Dell EMC Unity™ Family

Version 5.x

Configuring SMB File Sharing

H16899

REV 04

DELL EMC

Published June 2019

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

CONTENTS

Additional resources

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

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

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

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

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

Special notice conventions used in this document

DANGER

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

WARNING

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

CAUTION

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

NOTICE

Addresses practices not related to personal injury.

Note

Presents information that is important, but not hazard-related.

PART 1

Basic Functionality

CHAPTER 1

Overview

Unity SMB support

All Unity releases support SMB 1 through SMB 3.02, which supports enhancements such as Continuous Availability, Offload Copy, Protocol Encryption, Multichannel, and Shared VHDX Support. Some of these features, such Multichannel and Shared VHDX Support, do not require any special configuration on the Unity system. For Multichannel, if there are multiple interfaces created on multiple ports, the SMB 3 protocol automatically uses all available TCP connections for a single SMB session. Shared VHDX support provides the ability to enable Virtual Hard Disk sharing on Hyper-V to share a virtual disk between multiple nodes.

Starting with Unity OE version 4.2, SMB 3.1.1 is also supported, which adds reliability enhancements for Continuous Availability (CA) for Hyper-V Cluster Client Failover (CCF), and improved security and encryption traffic performance. The SMB version used depends on the client operating system.

SMB support is enabled on the NAS server level during or after creation, allowing you to create SMB-enabled file systems on that NAS Server. When enabling SMB support on a NAS server, the server can either be standalone or Active Directory domain-joined. Domain- joined NAS servers are placed in the OU=Computers, OU=EMC NAS Servers organizational unit by default.

Unity also supports the Microsoft Distributed File System (DFS) Namespace, which provides the ability to present shares from multiple file systems through a single mapped share. You can configure a Unity SMB server as a standalone DFS root node or as a leaf node on an Active Directory DFS root.

Note

DFS Replication (DFS-R) is not supported by Unity systems. If replication is required, the native asynchronous replication feature can be used to replicate the file system instead.

SMB file systems and shares have the following additional advanced protocol options. All of these options, except for Oplocks Enabled, are disabled by default.

Protocol option	Level
Sync Writes Enabled	File system
Oplocks Enabled	File system
Notify on Write Enabled	File system
Notify on Access Enabled	File system
Continuous Availability	Share
Protocol Encryption	Share
Access-Based Enumeration	Share
Branch Cache Enabled	Share
Offline Availability	Share

Unisphere storage provisioning

Storage provisioning is the process of allocating available drive capacity to meet the capacity, performance, and availability requirements of hosts and applications. When you provision storage with Unisphere, you create storage resources to which hosts and applications can connect in order to access storage.

When you provision a storage resource in Unisphere, the system uses thin provisioning by default. This type of provisioning can improve storage efficiency while reducing the time and effort required for monitoring and rebalancing existing pool resources. Organizations can purchase less storage capacity up front, and increase available drive capacity (by adding drives) on an on-demand basis, and according to actual storage usage, instead of basing drive requirements in the requests or predictions of connected hosts. Thin provisioning allows multiple storage resources to subscribe to common storage capacity within a pool, while the system allocates only a portion of the physical capacity requested by each storage resource. The remaining storage is available for other storage resources to use.

Note

All storage resources require some amount of metadata from the pools where the storage resources were provisioned.

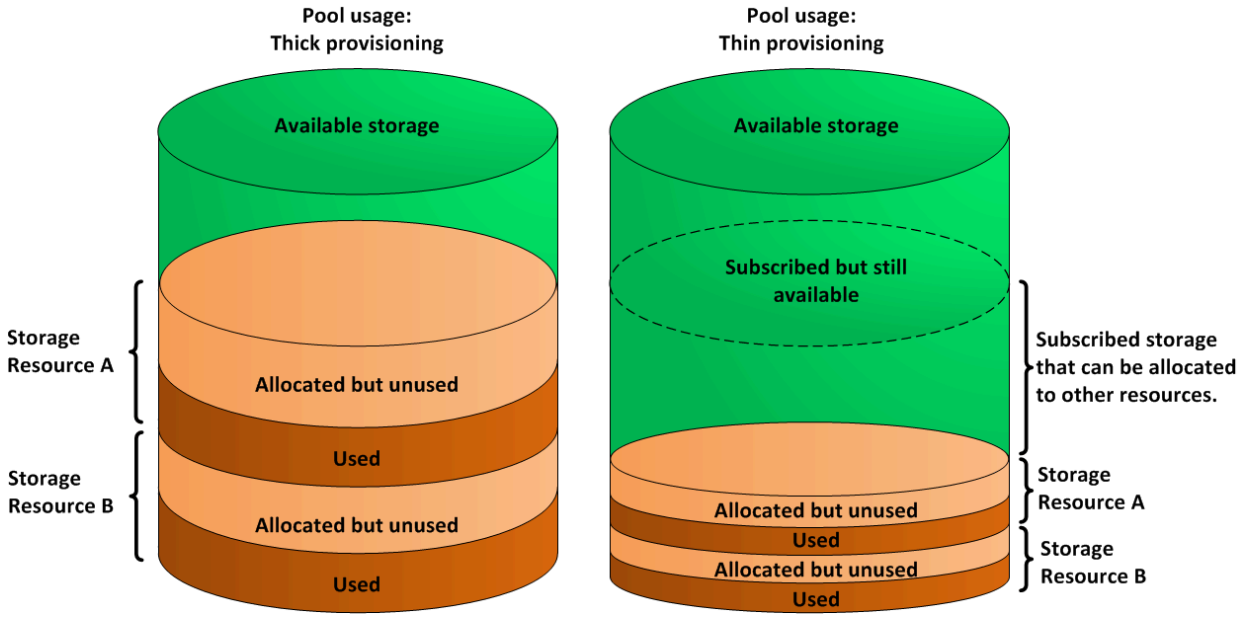
Thick and thin provisioning

The following table describes the differences between thick and thin provisioning:

Table 1 Differences between thick and thin provisioning

Provisioning type	Description
Thick provisioning	The amount of storage requested for a storage resource is exclusively allocated for it. This storage is reserved, and the unused portion cannot be used or distributed among other storage resources associated with the same pool.
Thin provisioning	The amount of storage requested for a storage resource is not immediately allocated for it. Instead, the system allocates an initial quantity of storage to the storage resource. When the amount of storage consumed within the storage resource approaches the limit of the current allocation, the system allocates additional storage to the storage resource from the pool. Thin provisioning is required for data reduction.

Figure 1 Difference between thick and thin provisioning



Creating a thin storage resource

When you create a thin storage resource, you specify a target size for the resource. The size represents the maximum capacity to which the storage resource can grow without being increased by an administrator. The system reserves only a portion of the requested size, called the initial allocation. The requested size of the storage resource represents a subscribed quantity. Additional storage is allocated on-demand.

When a host or application uses approximately 75% of its initial allocation, an additional incremental quantity of storage is automatically allocated to the storage resource. The incremental allocation process continues until the quantity of storage allocated for the storage resource reaches the limit determined by its target size.

Note

A storage resource may appear full when data copied or written to the storage resource is greater than the space available at that time. When this occurs, the system begins to automatically extend the storage space and accommodate the write operation. As long as there is enough extension space available, this operation will complete successfully.

Pool subscription levels

Because storage resources can subscribe to more storage than is actually available to them, pools can be over-provisioned to support more storage capacity than they actually possess. The system automatically generates notification messages when total pool usage reaches 85% of the pool's physical capacity. (You can customize this threshold.)

Thin provisioning best practices

The following general rules can help determine the best environments in which to use thin provisioning:

- Thin provisioning provides the benefit of space efficiency. It is recommended that you choose thin provisioning for a storage resource (selected by default), unless absolute and predictable performance is a higher requirement than space efficiency. In some workload environments, performance can actually improve with thin provisioning.
- Environments that can benefit from thin provisioning include:
  - Document repositories with rapidly rising capacity requirements. These repositories can benefit greatly from the improved capacity utilization offered by thin provisioning, provided their environments meet the previously outlined criteria.
  - Software development and source code repositories. These repositories are well-suited to thin provisioning, because their environments can usually tolerate some level of performance variability.
- Thin provisioning works best in file system environments where files are not frequently deleted. Many file systems do not efficiently reuse the space associated with deleted files, which can result in an allocated but unused space in the thin-provisioned file system.
- Consider the space consumption characteristics of databases before using thin provisioning. Some databases pre-allocate the storage space for data before writing to it. This space is allocated within a thin-provisioned storage resource, and this can reduce the capacity utilization within the pool. For more information, consult your database vendor documentation.

