 (2.0)</td>
<td>4,031 (3.9)</td>
<td>8,063 (7.9)</td>
<td>16,127 (15.7)</td>
<td>32,255 (31.5)</td>
<td>64,511 (63.0)</td>
<td>129,023 (126.0)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>1,015 (1.0)</td>
<td>2,031 (2.0)</td>
<td>4,062 (4.0)</td>
<td>8,124 (7.9)</td>
<td>16,248 (15.9)</td>
<td>32,497 (31.7)</td>
<td>64,995 (63.5)</td>
<td></td>
</tr>
<tr>
<td>ETERNUS DX100 S3 (Copy table size: 512MB)</td>
<td>16</td>
<td>1,819 (1.8)</td>
<td>3,639 (3.6)</td>
<td>7,279 (7.1)</td>
<td>14,559 (14.2)</td>
<td>29,119 (28.4)</td>
<td>58,238 (56.9)</td>
<td>116,476 (113.7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>963.3 (0.9)</td>
<td>1,926.5 (1.9)</td>
<td>3,853.1 (3.8)</td>
<td>7,706.1 (7.5)</td>
<td>15,412.2 (15.1)</td>
<td>30,824.5 (30.1)</td>
<td>61,648.9 (60.2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>496 (0.5)</td>
<td>992 (1.0)</td>
<td>1,983.9 (1.9)</td>
<td>3,967.9 (3.9)</td>
<td>7,935.8 (7.7)</td>
<td>15,871.5 (15.5)</td>
<td>31,743 (31.0)</td>
<td></td>
</tr>
</tbody>
</table>
## B. Snapshot Configurable NAS Volume Capacity (Guideline)

<table>
<thead>
<tr>
<th>ETERNUS DX</th>
<th>Number of snapshot generations</th>
<th>Resolution x1</th>
<th>x2</th>
<th>x4</th>
<th>x8</th>
<th>x16</th>
<th>x32</th>
<th>x64</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETERNUS DX200 S3 (Copy table size: 512MB)</td>
<td>16</td>
<td>1,819 (1.8)</td>
<td>3,639 (3.6)</td>
<td>7,279 (7.1)</td>
<td>14,559 (14.2)</td>
<td>29,119 (28.4)</td>
<td>58,238 (56.9)</td>
<td>116,476 (113.7)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>963 (0.9)</td>
<td>1,926 (1.9)</td>
<td>3,853 (3.8)</td>
<td>7,706 (7.5)</td>
<td>15,412 (15.1)</td>
<td>30,824 (30.1)</td>
<td>61,648 (60.2)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>495 (0.5)</td>
<td>991 (1.0)</td>
<td>1,983 (1.9)</td>
<td>3,967 (3.9)</td>
<td>7,935 (7.7)</td>
<td>15,871 (15.5)</td>
<td>31,743 (31.0)</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>251 (0.2)</td>
<td>503 (0.5)</td>
<td>1,006 (1.0)</td>
<td>2,012 (2.0)</td>
<td>4,024 (3.9)</td>
<td>8,049 (7.9)</td>
<td>16,099 (15.7)</td>
</tr>
<tr>
<td>ETERNUS DX500 S3 (Copy table size: 1,024MB (1GB))</td>
<td>16</td>
<td>3,640 (3.6)</td>
<td>7,280 (7.1)</td>
<td>14,561 (14.2)</td>
<td>29,123 (28.4)</td>
<td>58,246 (56.9)</td>
<td>116,492 (113.8)</td>
<td>232,984 (227.5)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>1,927 (1.9)</td>
<td>3,854 (3.8)</td>
<td>7,708 (7.5)</td>
<td>15,416 (15.1)</td>
<td>30,832 (30.1)</td>
<td>61,664 (60.2)</td>
<td>123,329 (120.4)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>992 (1.0)</td>
<td>1,984 (1.9)</td>
<td>3,969 (3.9)</td>
<td>7,939 (7.8)</td>
<td>15,879 (15.5)</td>
<td>31,759 (31.0)</td>
<td>63,518 (62.0)</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>503 (0.5)</td>
<td>1,007 (1.0)</td>
<td>2,014 (2.0)</td>
<td>4,028 (3.9)</td>
<td>8,057 (7.9)</td>
<td>16,115 (15.7)</td>
<td>32,231 (31.5)</td>
</tr>
<tr>
<td>ETERNUS DX600 S3 (Copy table size: 4,096MB (4GB))</td>
<td>16</td>
<td>14,563 (14.2)</td>
<td>29,126 (28.4)</td>
<td>58,252 (56.9)</td>
<td>116,504 (113.8)</td>
<td>233,008 (227.5)</td>
<td>466,017 (455.1)</td>
<td>932,035 (910.2)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>7,709 (7.5)</td>
<td>15,419 (15.1)</td>
<td>30,838 (30.1)</td>
<td>61,676 (60.2)</td>
<td>123,353 (120.5)</td>
<td>246,707 (240.9)</td>
<td>493,415 (481.9)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>3,971 (3.9)</td>
<td>7,942 (7.8)</td>
<td>15,885 (15.5)</td>
<td>31,771 (31.0)</td>
<td>63,542 (62.1)</td>
<td>127,084 (124.1)</td>
<td>254,168 (248.2)</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>2,015 (2.0)</td>
<td>4,031 (3.9)</td>
<td>8,063 (7.9)</td>
<td>16,127 (15.7)</td>
<td>32,255 (31.5)</td>
<td>64,511 (63.0)</td>
<td>129,023 (126.0)</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>1,015 (1.0)</td>
<td>2,031 (2.0)</td>
<td>4,062 (4.0)</td>
<td>8,124 (7.9)</td>
<td>16,248 (15.9)</td>
<td>32,497 (31.7)</td>
<td>64,995 (63.5)</td>
</tr>
</tbody>
</table>