Advantages of thin and standard provisioning

Thin provisioning provides the following advantages:

- Provides the most efficient allocation of storage capacity based on usage.
- Promotes ease of use in setting up and managing pool capacity.
- Minimizes the host impact of adding pool resources based on host storage usage.
- Optimizes storage usage in situations where space consumption is difficult to forecast.

Planning considerations

The following table summarizes the tasks to perform in a Windows Server environment before you start configuring SMB on your Unity system. For more information on performing these tasks, see the Unity online help and the Windows Server documentation.

1. Configure one or more DNS servers.
2. If you are joining the NAS server to the Active Directory (AD), configure at least one NTP server on the storage system to synchronize the date and time. It is recommended that you set up a minimum of two NTP servers per domain to avoid a single point of failure.
3. Create a domain account in Active Directory.
4. Optionally configure VLANs and tenants if you plan to implement multi-tenancy.

Related features and functionality information

Specific information related to the features and functionality described in this document is included in the following for Unity:

- Unisphere Online Help
- *Configuring Hosts to Access SMB File Systems*
- *Configuring Replication*
- *Unisphere Command Line Interface User Guide*
- *Service Commands Technical Notes*

The complete set of customer publications is available on the Online Support website at http://Support.EMC.com. After logging in to the website, click the **Support by Product** page, to locate information for the specific feature required.

CHAPTER 2

Configuring NAS servers

Overview of configuring NAS servers

Before you can provision SMB file storage on the storage system, a NAS server that is appropriate for managing SMB must be running on the system. A NAS server is a file server that uses the SMB protocol, NFS protocol, or both to share data with network hosts. It also catalogs, organizes, and optimizes read and write operations to the associated file systems.

Configuring a NAS server requires specifying the following information:

- SP that the NAS server will run on.
- Pool used to store the NAS server's configuration data, such as anti-virus configurations, NDMP settings, network Interfaces, and IP addresses.
- IP addresses that will be assigned to the NAS server to allow network hosts to access the shared data.

You can balance the performance load on the storage system's SPs by choosing which NAS servers run on each SP, and which file systems are associated with which NAS server. For example, if you plan to provide file systems for two high-load database applications, you can choose to run a separate NAS server on each SP, and provision the storage for each application from a separate NAS server. This balances system performance by ensuring that the applications draw their processing resources from separate SPs.

Create a NAS server for Windows-only file sharing (SMB)

Before you begin

Obtain the following information:

- (Optional) Name of the tenant to associate with the NAS server.
- Name of the pool to store the NAS server's metadata.
- Storage Processor (SP) on which the NAS server will run.
- IP address information for the NAS server.
- VLAN ID, if the switch port supports VLAN tagging. If you associate a tenant with the NAS server, you must choose a VLAN ID.
- If you are configuring a standalone NAS server, obtain the NetBIOS name, and workgroup, and define what will be used for the standalone SMB server's local administrator account.
- If you are joining the NAS server to the Active Directory (AD), configure NTP on the storage system. Then obtain the SMB computer name (used to access SMB shares), Windows domain name, and the username and password of a domain administrator or a user who has a sufficient domain access level to join the AD. You can optionally specify the NetBIOS name and organizational unit. The NetBIOS name defaults to the first 15 characters of the SMB server name. The organizational unit defaults to OU=Computers,OU=EMC NAS servers.
- DNS server information (optional for a standalone NAS server).
- Replication information (optional).

It is recommended that you balance the number of NAS servers on both SPs.

Procedure

1. Under **Storage**, select **File** > **NAS Servers**.
2. Select the **Add** icon.
3. On the **General** and **Interface** pages, specify the relevant settings. Note the following:
   - On the **General** page, the **Server name** identifies the NAS server. It is not a network name.
   - Optionally select a tenant to associate with the NAS server.

     Note

     Once you create a NAS server that has an associated tenant, you cannot change this association.

   - On the **Interface** page, optionally select a VLAN. If you selected a tenant on the **General** page, you must select a VLAN. The list of VLANs represent the VLANs associated with the selected tenant.
4. On the **Sharing Protocols** page:
   - Select **Windows Shares (SMB, CIFS)**. Then select **Standalone** to create a standalone SMB server, or select **Join to the Active Directory domain** to create a domain member SMB server.
   - If you join the NAS server to the AD, optionally click **Advanced** to change the default NetBios name and organizational unit.
5. On the **DNS** page, configure DNS for the NAS server. This step is mandatory when joining to an AD domain, but optional for a standalone NAS server.
6. On the **Replication** page, optionally select a replication mode and Recovery Point Objective (RPO) for the NAS server.

Configure NAS server sharing protocols and FTP/SFTP settings

You can configure SMB support when you create a NAS server or change its properties. You can configure FTP/SFTP support for an existing NAS server only.

If you are creating a NAS server, access the NAS server sharing protocol options from the **Sharing Protocols** window in the **Create a NAS server** wizard.

If you are changing NAS server properties, follow these steps to access the NAS server sharing protocol and FTP options:

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

SMB support

If you are changing NAS server properties, select the **SMB** sub-tab on the **Sharing Protocols** tab.

Task	Description
Enable or disable the NAS server's ability to serve files using the SMB protocol.	Select or clear the **Enable Windows shares (SMB, CIFS Server)** option. You cannot disable this option if multiprotocol sharing mode is enabled.
Configure SMB without Active Directory (AD) support.	Select **Standalone** and specify the requested information.
Configure SMB with AD support.	1. Select **Join to the Active Directory domain**. 2. Specify the requested information. 3. Optionally, click **Show Advanced** to change the default NetBios name and organizational unit.

FTP/SFTP support

You can configure FTP or FTP over SSH (SFTP) settings for an existing NAS server only. Select the **FTP** sub-tab on the **Sharing Protocols** tab.

Task	Description
Enable or disable the NAS server's ability to share files using the FTP protocol.	Select or clear **Enable FTP**. If this option is selected, optionally click the other options to customize user authentication, user home directory, and message settings.
Enable or disable the NAS server's ability to share files using the SFTP protocol.	Select or clear **Enable SFTP**. If this option is selected, optionally click the other options to customize user authentication, user home directory, and message settings.

FTP access can be authenticated using the same methods as SMB. Once authentication is complete, access is the same as SMB for security and permission purposes. If the format is `domain@user` or `domain\user`, SMB authentication is used. SMB authentication uses the Windows Domain Controller.

To use local files for FTP access, the `passwd` file must include an encrypted password for the users. This password is used for FTP access only. The `passwd` file uses the same format and syntax as a standard Unix system, so you can leverage this to generate the local `passwd` file. On a Unix system, use `useradd` to add a new user and `passwd` to set the password for that user. Then, copy the hashed password from the `/etc/shadow` file, add it to the second field in the `/etc/passwd` file, and upload the `/etc/passwd` file to the NAS server.

Change NAS server properties

When changing NAS server properties, note that you cannot disable DNS for NAS servers that support SMB file sharing and that are joined to an Active Directory (AD).

Procedure

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

3. On the **General** tab:
   - Change the NAS server name.
   - Select **SP Owner** to transition from one SP to the other SP for this NAS server. For example, you may want to do this if you have an overloaded SP, and want to reduce the load by moving the server to the other SP.
4. On the **Network** tab:
   - Select the **Interfaces & Routes** sub-tab to add, change, delete, or verify NAS server interfaces, enable or disable IP packet reflect for the NAS server, or change the NAS server's preferred interfaces. Select an interface, and then select **Show external routes for interfaces** to access the per-interface routing table, where you can add, change, or delete the selected interface's routes for responding to client requests.
   - Select the **Routes to External Services** sub-tab to add, change, or verify NAS server routes for external service requests, or to configure default gateways.
5. On the **Naming Services** tab, configure DNS and either configure the UNIX Directory Service (UDS) for the NAS server (LDAP or NIS) or use local files. Alternatively, you can use local files with a UDS. In this case, the system checks the local files first.
6. On the **Sharing Protocols** tab:
   - Select the **SMB** sub-tab to enable or disable support for Windows shares and to change SMB properties.
   - Select the **FTP** sub-tab to enable or disable FTP or SFTP, or to change FTP or SFTP properties.
7. On the **Protection & Events** tab:
   - Select the **NDMP Backup** sub-tab to enable or disable NDMP, and to change the NDMP password.
   - Select the **DHSM** sub-tab to enable or disable Distributed Hierarchical Storage Management (DHSM) and to change the DHSM password.
   - Select the **Events Publishing** sub-tab to enable or disable Events Publishing, create or modify an event pool, and create or modify events policy settings.
8. On the **Security** tab, select the **Antivirus** sub-tab to enable or disable the antivirus service and to retrieve or upload the antivirus configuration file.
9. On the **Replication** tab, optionally select a replication mode and Recovery Point Objective (RPO) for the NAS server.

View the active LDAPS CA certificate for a NAS server

This option is available for anonymous and simple LDAP authentication that uses SSL and enforces certification.

Procedure

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

3. Select the **Naming Services** tab, and then select the **LDAP/NIS** sub-tab.
4. Click **Retrieve CA Certificate**.

Upload an LDAPS CA certificate for a NAS server

Procedure

1. Under **Storage**, select **File** > **NAS Servers**.
2. Select the relevant NAS server, and click the **Edit** icon.
3. On the **Naming Services** tab, select the **LDAP/NIS** sub-tab.
4. Select **LDAP Secure (Use SSL)** and **Enforce Certification Authority (CA) Certificate**, if these options are not already selected. These options are available for Anonymous and Simple authentication.
5. Select **Upload CA Certificate**, locate the certificate to upload, locate the certificate, and click **Start Upload**.

NDMP settings

The Network Data Management Protocol (NDMP) provides a standard for backing up file servers on a network. NDMP allows centralized applications to back up file servers running on various platforms and platform versions. NDMP reduces network congestion by isolating control path traffic from data path traffic, which permits centrally managed and monitored local backup operations. Enabling NDMP for file system storage resources makes it possible to use third party NDMP products to back up and restore file system data.

You can enable NDMP by configuring NAS server settings.

Understanding Common AntiVirus Agent (CAVA)

Common AntiVirus Agent (CAVA) provides an antivirus solution to clients using a NAS server. It uses an industry-standard SMB protocol in a Microsoft Windows Server environment. CAVA uses third-party antivirus software to identify and eliminate known viruses before they infect files on the storage system.

Why is antivirus important?

The storage system is resistant to the invasion of viruses because of its architecture. The NAS server runs data access in real-time using an embedded operating system. Third parties are unable to run programs containing viruses on this operating system. Although the operating system software is resistant to viruses, Windows clients that access the storage system require virus protection. Virus protection on clients reduces the chance that they will store an infected file on the server, and protects them if they open an infected file. This antivirus solution consists of a combination of the operating system software, CAVA agent, and a third-party antivirus engine. The CAVA software and a third-party antivirus engine must be installed on a Windows Server in the domain.

For additional information about CAVA, which is part of Common Event Enabler (CEE), refer to *Using the Common Event Enabler on Windows Platforms* on Online Support.

CHAPTER 3

Configuring file systems

Create a file system

Before you begin

Make sure there is a NAS server configured to support the SMB protocol, and that a pool exists with enough available storage space.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the **Add** icon.
3. On the **Protocol** window, select **Windows Shares (SMB)**. Then select the associated NAS server.
4. Optionally click **Advanced** to select advanced SMB settings.
5. Continue following the steps in the wizard while noting the following:
   - On the **Storage** page, the **Thin** checkbox is selected by default. If you do not want to create a thin file system, remove the checkmark from the **Thin** checkbox. Removing the checkmark also disables the **Data Reduction** option.
   - On the **Storage** page, select the **Data Reduction** checkbox to enable data reduction on the file system. Data reduction is applied on all new incoming writes. Data that already exists on the file system does not have data reduction applied. Data reduction can be enabled only on thin file systems that reside in All-Flash pools, and only for thin file systems created on Unity systems running OE version 4.2.x or later.
   - On the **Shares** page, optionally, configure the initial share for the file system.
   - You can configure a snapshot schedule for the file system when you create the file system, or you can do this at a later time.

Advanced SMB file system settings

You can set these advanced settings when you change the configuration of an existing SMB-enabled or multiprotocol-enabled file system.

Setting	Description
Sync Writes Enabled	When you enable the synchronous writes option for a Windows (SMB) or multiprotocol file system, the storage system performs immediate synchronous writes for storage operations, regardless of how the SMB protocol performs write operations. Enabling synchronous writes operations allow you to store and access database files (for example, MySQL) on storage system SMB shares. This option guarantees that any write to the share is done synchronously and reduces the chances of data loss or file corruption in various failure scenarios, for example, loss of power. This option is disabled by default.

Setting	Description
	Note The synchronous writes option can have a big impact on performance. It is not recommended unless you intend to use Windows file systems to provide storage for database applications.
Oplocks Enabled	(Enabled by default) Opportunistic file locks (oplocks) allow SMB clients to buffer file data locally before sending it to a server. SMB clients can then work with files locally and periodically communicate changes to the storage system rather than having to communicate every operation over the network to the storage system. This feature is enabled by default for Windows (SMB) and multiprotocol file systems. Unless your application handles critical data or has specific requirements that make this mode or operation unfeasible, leaving the oplocks enabled is recommended. The following oplocks implementations are supported: • Level II oplocks, which informs a client that multiple clients are currently accessing a file, but no client has yet modified it. A level II oplock lets the client perform read operations and file attribute fetches by using cached or read-ahead local information. All other file access requests must be sent to the server. • Exclusive oplocks, which informs a client that it is the only client opening the file. An exclusive oplock lets a client perform all file operations by using cached or read-ahead information until it closes the file, at which time the server must be updated with any changes made to the state of the file (contents and attributes). • Batch oplocks, which informs a client that it is the only client opening the file. A batch oplock lets a client perform all file operations by using cached or read-ahead information (including opens and closes). The server can keep a file opened for a client even though the local process on the client machine has closed the file. This mechanism curtails the amount of network traffic by letting clients skip the extraneous close and open requests.
Notify on Write Enabled	Enable notification when a file system is written to. This option is disabled by default.
Notify on Access Enabled	Enable notification when a file system is accessed. This option is disabled by default.
Enable SMB Events publishing	Enable the processing of SMB events for this file system.

Change file system properties

If the associated NAS server is a replication destination, many configuration options cannot be changed.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the relevant file system, and then select the **Edit** icon.
3. On the **General** tab:
   - You can change the description of the file system and the file system size.
   - You can view the file system capacity, including used space and free space, on this tab.
   - If a thin file system was created on a Unity system running OE version 4.1, you can also change the minimum allocation size. You cannot reduce the storage size lower than the current allocation.
   - You can enable data reduction for thin file systems created on a Unity system running OE version 4.2.x or later. As data reduction is applied to all new incoming writes to a file system, data reduction statistics (such as data reduction ratio) display on the Properties page.
     If data reduction is enabled and then subsequently disabled, existing data in the file system will remain as is, but newly-written data will not have data reduction applied.
   - If data reduction is enabled, you can also enable Advanced Deduplication, which provides the ability to reduce the amount of data storage needed by eliminating redundant data from the system. Once enabled, all incoming writes to the system will have advanced deduplication applied.
     Advanced deduplication is available only on:
     - Dynamic or Traditional pools in Unity 380F, 480F, 680F, and 880F systems
     - Dynamic pools in Unity All-Flash 450F, 550F, and 650F systems
     - All-Flash pools in Unity Hybrid 380, 480, 680, and 880 systems
   - You can change capacity alarm threshold settings for when Info, Warning, and Error alert messages are generated.
4. On the **Snapshots** tab, manage the file system's snapshots or configure a snapshot schedule for the file system.
5. On the **FAST VP** tab, change the file system tiering policy and view the data distribution per tier.
6. On the **Advanced** tab, optionally do any of the following:
   - Change the advanced SMB properties of a file system.
   - Enable Events Publishing for a file system.
7. On the **Quota** tab, configure or change settings for file system quotas and quota trees.
8. On the **Replication** tab, configure or change the file system replication settings.