Unit: GB (rounded down to the nearest whole number), the contents of the parentheses are TB.
When a Secondary Backup Is Performed Using a Backup between ETERNUS DX Storage Systems (REC)

The values in the table are calculated based on the requirements when the following copies are set for the NAS user volume.

- Requirements described in "● When a Backup Is Performed Using QuickOPC with OPC Restoration" (page 178) and requirements when a secondary backup is performed using a backup between ETERNUS DX storage systems (REC).

Figure 27 Operational Configuration (When a Secondary Backup Is Performed Using a Backup between ETERNUS DX Storage Systems (REC))

*1: A NAS user volume is not required when the ETERNUS DX (on the backup side) does not conduct NAS operations.

Table 24 Guidelines for Snapshot Configurable NAS Volume Capacity (When QuickOPC and REC Are Used)

<table>
<thead>
<tr>
<th>ETERNUS DX</th>
<th>Number of snapshot generations</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>x1</td>
</tr>
<tr>
<td>ETERNUS DX100 S3 (Copy table size: 512MB)</td>
<td>16</td>
<td>1,724 (1.7)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>935 (0.9)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>488 (0.5)</td>
</tr>
<tr>
<td>ETERNUS DX200 S4 (Copy table size: 512MB)</td>
<td>16</td>
<td>1,724 (1.7)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>935 (0.9)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>488 (0.5)</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>249 (0.2)</td>
</tr>
<tr>
<td>ETERNUS DX</td>
<td>Number of snapshot generations</td>
<td>Resolution</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>x1</td>
<td>x2</td>
</tr>
<tr>
<td>ETERNUS DX500 S4 (Copy table size: 1,024MB (1GB))</td>
<td>16</td>
<td>3,448 (3.4)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>1,871 (1.8)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>977 (1.0)</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>499 (0.5)</td>
</tr>
<tr>
<td>ETERNUS DX600 S4 (Copy table size: 4,096MB (4GB))</td>
<td>16</td>
<td>13,796 (13.5)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>7,489 (7.3)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>3,912 (3.8)</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>2,000 (2.0)</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>1,011 (1.0)</td>
</tr>
<tr>
<td>ETERNUS DX200 S3 (Copy table size: 512MB)</td>
<td>16</td>
<td>1,724 (1.7)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>935 (0.9)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>488 (0.5)</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>249 (0.2)</td>
</tr>
<tr>
<td>ETERNUS DX500 S3 (Copy table size: 1,024MB (1GB))</td>
<td>16</td>
<td>3,448 (3.4)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>1,871 (1.8)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>977 (1.0)</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>499 (0.5)</td>
</tr>
<tr>
<td>ETERNUS DX600 S3 (Copy table size: 4,096MB (4GB))</td>
<td>16</td>
<td>13,796 (13.5)</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>7,489 (7.3)</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>3,912 (3.8)</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>2,000 (2.0)</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>1,011 (1.0)</td>
</tr>
</tbody>
</table>
Unit: GB (rounded down to the nearest whole number), the contents of the parentheses are TB.
## C. Audit Log Messages

This appendix explains the audit log messages that are notified when audit logs are used in the NAS environment.