   Note

   Replication can be set on the file-system level only if the replication session already exists for the NAS server where the file system resides.

9. On the **FLR** tab (FLR-enabled file systems only), optionally modify the retention periods, enable auto-lock of new files, set an auto-lock policy interval, or enable automatic deletion of files once the retention period expires.

Note

If the file system is a replication destination, FLR properties cannot be modified.

About Events Publishing

Events Publishing allows third-party applications to register to receive event notification and context from the storage system when accessing file systems by using the SMB protocol. The Events Publishing agent delivers to the application both event notification and associated context in one message. Context may consist of file metadata or directory metadata that is needed to decide business policy.

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

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

Table 2 Event descriptions

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

Create Events Publishing notifications

Before you begin

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

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

Procedure

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

About automatic file system shrink and extend

The system automatically shrinks and extends a thin file system based on capacity needs.

Thin-provisioned file systems are automatically extended or shrunk by the system when certain conditions are met. Automatic extend prevents the file system from running out of space. Automatic shrink improves space allocation by releasing any unused space back to the storage pool. The automatic shrink and automatic extend operations are based on a high water mark (HWM) for auto-extend and a low water mark (LWM) for auto-shrink.

For file systems smaller than 2.5 tebibytes (TiB) in size:

- The file system is automatically extended when the used space exceeds and sustains over 75% of the allocated space. This is the fixed high water mark (HWM) for file systems less than 2.5 TiBs.
- The file system automatically shrinks and returns space to the pool when the used space is 70% less than the allocated space. This is the fixed low water mark (LWM) for file systems less than 2.5 TiBs.

For file systems larger than 2.5 TiBs in size, the high and low watermarks will be dynamic and operate based on the following:

- Auto-extend will wait until nearly all of the allocated space capacity is used before extending file systems larger than 2.5 TiBs.

- Auto-shrink will not require a large amount of capacity to be freed back to the pool as part of the shrink operation.

For larger file systems greater than 2.5 TiBs, the maximum extend size is 1 TiB. This helps avoid over-allocation of space from the pool to that file system that may not be immediately used.

You can set a minimum allocated size for a thin file system; automatic and manual shrink operations will not be able to reduce the size of the file system below this minimum. The default minimum allocated size for a thin file system is 3G.

About manual file storage resource shrink and extend

You can manually extend or shrink file systems.

File resource shrink

The shrink operation reduces the space the file resource uses from the pool, allowing the pool to reclaim the free, unused space from the target file resource.

For thick-provisioned file resources, you can shrink the size of the resource and return unused space to the pool. For example, if a thick file system is shrunk from a size of 1 TB down to 500 GB:

- The amount of used space for the resource remains the same.
- The free space for the resource is reduced by 500 GB.
- The total pool free space is increased by slightly less than 500 GB.
- The pool size used for the resource is reduced to approximately 500 GB.

The system displays a message indicating exactly how much space will be reclaimed by the pool as a result of the shrink operation.

For thin-provisioned file resources, you can manually shrink the size of a file resource to a size that is equal to or less than the allocated size.

Note

For Unity systems running OE version 4.1.x, the minimum size of a thin storage resource is 3 GB. You cannot shrink a thin file resource below the size used. For Unity systems running OE version 4.2 or later, the thin file storage resource minimum allocated size option is not supported.

File resource extend

The manual extend operation does the following for thin- and thick-provisioned file resources:

- For thin-provisioned file resources, increases the visible (virtual) size of the resource without increasing the actual size allocated to the resource from the pool.
- For thick-provisioned file resources, increases the actual space allocated to the resource from the pool.

Note

You cannot extend a thick file resource beyond the total pool free size.

Manually shrink or extend the size of a file storage resource

The ability to manually shrink or extend the size of a storage resource applies to file systems. A manual shrink allows the pool to reclaim space, while a manual extend allocates more space to the storage resource.

Note

You can cancel a manual shrink operation, but the progress made prior to cancellation will not be reverted.

Procedure

1. Select a storage resource, and then click the **Edit** icon.
2. In the **Size** field, enter the new reduced (shrink) or increased (extend) size of the storage resource.

   Note

   For Unity systems running OE version 4.1.x, the minimum size of a storage resource is 3 GB. You cannot shrink below the size used or extend beyond the total pool free size.

CHAPTER 4

Configuring file system shares

Share local paths and export paths

The following table describes the path settings for shares:

Setting	Description
Local path	The path to the file system storage resource on the storage system. This path specifies the unique location of the share on the storage system. **SMB shares** • An SMB file system allows you to create multiple shares with the same local path. In these cases, you can specify different host-side access controls for different users, but the shares within the file system will all access common content. • A directory must exist before you can create shares on it. Therefore, if you want the SMB shares within the same file system to access different content, you must first create a directory on the Windows host that is mapped to the file system. Then, you can create corresponding shares using Unisphere. You can also create and manage SMB shares from the Microsoft Management Console.
Export path	The path used by the host to connect to the share. Unisphere creates the share export path based on the name of the share and the name of the file system where it resides. Hosts use either the file name or the export path to mount or map to the share from a network host.

Create an SMB share

Before you begin

The file system or snapshot you choose as the share's source must be associated with a NAS server that supports the SMB protocol.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the relevant file system, and then select **More Actions** > **Create an SMB share (CIFS)**.
3. On the **File System** page, specify whether the share is for the selected file system or for a snapshot of the selected file system.
4. On the **General** page, enter the relevant information, noting the following:
   - The value specified in the **Share Name** field, along with the NAS server name, constitutes the name by which hosts access the share.
   - Share names must be unique at the NAS server level per protocol.
   - **Local Path** must correspond to an existing folder name within the file system that was created from the host-side.

5. On the **Advanced** page, optionally configure advanced settings for the share.

After you finish

Once you create a share, you can modify it using the Microsoft Management Console. For information, see *Configuring Hosts to Access SMB File Systems*, which is available on the support website.

Advanced SMB share properties

You can configure the following advanced SMB share properties when you create an SMB share or change its properties:

Option	Description
Continuous Availability	Gives host applications transparent, continuous access to a share following a failover of the NAS server on the system (with the NAS server internal state saved or restored during the failover process). **Note** Enable continuous availability for a share only when you want to use Microsoft Server Message Block (SMB) 3.0 protocol clients with the specific share.
Protocol Encryption	Enables SMB encryption of the network traffic through the share. SMB encryption is supported by SMB 3.0 clients and above. By default, access is denied if an SMB 2 client attempts to access a share with protocol encryption enabled. You can control this by configuring the RejectUnencryptedAccess registry key on the NAS Server. 1 (default) rejects non-encrypted access and 0 allows clients that do not support encryption to access the file system without encryption.
Access-Based Enumeration	Filters the list of available files and directories on the share to include only those to which the requesting user has read access. **Note** Administrators can always list all files.
Branch Cache Enabled	Copies content from the share and caches it at branch offices. This allows client computers at branch offices to access the content locally rather than over the WAN. BranchCache is managed from Microsoft hosts.
Distributed File System (DFS)	(Read only) Lets you group files located on different shares by transparently connecting them to one or more DFS namespaces. This simplifies the process of moving data from one share to another. This option is read only in Unisphere because you manage DFS from Microsoft hosts. For information, see the MIcrosoft Distributed File System documentation.
Offline Availability	Configures the client-side caching of offline files:

Option	Description
	• **Manual**: Files are cached and available offline only when caching is explicitly requested. • **Programs and files opened by users**: All files that clients open from the share are automatically cached and available offline. Clients open these files from the share when they are connected to it. This option is recommended for files with shared work. • **Programs and files opened by users, optimize for performance**: All files that clients open from the share are automatically cached and available offline. Clients open these files from the share's local cache, if possible, even when they are connected to the network. This option is recommended for executable programs. • **None**: Client-side caching of offline files is not configured.

Change SMB share properties

Procedure

1. Under **Storage**, select **File** > **SMB Shares**.
2. Select the relevant share, and then click the **Edit** icon.
3. On the **General** tab, change the share description.
4. On the **Advanced** tab configure advanced SMB properties.

CHAPTER 5

Performance metrics for SMB

View historical performance metrics

Procedure

1. Under **System**, select **Performance**.
2. Select the historical metrics dashboard for the system for which you created a performance metrics display.
3. For each system dashboard, you can define the time range of the values displayed for all the metric line charts on that dashboard. The default time range is **Last 1 hour**. Alternatively, select one of the other time range values.

   The time range selections are enabled only if Unisphere has data spanning that time range.
4. For a custom time range, select **Custom** and choose the start and end dates and times of the charts displayed. Click **OK**.
5. To drill down into the data displayed in the line chart, you can breakdown the data displayed into individual lines that show the categories and contributors that provide data to the performance metric. Choose among the breakdown categories available for a particular metric.

   Each contributor displays as a different color line in the chart and is identified in the legend. You can quickly remove and add each contributor by clicking on its name in the legend. Use the breakdown display to determine if one contributor is adding to the aggregated total more than another contributor as well as analyze how a contributor's activity increases or decreases at a particular time.
6. Hover over a data point in the chart to display the date, time, and measurement associated with that data point. Gaps in metric data collection are displayed as gaps in the line chart.
7. For object-level line charts, such as those for LUNS, file systems, drives, and so forth, you can select **Percentage View** to view the data points as percentage values instead of absolute values.

View real-time performance metrics

Procedure

1. Under **System**, select **Performance**.
2. Select the real-time metrics dashboard for the system for which you created a performance metrics display.
3. Hover over a data point in the chart to display the date, time, and measurement associated with that data point. Gaps in metric data collection are displayed as gaps in the line chart.
4. For object-level line charts, such as those for LUNS, file systems, drives, and so forth, you can select **Percentage View** to view the data points as percentage values instead of absolute values.

File System Client Bandwidth

Total amount of file system client I/O requests, in KB/s, for the selected file systems.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following category:

This category...	Groups or filters data by the...
Read/Write	Traffic types: read I/O and write I/O.

File System Client Response Time

Average time spent completing file system client I/O requests, in microseconds, for the selected file systems.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following category:

This category...	Groups or filters data by the...
Read/Write	Traffic types: read I/O and write I/O.

File System Client I/O Size

Average size of file system client I/O requests, in KB, for the selected file systems.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following category:

This category...	Groups or filters data by the...
Read/Write	Traffic types: read I/O and write I/O.

File System Client IOPS

Total number of file system client I/O requests, in I/O per second, for the selected file systems.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following category:

This category...	Groups or filters data by the...
Read/Write	Traffic types: read I/O and write I/O.

System - Client File System Bandwidth

Total amount of file system client I/O requests, in KB/s, across all file systems in the storage system.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

System - Client File System Response Time

Average time spent completing file system client I/O requests, in microseconds, across file systems in the storage system.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

System - Client File System I/O Size

Average size of file system client I/O requests, in KB, across all file systems in the storage system.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

System - Client File System IOPS

Total number of file system client I/O requests, in I/O per second, across all file systems in the storage system.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

System - CIFS Bandwidth

Total amount of CIFS (SMB) I/O requests, in KB/s, across all ports in the storage system.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

System - CIFS I/O Size

Average size of CIFS (SMB) I/O requests, in KB, across all ports in the storage system. Calculated as a weighted average, which gives more weight to the SP with the highest number of CIFS I/O requests.

Breakdown and filter categories
The aggregated data can be broken down by or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

System - CIFS IOPS

Total number of CIFS (SMB) I/O requests, in I/O per second, across all ports in the storage system.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

System - CIFS Response Time

Average time spent completing CIFS I/O requests, in microseconds, across all file systems in the storage system. Calculated as a weighted average, which gives more weight to the file systems with the highest number of I/O requests.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

File System Bandwidth

Total amount of internal I/O requests, in KB/s, for the selected file systems.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following category:

This category...	Groups or filters data by the...
Read/Write	Traffic types: read I/O and write I/O.

File System I/O Size

Average size of internal I/O requests, in KB, for the selected file systems.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following category:

This category...	Groups or filters data by the...
Read/Write	Traffic types: read I/O and write I/O.

File System IOPS

Total number of internal I/O requests, in I/O per second, for the selected file systems.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following category:

This category...	Groups or filters data by the...
Read/Write	Traffic types: read I/O and write I/O.

System - File System Bandwidth

Total amount of internal I/O requests, in KB/s, across all file systems in the storage system.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

System - File System I/O Size

Average size of internal I/O requests, in KB, across all file systems in the storage system.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

System - File System IOPS

Total number of internal I/O requests, in I/O per second, across all file systems in the storage system.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following categories:

This category...	Groups or filters data by the...
Storage Processor	SPs that processed the network traffic.
Read/Write	Traffic types: read I/O and write I/O.

Tenant Bandwidth

Total amount of I/O requests, in KB/s, for the selected tenant.

Breakdown and filter categories
The aggregated data can be broken down or filtered by the following category:

This category...	Groups or filters data by the...
Read/Write	Traffic types: read I/O and write I/O.

PART 2

Advanced functionality

CHAPTER 6

Managing quotas

About file system quotas

You can track and limit drive space consumption by configuring quotas for file systems at the file system or directory level. You can enable or disable quotas at any time, but it is recommended that you enable or disable them during non-peak production hours to avoid impacting file system operations.

Note

You cannot create quotas for read-only file systems.

Quota configurations

The storage system supports three types of quota configurations:

Quota configuration	Description
User quota on a file system	Limits the amount of storage consumed by an individual user storing data on the file system.
Quota on a directory (called a quota tree once a quota is applied)	Limits the total amount of storage consumed on the directory. You can use quota trees to: • Set storage limits on a project basis. For example, you can establish quota trees for a project directory that has multiple users sharing and creating files in it. • Track directory usage by setting the tree quota's hard and soft limits to 0 (zero). **Note** If you change the limits for a quota tree, the changes take effect immediately, without disrupting file system operations.
User quota on a quota tree	Limits the amount of storage consumed by an individual user storing data on the quota tree.

Soft and hard limits

A quota can have a soft limit, hard limit, or both.

- A soft limit is a preferred limit on storage usage. The system issues a warning when a soft limit is reached.
  You can set a grace period for a file system or a quota tree, which counts down time once the soft limit is met. If the grace period expires, users cannot write to the file system or quota tree until more space becomes available, even if the hard limit has not been met.

  Note

  If you update the grace period value, the new value affects only the quota or quotas which will exceed the soft limit after the update is performed. Any existing quotas which have been counting down using the older grace period value will not be affected.

- A hard limit is an absolute limit on storage usage.

If a hard limit is reached for a user quota on a file system or quota tree, the user will not be able to write data to the file system or tree until more space becomes available. If a hard limit is reached for a quota tree, no user will be able to write data to the tree until more space becomes available.

Recommended approach for configuring quotas

It is recommended that you configure quotas before the storage system becomes active in a production environment, and that you follow this basic procedure:

1. Create a file system.
2. Determine which quota policy best suits the file system's environment, and select that policy. The default policy is File Size, which calculates drive usage in terms of logical file sizes, and ignores the size of directories and symbolic links.
3. Enable the enforcement of user quotas at the file system level, and define default limits for those quotas. If default limits are not specified, the system sets no drive usage limits for users, unless explicit user limits are defined for each individual user. Set default quotas in an environment where you want the same set of limits applied to many users.
4. Specify the grace period for which users of the file system can remain over the soft limit before it becomes the hard limit.

   Note

   If you update the grace period value, the new value affects only the quota or quotas which will exceed the soft limit after the update is performed. Any existing quotas which have been counting down using the older grace period value will not be affected.

5. Define explicit quotas for individual users at the file-system level, if the environment requires this type of usage-control granularity. The explicit quotas you define supersede the default quota definitions.
6. Create quota trees for each directory or subdirectory for which you want to have quotas.
7. For each quota tree, optionally change the default limits for users at the quota tree level. These limits are inherited from file system settings when a quota trees is created. If default limits are not set, the quotas feature sets no drive usage limits for quota tree users, unless explicit user limits are defined for each individual user. Set default limits in an environment where you want the same set of limits applied to many users.
8. For each quota tree, define explicit quotas for users if the environment requires this type of individual-usage-control granularity.