### Audit Log Format

An audit log consists of information, such as the date and user name, that is separated using a pipe "|". The output format, the details of each item, and an output example of audit log messages are shown below. The number under each underline indicates an item in the table below.

<table>
<thead>
<tr>
<th>date</th>
<th>message-id</th>
<th>message-status</th>
<th>user-name</th>
<th>syscall</th>
<th>syscall-result</th>
<th>file-id</th>
<th>mode</th>
<th>dir/file1</th>
<th>dir/file2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 25 Details of Each Item in Audit Log Messages

<table>
<thead>
<tr>
<th>Number</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>date</td>
<td>Date and time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access date and time</td>
</tr>
<tr>
<td>2</td>
<td>message-id</td>
<td>Sequential ID that is given to each syscall access</td>
</tr>
<tr>
<td>3</td>
<td>message-status</td>
<td>A 6-digit number that indicates the validity of the logs 001110</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The validity of the logs are indicated by the first digit. &quot;0&quot;: valid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number other than &quot;0&quot;: invalid</td>
</tr>
<tr>
<td>4</td>
<td>user-name</td>
<td>Access user name</td>
</tr>
<tr>
<td>5</td>
<td>syscall</td>
<td>open,openat,creat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The data and property in the files are accessed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>utimensat,utime,utimes,futimesat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The time of a file is updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>setxattr,lsetxattr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The attributes of files are updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unlink,unlinkat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The files are deleted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mkdir,mkdirat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The directories are created.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rmdir</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The directories are deleted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rename,renameat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The files and directories are renamed or moved.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dir/file1: names of directory/file before renaming and moving</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dir/file2: names of directory/file after renaming and moving</td>
</tr>
<tr>
<td>6</td>
<td>syscall-result</td>
<td>Syscall result (ok, fail)</td>
</tr>
<tr>
<td>7</td>
<td>file-id</td>
<td>File ID</td>
</tr>
<tr>
<td>8</td>
<td>mode</td>
<td>Whether the target is a directory or file (dir, file)</td>
</tr>
<tr>
<td>9</td>
<td>dir/file1</td>
<td>Directory name or file name of the target</td>
</tr>
<tr>
<td>10</td>
<td>dir/file2</td>
<td>Directory name or file name of the target (only for rename/renameat)</td>
</tr>
</tbody>
</table>
The details that are displayed in "syscall" are shown below.

**Table 26 Details That Are Displayed in "syscall"**

<table>
<thead>
<tr>
<th>Operation</th>
<th>syscall</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opening files</td>
<td>open</td>
<td>-</td>
</tr>
<tr>
<td>Copying files to client PCs</td>
<td>open</td>
<td>-</td>
</tr>
<tr>
<td>Copying directories to client PCs</td>
<td>-</td>
<td>No audit log</td>
</tr>
<tr>
<td>Creating files</td>
<td>setxattr</td>
<td>-</td>
</tr>
<tr>
<td>Overwriting files</td>
<td>open, utimensat</td>
<td>-</td>
</tr>
<tr>
<td>Copying files from client PCs</td>
<td>setxattr, open, utimensat</td>
<td>-</td>
</tr>
<tr>
<td>Creating directories</td>
<td>mkdir, setxattr</td>
<td>-</td>
</tr>
<tr>
<td>Copying directories from client PCs</td>
<td>mkdir, setxattr, utimensat</td>
<td>-</td>
</tr>
<tr>
<td>Deleting files</td>
<td>unlink</td>
<td>-</td>
</tr>
<tr>
<td>Deleting directories</td>
<td>rmdir</td>
<td>-</td>
</tr>
<tr>
<td>Renaming files</td>
<td>rename, setxattr</td>
<td>Same as moving files</td>
</tr>
<tr>
<td>Renaming directories</td>
<td>rename</td>
<td>Same as moving files</td>
</tr>
<tr>
<td>Moving files</td>
<td>rename, setxattr</td>
<td>Same as renaming files</td>
</tr>
<tr>
<td>Moving directories</td>
<td>rename</td>
<td>Same as renaming files</td>
</tr>
<tr>
<td>Referencing the properties of the file</td>
<td>open</td>
<td>-</td>
</tr>
<tr>
<td>Changing the file permissions</td>
<td>open, setxattr</td>
<td>-</td>
</tr>
<tr>
<td>Deleting the properties of the file</td>
<td>open, setxattr</td>
<td>-</td>
</tr>
<tr>
<td>Changing the directory permissions</td>
<td>setxattr</td>
<td>-</td>
</tr>
</tbody>
</table>