Quota policies

Before enabling and defining quotas, ensure that the file system is configured to use the quota policy that best suits the client environment:

- File Size policy (default): Calculates drive usage in terms of logical file sizes, and ignores the size of directories and symbolic links. Use this policy where file sizes are critical to quotas, such as where user usage is based on the size of the files created, and exceeding the size limit is unacceptable.

Note

It is recommended that you use this policy for SMB file systems.

- Blocks policy: Calculates drive usage in terms of file system blocks (8 KB units), and includes drive usage by directories and symbolic links in the calculations. With this policy, any operation resulting in allocating or removing blocks, such as creating, expanding, or deleting a directory; writing or deleting files; or creating or deleting symbolic links changes block usage. Block usage depends solely on the number of bytes added to or removed from the file.

Note

When using the Blocks policy, a user can create a sparse file whose size is larger than the file size, but that uses fewer blocks on the drive.

If the grace period is set to 0, warnings will be generated when soft quotas are reached, the client will not get quota exceeded errors until the hard limit is exceeded. If the use of default soft quotas is required, set the specific grace periods you desire, or keep the default grace period of one week.

Note

If you update a grace period value, the new value affects only the quota or quotas which will exceed the soft limit after the update is performed. Any existing quotas which have been counting down using the older grace period value will not be affected.

Enable or disable the enforcement of user quotas on a quota tree

Enabling or disabling the enforcement of user quotas on a quota tree impacts system performance, but does not disrupt file system operations. It is recommended that you perform these operations only during non-peak production hours. Once user quota enforcement is enabled, you can change quota settings without impacting performance.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the file system, and then select the **Edit** icon.
3. On the **Quota** tab, select the **Quota Tree** sub-tab.
4. Do either of the following:
   - To enforce user quotas, locate the quota tree, and select the **No** link in the **Enforce User Quotas** column. Then select **Enforce User Quotas**.
   - To disable the enforcement of user quotas, locate the quota tree, and select the **Yes** link in the **Enforce User Quotas** column. Then clear **Enforce User Quotas**.

Enable or disable the enforcement of user quotas on a file system

Enabling or disabling the enforcement of user quotas on a file system impacts system performance, but does not disrupt file system operations. It is recommended that you perform these operations only during non-peak production hours. Once user quota enforcement is enabled, you can change quota settings without impacting performance.

Note

When you enable user quotas, you can also set default user quota limits and a default grace period. Explicit user quotas will override these defaults.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the file system, and then select the **Edit** icon.
3. On the **Quota** tab, select the **File System** sub-tab.
4. Select **Manage Quota Settings**.
5. Select or clear **Enforce User Quotas**.
6. If you are enabling user quotas, optionally do the following:
   - Change the quota policy for the file system.
   - Change the default quota limits and grace period. These limits apply to all file system users who do not have explicit user quotas defined. A value of 0 indicates no limit.

Create a user quota on a file system

Create a user quota on a file system to limit or track the amount of storage space that individual users consume on that file system. When you create or modify user quotas, you have the option to use default hard and soft limits that are set at the file-system level.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the file system, and then select the **Edit** icon.
3. On the **Quota** tab, select the **File System** sub-tab.
4. Select the **Add** icon.
5. In the **Create User Quota** wizard, select the **Add** icon, and then provide the requested information. To track space consumption without setting limits, set **Soft Limit** and **Hard Limit** to 0, which indicates no limit.

Create a quota tree on a file system

Create a quota tree at the directory level of a file system to limit or track the total storage space consumed for that directory.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the file system, and then select the **Edit** icon.
3. On the **Quota** tab, select the **Quota Tree** sub-tab.
4. Select the **Add** icon.
5. Follow the steps in the wizard. To track space consumption without setting limits, set the **Soft Limit** and **Hard Limit** fields to 0, which indicates no limit.

Create a user quota on a quota tree

Create a user quota on a quota tree to limit or track the amount of storage space that individual users consume on that tree. When you create user quotas, you have the option to use the default hard and soft limits that are set at the quota-tree level.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the file system, and then select the **Edit** icon.
3. On the **Quota** tab, select the **Quota Tree** sub-tab.
4. Select the quota tree, and then select the **Edit** icon.
5. On the **User Quotas** tab, be sure that **Enforce User Quotas** is selected, and provide the limits information. To track space consumption without setting limits, set the **Soft Limit** and **Hard Limit** fields to 0, which indicates no limit.

View file system storage space usage by user

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the file system, and then click the **Edit** icon.
3. Select the **Quota** tab to view the User Quota Report.

View quota tree storage space usage

You can view total quota tree storage space usage or quota tree space usage by user.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the file system, and then click the **Edit** icon.
3. On the **Quota** tab, select the **Quota Tree** sub-tab.

   The system displays the total storage space usage by quota tree.
4. To view quota tree storage space usage by user, select the quota tree, select the **Edit** icon, and then select the **User Quotas** tab.

Change quota properties for a file system

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the relevant file system, and then select the **Edit** icon.
3. On the **Quota** tab, select the **File System** sub-tab.
4. Change the limit settings for a user quota by selecting the quota and then selecting the **Edit** icon.
5. Select **Manage Quota Settings**, and do any of the following:
   - Change the quota policy for the file system.
   - Enforce user quotas on the file system.
   - Change the default soft limit, hard limit, and grace period for new user quotas on the file system. You can change these values for individual user quotas when you create them or when you modify their properties.

   Note

   If you update the grace period value, the new value affects only the quota or quotas which will exceed the soft limit after the update is performed. Any existing quotas which have been counting down using the older grace period value will not be affected.

Change properties for a quota tree

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the relevant file system, and then select the **Edit** icon.
3. On the **Quota** tab, select the **Quota Tree** sub-tab.
4. Select the relevant quota tree, and then select the **Edit** icon.
5. On the **General** tab, do any of the following:
   - Select **Use Default Limits** to keep the file system's default limits and grace period on the quota tree.
   - Clear **Use Default Limits** to override the file system's default limits and grace period.
   - Change the hard limit, soft limit, and grace period settings for the quota tree.

   Note

   If you update the grace period value, the new value affects only the quota or quotas which will exceed the soft limit after the update is performed. Any existing quotas which have been counting down using the older grace period value will not be affected.
6. On the **User Quotas** tab, do any of the following:

- Select or clear **Enforce User Quotas** to enable or disable the enforcement of user quotas on the quota tree.
  These actions impact system performance, but do not disrupt file system operations. It is recommended that you perform these operations only during non-peak production hours. You can change other quota settings without impacting performance.
- If you enable the enforcement of user quotas on the quota tree, you can specify the soft and hard limits for those quotas. (You can override these values when you create individual quotas.)
- Create a new user quota on the quota tree.
- Edit properties for existing user quotas.

Change the quota policy for a file system

Changing the quota policy for a file system can impact system performance, because it causes a system rescan. Therefore, it is recommended that you perform this action during off-peak hours.

Procedure

1. Under **Storage**, select **File** > **File Systems**.
2. Select the file system, and then select the **Edit** icon.
3. On the **Quota** tab, select **Manage Quota Settings**.
4. Change the quota policy, as desired.

CHAPTER 7

Configuring IP routes

About NAS server routing

You configure the IP interfaces and routing settings independently for each NAS server.

Configuring routes for responding to client requests
There are two ways to configure the routes for responding to client requests:

- Configure routing with IP packet reflect enabled.
- Configure routing with IP packet reflect disabled.

Every outbound packet sent in response to a client request always exits thorough the same interface that the inbound request used. This does not depends on IP packet reflect settings.

When IP packet reflect is enabled, you do not have to configure routing to clients that connect to the storage system, because the reply packets are sent back to the host or router where the packets came from. IP packet reflect is disabled by default.

Note

Requests that originate from the Unity system cannot leverage IP packet reflect, so you may still need to configure routing for external services, such as DNS and LDAP, when IP packet reflect is enabled.