● Output Example of the Audit Log Messages

```
2015-05-19 15:49:58.111|9839|001110|user-name|setxattr|ok|2102268|dir/file.txt
```
Output Examples of the Audit Logs

- **xxx.txt Is Opened with a Text Editor**
  
  2015-07-31 11:59:16.396|2|001110|audittest2|open|ok|30|file|xxx.txt

- **xxx.txt Is Copied to the Client PC**
  
  2015-07-31 17:33:43.151|13|001110|audittest2|open|ok|31|file|fld1/xxx.txt

- **xxx.txt Is Created with a Text Editor**
  
  
  
  2015-07-31 17:48:52.544|22|001110|audittest2|setxattr|ok|36|file|xxx.txt

- **The File Is Saved with the Text Editor**
  
  2015-08-03 11:39:14.207|11|001110|audittest2|open|ok|39|file|fld1/file1.txt
  
  2015-08-03 11:39:18.727|12|001110|audittest2|open|ok|39|file|fld1/file1.txt
  
  2015-08-03 11:39:18.727|13|001110|audittest2|utimensat|ok|39|file|fld1/file1.txt

- **The File Is Copied from the Client PC**
  
  2015-08-03 11:43:16.757|14|001110|audittest2|setxattr|ok|40|file|fld1/file2.txt
  
  2015-08-03 11:43:16.757|15|001110|audittest2|open|ok|40|file|fld1/file2.txt
  
  2015-08-03 11:43:16.767|16|001110|audittest2|utimensat|ok|40|file|fld1/file2.txt
  
  2015-08-03 11:43:16.767|17|001110|audittest2|utimensat|ok|40|file|fld1/file2.txt
  
  2015-08-03 11:43:16.767|18|001110|audittest2|utimensat|ok|40|file|fld1/file2.txt

- **The Directory Is Moved to a Different Directory**
  
  2015-08-03 14:51:27.348|510048|004440|audittest2|rename|ok|44|dir|dirl|dir2/dirl
C. Audit Log Messages

Output Examples of the Audit Logs

- **The File Properties Are Referenced**

```
2015-08-03 15:56:46.298|510051|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 15:56:46.328|510052|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 15:56:46.338|510053|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 15:56:46.458|510054|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 15:56:46.718|510055|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 15:56:46.718|510056|001110|audittest2|open|ok|48|file|dir2/file1.txt
```

- **The File Permissions Are Changed**

```
2015-08-03 16:11:10.708|510080|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 16:11:10.728|510081|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 16:11:10.748|510082|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 16:11:10.748|510083|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 16:11:10.768|510084|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 16:11:10.778|510085|001110|audittest2|open|ok|48|file|dir2/file1.txt
2015-08-03 16:11:26.808|510086|001110|audittest2|setxattr|ok|48|file|dir2/file1.txt
2015-08-03 16:11:26.808|510087|001110|root|setxattr|ok|48|file|dir2/file1.txt
```

- **The Directory Permissions Are Changed**

```
2015-08-04 11:17:39.159|28|001110|audittest2|setxattr|ok|51|dir|dir3
2015-08-04 11:17:39.159|29|001110|audittest2|setxattr|ok|51|dir|dir3
```

- **The Directories Are Renamed**

```
2015-08-04 20:01:03.122|1002|004440|audittest2|rename|ok|28|dir|dir1|dir01
```
D. Notes for Data Migrations

This appendix provides notes for data migrations to a NAS volume in the ETERNUS DX.

Actions to Take Before Data Migrations

Check that the data to be migrated meets the specifications of the ETERNUS DX NAS file system. If some of the data does not meet the specifications, take the actions listed in the following table before the migration.

Table 27 Actions to Take Before Data Migrations

<table>
<thead>
<tr>
<th>Categories</th>
<th>Item</th>
<th>What to check</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Character set</td>
<td>Does the file name include characters encoded with non-UTF-8 character sets? (*1)</td>
<td>Change the character set of the file name to UTF-8.</td>
</tr>
<tr>
<td></td>
<td>File name</td>
<td>Is there a file with the name &quot;.streams&quot; included in the data?</td>
<td>Change the file name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For details, refer to cautions in &quot;Displaying/Hiding Alternate Data Streams&quot; (page 43).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Characters in the file name</td>
<td>Does the file that will be shared by the Windows OS have a file name without any of the following characters? &quot;&quot; (double quotation mark), * (asterisk), / (slash), : (colon), &lt;, &gt;, ?, ,</td>
<td>Change the file name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(*1)</td>
</tr>
<tr>
<td>File name length</td>
<td></td>
<td>Is the length of the file name 255 bytes or less? (*1)</td>
<td>Change the file name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory</td>
<td>Directory name</td>
<td>Is there a directory with the name &quot;.streams&quot; included in the data?</td>
<td>Change the directory name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For details, refer to cautions in &quot;Displaying/Hiding Alternate Data Streams&quot; (page 43).</td>
<td></td>
</tr>
<tr>
<td>Security setting</td>
<td></td>
<td>Is [Read permissions] enabled for the directories that are shared by the Windows OS? (*2)</td>
<td>Enable [Read permissions].</td>
</tr>
<tr>
<td>Data to be migrated</td>
<td>Amount of data</td>
<td>Does the value stay below the maximum value of the file system? (*3)</td>
<td>If the value exceeds the maximum value, migrate the data into multiple, separate NAS volumes. (*4)</td>
</tr>
<tr>
<td></td>
<td>Number of directories and files</td>
<td></td>
<td>If the value exceeds the maximum value, migrate the data into multiple, separate NAS volumes.</td>
</tr>
<tr>
<td></td>
<td>Number of subdirectories per directory</td>
<td></td>
<td>If the value exceeds the maximum value, change the directory layout.</td>
</tr>
<tr>
<td></td>
<td>Number of ACL entries</td>
<td></td>
<td>If the value exceeds the maximum value, reduce the number of ACL settings to below the maximum value.</td>
</tr>
<tr>
<td></td>
<td>Existence of special files</td>
<td>Does the data include files not listed below?</td>
<td>Change the data structure to exclude those files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• File</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Directory</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Symbolic link</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hard link</td>
<td></td>
</tr>
</tbody>
</table>
### Property Information of the Files that are Migrated from the Windows OS

Due to differences in the file system specifications, the inheritable property information differs from that of the Windows OS. For details on the inheritable property information, refer to the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Inheritance possibility</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Owner</td>
<td>○</td>
<td>If Active Directory is used, allow SIDs to be resolved.</td>
</tr>
<tr>
<td></td>
<td>×</td>
<td>The owner is set to the user who copied the file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation date and time</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td>Modification date and time</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td>Access date and time</td>
<td>×</td>
<td>The migrated day and time are set.</td>
</tr>
<tr>
<td>Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbolic link</td>
<td>×</td>
<td>The file is copied but the link cannot be migrated.</td>
</tr>
<tr>
<td>Hard link</td>
<td>×</td>
<td>The file is copied but the link cannot be migrated.</td>
</tr>
<tr>
<td>Shortcut</td>
<td>×</td>
<td>The shortcut can be migrated but the link information must be modified accordingly.</td>
</tr>
<tr>
<td>Junction</td>
<td>×</td>
<td>The file is copied but the junction cannot be migrated.</td>
</tr>
</tbody>
</table>
### Notes for Data Migrations

**Property Information of the Files that are Migrated from the Windows OS**

<table>
<thead>
<tr>
<th>Item</th>
<th>Inheritance possibility</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Security (ACL)</td>
<td>If Active Directory is used, allow SIDs to be resolved. If local user authentication is used, the security information (ACL) cannot be migrated. The migratable well-known SIDs are the only ones that are supported in the ETERNUS DX. For details, refer to &quot;Access Control (ACL Function)&quot; (page 36). If a file is copied without migrating the security information, the owner is set to the user who copied the file.</td>
</tr>
<tr>
<td>File attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read-only</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Hidden</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Directory</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Archive</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Compress</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Encrypt</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Offline</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Scrubbing</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>×</td>
<td></td>
</tr>
</tbody>
</table>

○: Possible, ×: Not possible
E. Firmware Release Information

This appendix provides firmware modification information, such as information on functions that have been added or modified.

The firmware version that is currently in use can be checked via ETERNUS Web GUI or ETERNUS CLI.