When IP packet reflect is disabled, each NAS server interface uses static routing for directing packets to their destinations. To configure routes for responding to client requests, use the per-interface routing table, which is located by selecting **Show external routes for interfaces** on the **Network** tab of the NAS server properties page. You can add, modify, and delete routes in this table. Each route in the routing table directs a packet from the NAS server interface to which the route is linked.

Note

With static routing, the system does not check the link status or router availability. IP reflect, however, provides a return response that uses the request path of the client, without regard to the servers default or statically configured routes. If there is a router failure, replacement, or IP change, IP packet reflect supports the correct routing without interrupting the client connection.

Configuring routes to external services
In most cases, the NAS server interfaces are configured with a default gateway, which is used to route requests from a NAS server's interface to external services. You can add or view the default gateway for each NAS server interface by accessing the **External Services Access Routes** table. To access this table, select the **Routes to External Services** sub-tab on the **Network** tab of the NAS server properties page.

You can add or view default gateways by accessing the **Manage Routes** page, which displays all routes configured for the storage system in one place. To access this page, select the **Settings** icon, and then select **Access** > **Routing**.

You can add additional routes to these tables, as you would to any standard routing table, and you can modify or delete existing routes. When you make changes to routes in one table, the changes are reflected in the other table.

In a complex environment, you may need to configure granular routes to external services. To access a server from a specific interface through a specific gateway, add

a route with the following information following to the **External Services Access Routes** table:

From: <interface_ip>
Type: host
Gateway: <gateway_ip>
Destination: <external_server_ip>
Netmask/Prefix Length: 255.255.255.0

For example, to configure resilient DNS access, the standard recommendation is to configure the NAS server with three DNS servers, with each being accessed by a different physical or virtual connection. To do this:

- Add three DNS server IP addresses to the NAS server DNS configuration.
- Configure three NAS server interfaces, with each on a different physical port and/or VLAN.
- Add three routes as shown above, with each using a different NAS server interface IP and a different DNS server IP.

To access a server located on a different subnet, add a route like the following with the following information to the **External Services Access Routes** table.

From: <interface_ip>
Type: net
Gateway: empty
Destination: < subnet number>
Netmask/Prefix Length: <length>

NAS server routing tables

The per-interface routing table specifies routes from NAS server interfaces to client hosts. The system logic for picking the route of the per-interface table follows these rules:

- The routes are chosen from the NAS server's interfaces.
- The chosen interface must be active.
- If there are multiple routes to the same destination, the route specified by the preferred interface is chosen.
- If there are multiple routes to the same destination and there is no preferred interface, the most specific route takes precedence over the other routes. The order of precedence is host, net, default, with host being the most specific

The **External Services Access Routes** table is dynamically created by merging the per-interface routing tables with preferred interface information. The system chooses the best possible routing configuration when NAS server interfaces are added, modified, or deleted, either manually or through replication changes. The system logic for picking the route of the **External Services Access Routes** table follows these rules:

- The routes are chosen from the NAS server's interfaces.
- If there are multiple routes to the same destination, the route specified by the preferred interface is chosen.
- If there are multiple routes to the same destination and there is no preferred interface, the most specific route takes precedence over the other routes. The order of precedence is host, net, default, with host being the most specific

For both routing tables, the system logic also contains algorithms for handling more complicated configurations.

NAS server interfaces

When you modify an IP interface for a NAS server, you can specify whether it:

- Is a production or backup interface.
- Is a preferred interface, which is used for outgoing communication with non-locally connected hosts.

Preferred interfaces for NAS servers

If you have multiple interfaces configured for a NAS server, the system will automatically select the interface that the default route uses for outgoing communication to external services. To change which interface is selected, you can specify preferred interface settings.

The NAS server uses preferred interfaces in the following circumstances:

- The application does not specify the source interface.
- The destination is on a remote subnet.

Note

Locally connected hosts, which are attached to the same subnets as the NAS server interfaces, are accessed by using corresponding interfaces directly, and not through the preferred interface gateways.

You can select one preferred interface for each of the following interface types:

- IPv4 interface of type Production
- IPv6 interface of type Production
- IPv4 interface of type Backup & DR Testing
- IPv6 interface of type Backup & DR Testing

When the **Preferred Interface** field is set to **Auto** (the default), the system selects the preferred interface automatically, based on how many routes the interface has and how wide the destination range is of its routes. For most user environments using **Auto** provides an optimal selection of the preferred interface.

When a NAS server initiates outbound traffic to an external service, it compiles a list of all the available network interfaces on the proper subnet and performs one of the following actions if a preferred interface of the appropriate type (IPv4 or IPv6) is in the compiled list:

- If the preferred production interface is active, the system uses the preferred production interface.
- If the preferred production interface is not active, and there is a preferred active backup interface, the system uses the preferred backup interface.
- If the preferred production interface is not active (as in the case of a NAS server failover), and there is no preferred backup interface, the system does nothing.

If a preferred interface is not in the compiled list, the underlying operating environment platform chooses the network interface.

IP Packet reflect functionality for NAS server interfaces

IP packet reflect functionality for NAS servers ensures that outbound (reply) packets always exit through the next hop gateway through which inbound (request) packets entered. Because the majority of network traffic on a NAS server (including all file system I/O) is client-initiated, the NAS server can use IP packet reflect to reply to client requests. IP packet reflect is disabled by default.

Note

Interface selection is not affected by IP packet reflect settings.

IP packet reflect provides the following advantages:

- With IP packet reflect, there is no need to determine the route for sending the reply packets.
- Improves network security. Because reply packets always go out the same next hop gateway as the request packets, request packets cannot be used to indirectly flood other LANs. In cases where two network devices exist, one connected to the Internet and the other connected to the intranet, replies to Internet requests do not appear on the intranet.
- Supports multiple subnets, with each on a different NIC. With this configuration, each subnet uses a router, and the router port for each subnet filters incoming packets, so only packets from that subnet are forwarded. Replies, therefore, must be sent through the same next hop gateway as the incoming requests. IP packet reflect satisfies this requirement.
- Helps clients that have a single IP address and multiple MAC addresses. Although unusual, this configuration creates a problem for the server if IP packet reflect is not enabled. For each IP address, the NAS server keeps only one associated MAC address in the Address Resolution Protocol (ARP) table. With IP packet reflect enabled, this problem is resolved, because the server does not need to look up the MAC address from the ARP database for the reply. Instead, the server uses the MAC address of the request to send the reply.

Manage NAS server network interfaces and default routes

Procedure

1. Under **Storage**, select **File** > **NAS Servers**.
2. Select the NAS server to modify, and select the **Edit** icon.
3. Select the **Network** tab.
4. Make the desired changes as follows:

Task	Description
Add a network interface and default route	a. In the **Network Interfaces** field, select the **Add** icon, and then select the type of IP interface to add. b. Select the port and enter the IP address for the new interface. c. Optionally enter a gateway to use for the default route.

Task	Description
	d. If the switch port supports VLAN tagging, optionally specify a VLAN ID (between 0 and 4095) for the VLAN with which the NAS server is associated. If the NAS server is associated with a tenant, you must select a VLAN ID.
Modify a network interface	a. In the **Network Interfaces** field, select the network interface to modify, and then select the **Edit** icon. b. Modify the desired values.
Specify or change the preferred network interfaces	a. Select **Change Preferred Interface**. b. Select the appropriate preferred interfaces or select **Auto**.
Remove a network interface	Select the network interface you wish to remove from the NAS Server configuration, and click the **Delete** icon. **Note** If you delete a preferred interface, the system will select a new preferred interface.

Manage NAS server routes for responding to client requests

Procedure

1. Under **Storage**, select **File** > **NAS Servers**.
2. Select the NAS server, and then select the **Edit** icon.
3. Select the **Network** tab, and then select the interfaces for which you are configuring routes.
4. Select **Show external routes for interfaces**, near the bottom of the screen.
5. To add a route, select the **Add** icon in the per-interface routing table, and then specify the relevant information.
6. To change a route, follow these steps.
   a. Select the interface in the network interfaces table.
   b. Select the route and select the **Edit** icon in the per-interface routing table.
   c. Specify the relevant information.

Manage NAS server routes for external service requests

Routes for external service requests are routes that the system uses to request external services, such as LDAP or DNS.

Procedure

1. Under **Storage**, select **File** > **NAS Servers**.
2. Select the NAS server, and then select the **Edit** icon.
3. Select the **Network** tab.
4. Select **Routes to External Services**.

5. To add a route, select the **Add** icon, and then specify the relevant information.
6. To change a route, select the route, select the **Edit** icon, and then specify the relevant information.
7. To hide default and local subnet routes from view, select **More Actions** > **Hide default and local subnet routes**.

Enable or disable IP packet reflect for a NAS server

Before you begin

You can enable or disable IP packet reflect for each NAS server. IP packet reflect is disabled for all NAS servers by default.
Before you disable IP packet reflect, make sure that the hosts are reachable through a default, network, or host route. Otherwise, some hosts may become unavailable when IP packet reflect is disabled.

Procedure

1. Under **Storage**, select **File** > **NAS Servers**.
2. Select the NAS server to modify, and select the **Edit** icon.
3. Select the **Network** tab.
4. In the **Packet Reflect** field, select the **Edit**, icon, and then select **Enabled** or **Disabled**.

Verify NAS server routes

You can verify NAS server routes using the Ping and Trace operations. You can verify routes from all system interfaces, except the management interface.

Procedure

1. Under **Storage**, select **File** > **NAS Servers**.
2. Select the NAS server, and then select the **Edit** icon.
3. Select the **Network** tab.
4. To verify routes from a specific interface:
   a. From the **Interfaces & Routes** sub-tab, select the interface, and then select **Ping/Trace**.
   b. Fill in the requested information, and select **Ping** or **Trace**.
5. To verify routes from any interface:
   a. Select the **Routes to External Services sub-tab**, and then select **Ping/Trace**.
   b. Fill in the requested information, and select **Ping** or **Trace**.

CHAPTER 8

Configuring IP multi-tenancy

About IP multi-tenancy

IP multi-tenancy provides the ability to assign isolated, file-based storage partitions to the NAS servers on a storage processor. Tenants are used to enable the cost-effective management of available resources, while at the same time ensuring that tenant visibility and management is restricted to assigned resources only.

With IP multi-tenancy, each tenant can have its own:

- IP addresses and port numbers.
- VLAN domain.
- Routing table.
- IP firewall.
- DNS server or other administrative servers to allow the tenant to have its own authentication and security validation.

IP multi-tenancy is implemented by adding a tenant to the storage system, associating a set of VLANs with the tenant, and then creating one NAS server for each of the tenant's VLANs, as needed. It is recommended that you create a separate pool for the tenant and that you associate that pool with all of the tenant's NAS servers.

Note the following about the IP multi-tenancy feature:

- There is a one-to-many relationship between tenants and NAS servers. A tenant can be associated with multiple NAS servers, but a NAS server can be associated with only one tenant.
- You can associate a NAS server with a tenant when you create the NAS server. Once you create a NAS server that is associated with a tenant, you cannot change this association. (You cannot associate this NAS server with any other tenant or remove the association with this tenant.)
- During replication, data for a tenant is transferred over the service provider's network rather than the tenant's network.
- Because multiple tenants can share the same storage system, a spike in traffic for one tenant can negatively impact the response time for other tenants.

Configuring IP multi-tenancy

To configure IP multi-tenancy, follow this process:

1. Create a storage pool for each tenant (recommended).
2. Add the tenants to the system. When you add tenants, you assign each one a non-overlapping set of VLANs.
3. Create a NAS server for each tenant. When you create a NAS server, select the tenant to associate with the NAS server, and select the tenant's pool, which will be used to store the NAS server's metadata. You can add network interface information for the tenant now or later on.

   Note

   In a network interface, each subnet must be unique for a given VLAN. Using the same subnet for different VLANs can cause connectivity issues.
4. Create the file systems and shares for each tenant.

Example

The following table shows the Unity components used for tenants T1 and T2. In this example, each tenant has two VLANs and separate NAS servers for the Engineering (eng) and Human Resources (hr) departments. Each NAS server has one file system and one share.

Table 3 Unity components for tenant T1

Pool	VLANs	NAS servers	File systems	Shares
T1_pool	900	T1_cifs_eng1	T1_cifs_eng_fs1	T1_cifs_eng_sh1
	900	T1_cifs_eng2	T1_cifs_eng_fs2	T1_cifs_eng_sh2
	901	T1_cifs_hr1	T1_cifs_hr_fs1	T1_cifs_hr_sh1
	901	T1_cifs_hr2	T1_cifs_hr_fs2	T1_cifs_hr_sh2

Table 4 Unity components for tenant T2

Pool	VLANs	NAS servers	File systems	Shares
T2_pool	902	T2_cifs_eng1	T2_cifs_eng_fs1	T2_cifs_eng_sh1
	902	T2_cifs_eng2	T2_cifs_eng_fs2	T2_cifs_eng_sh2
	903	T2_cifs_hr1	T2_cifs_hr_fs1	T2_cifs_hr_sh1
	903	T2_cifs_hr2	T2_cifs_hr_fs2	T2_cifs_hr_sh2

Add a tenant

Before you begin

Obtain the VLAN IDs to associate with the tenant.

Procedure

1. Under **Storage**, select **File** > **Tenants**.
2. Select the **Add** icon.
3. Specify the information on the **Add Tenant** window. If this is the first creation of a tenant in your environment, have the system automatically generate a UUID value for this tenant. Otherwise, for existing tenants in your environment that have a system generated UUID value, enter that UUID value manually.

Change tenant properties

Procedure

1. Under **Storage**, select **File** > **Tenants**.
2. Select the **Edit** icon.
3. Change the tenant name, and add or remove associated VLANs. You can add a VLAN ID to a tenant if:
   - The VLAN ID is not associated with an existing tenant.

- No network interfaces use the VLAN ID.

Configure file replication for a tenant

In a multi-tenancy environment, you can replicate the NAS servers, routes, and file systems for a specific tenant.
For general information about replication, see the Unity online help and *Configuring Replication*, which is available from the UnityOE Features Info Hub.

Procedure

1. Create a pool for the tenant on the destination system.
2. Add the tenant to the destination system. When you add the tenant, use the same UUID and VLANs as the tenant on the source system.
3. If you are configuring remote replication, perform the following steps to set up the remote connection. Once you set this up, the same connection can be used again for subsequent replication sessions between the same systems.
   a. Configure a mobility interface on the source and destination systems. The IP addresses of both systems should be on the same subnet.
   b. Configure a replication connection on the source system using the **Asynchronous** connection mode.
4. On the NAS server properties page, create a replication session for the NAS server associated with the file storage. When you configure this session, specify the pool you created in Step 1.

   Storage resources included in a NAS server automatically get replicated when a replication session is first configured for the NAS server. The replication session for the storage resources will inherit the same attributes as the associated replication session of the associated NAS server. For the storage resources you do not want participating in replication, you can choose to remove the associated replication sessions manually.
5. To configure automatic synchronization of the NAS server and all of its files, select **Sync** on the **Replication** tab of the source NAS server.
6. To replicate the NAS server and a specific file system, access the properties page for the source file system, and select **Sync** on the **Replication** tab.

CHAPTER 9

Troubleshooting an SMB configuration

Service commands for troubleshooting SMB issues in Unity

The following service commands are useful for troubleshooting SMB issues in Unity. For detailed information about service commands, see the *Service Commands Technical Notes*, which is available from the Unity All-Flash & Hybrid Info Hub.

Use case	Service command
Perform NAS server advanced management. This includes displaying and customizing the parameters of various NAS components, performing database maintenance, and performing network troubleshooting.	`svc_nas`
Obtain information about network connectivity to domain controllers as well as access rights, credentials, access logs, and so forth.	`svc_cifssupport`
Set up and manage the SMB file system's antivirus protection using the antivirus agent (CAVA).	`svc_cava`
Display the settings and server connection status for the Common Event Publishing Agent for a specified NAS server.	`svc_event_publishing`
Display or reset the counters for NDMP and PAX backup statistics.	`svc_pax`
View information about locks currently held for provisioned Unity storage.	`svc_lockd`
Dump the VHDX metadata (Hyper-V virtual disk files) to diagnose issues with VHDX files.	`svc_vhdx`