Table 29 Release Information List

<table>
<thead>
<tr>
<th>Firmware version</th>
<th>Release date</th>
<th>Detail of functional modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>V10L14</td>
<td>February 2014</td>
<td>• Support for the NAS function</td>
</tr>
<tr>
<td>V10L16</td>
<td>April 2014</td>
<td>• Support for concurrent CIFS/NFS operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Setting functions of NAS server name and DNS server (for ETERNUS CLI)</td>
</tr>
<tr>
<td>V10L21</td>
<td>August 2014</td>
<td>• Quota function (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Snapshot function</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support NAS volume capacity expansion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Increased the number of NAS volumes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Setting functions of Jumbo Frame and network transfer rate (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VLAN function (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bonding function (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Modified the NAS setting functions (for ETERNUS Web GUI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Display function of the NAS environment setting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Rename function of the NAS server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Setting function of the DNS server</td>
</tr>
<tr>
<td>V10L31</td>
<td>February 2015</td>
<td>• Virus scan function</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for SMB3.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for file system block size of 8KB/32KB</td>
</tr>
<tr>
<td>V10L33</td>
<td>June 2015</td>
<td>• Firewall function (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Modified the NAS setting functions (for ETERNUS Web GUI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Quota settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Changed the log output level while operating CIFS (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Increased the number of snapshot generations for NAS volumes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Expanded the maximum NAS volume capacity (block size: 8KB/32KB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Changed the maximum number of NAS volumes (for the ETERNUS DX200 S3) (*1)</td>
</tr>
<tr>
<td>V10L51</td>
<td>December 2015</td>
<td>• NAS data deletion function (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Packet trace acquisition function (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Audit log function (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FTP/FXP function</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NAS system volume deletion function (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for NFSv4.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for access permissions for specific group or user to CIFS shared folder</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for the use of Japanese for the CIFS shared folder name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for the Active Directory's trust relationships</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quota management of shared folders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SMB protocol change function (for ETERNUS CLI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for ETERNUS vCenter Plug-in 3.0.0</td>
</tr>
</tbody>
</table>

---

191

FUJITSU Storage ETERNUS DX S4/S3 series Hybrid Storage Systems Configuration Guide (NAS)
Copyright 2019 FUJITSU LIMITED

P3AM-8072-19ENZ0
## Firmware Release Information

<table>
<thead>
<tr>
<th>Firmware version</th>
<th>Release date</th>
<th>Detail of functional modification</th>
</tr>
</thead>
</table>
| V10L53           | June 2016    | • Changed the maximum number of NAS volumes (for the ETERNUS DX100 S3) (*2)  
|                  |              | • Increased the number of snapshot generations for NAS volumes (for the ETERNUS DX100 S3) (*2)  
|                  |              | • Support for the "no_root_squash" setting for NFS shared folders (for ETERNUS CLI)  
|                  |              | • Local user authentication  
|                  |              | • Home directories  
|                  |              | • Meta cache distribution (for ETERNUS CLI)  |
| V10L61           | December 2016| • Deleted the virus scan function |
| V10L71           | April 2017   | • Support for the ETERNUS DX100 S4/DX200 S4 |
| V10L81           | November 2017| • Support for the ETERNUS DX500 S4/DX600 S4 |
| V10L83           | July 2018    | • Expanded the number of characters that can be specified for the volume name (32 characters)  
|                  |              | • Improved the specification method for the NAS volume snapshot name |
| V10L85           | November 2018| • No change in the NAS functions (support for the Smart Setup Wizard to configure SAN environments) |
| V10L87 (*3)      | April 2019   | • No change in the NAS functions (support for Veeam Storage Integration for SAN environments) |

*1: When the Memory Extension (ETFMCB / ETFMCB-L / ETDMCBU / ETDMCBU-L) is installed  
*2: When the Memory Extension (ETFMCC / ETFMCC-L / ETDMCCU / ETDMCCU-L) is installed  
*3: Applicable to the ETERNUS DX100 S4/DX200 S4 and the ETERNUS DX500 S4/DX600 S4 only
• The content of this manual is subject to change without notice.

• This manual was prepared with the utmost attention to detail. However, Fujitsu shall assume no responsibility for any operational problems as the result of errors, omissions, or the use of information in this manual.

• Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.

• The content of this manual may not be reproduced or distributed in part or in its entirety without prior permission from Fujitsu.