Preface

This preface describes who should read the *Cisco COS Filesystem Gateway Release 1.4 User Guide*, how the guide is organized, and its document conventions. It contains the following sections:

- **Audience**, page v
- **Document Organization**, page v
- **Document Conventions**, page vi
- **Related Publications**, page vii
- **Obtaining Documentation and Submitting a Service Request**, page vii

**Audience**

This guide is for networking professionals managing the Cloud Object Storage (COS) product and its Filesystem Gateway (FSGW) option. Before using this guide, you should have experience working with Linux platforms and be familiar with the concepts and terminology of Ethernet, local area networking, clustering and high-availability, and network services such as DNS and NTP.

**Document Organization**

This document contains the following chapters and appendices:

<table>
<thead>
<tr>
<th>Chapters or Appendices</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Briefly describes the FSGW product, its function, and its key features.</td>
</tr>
<tr>
<td>Deployment</td>
<td>Provides deployment prerequisites and describes the steps to install and configure the FSGW.</td>
</tr>
<tr>
<td>Operation and Routine Maintenance</td>
<td>Gives procedures for updating the FSGW configuration, checking FSGW statistics using the GUI or the CLI, performing routine maintenance, and checking logs.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Provides tips for resolving common issues during FSGW installation and operation.</td>
</tr>
<tr>
<td>Global Namespace Option</td>
<td>Describes the Global Namespace (GNS) cost option available for FSGW Release 1.4.</td>
</tr>
</tbody>
</table>
Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><em>courier</em> font</td>
<td>Terminal sessions and information the system displays appear in <em>courier</em> font.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Tip**

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

**Caution**

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Warning**

**IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of
each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Warning Statements using this symbol are provided for additional information and to comply with regulatory and customer requirements.

Related Publications

Refer to the following documents for additional information about COS FSGW:

- Release Notes for Filesystem Gateway 1.4
- Cisco Cloud Object Storage Release 3.8.1 User Guide
- Cisco Cloud Object Storage Release 3.8.1 API Guide
- Cisco Cloud Object Storage Release 3.5.1 Troubleshooting Guide
- Cisco Media Origination System Release 2.7 User Guide
- Open Source Used in Filesystem Gateway 1.4

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation. To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What’s New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.
Overview

Product Description

Cisco Filesystem Gateway (FSGW) for Cisco Cloud Object Storage (COS) is an available option for COS 3.8.1 and compatible later releases. While earlier COS releases allowed access only to object storage, the FSGW option gives COS the ability to access files using Network File System (NFS) or Common Internet File System (CIFS), the two main file systems used by network attached storage (NAS).

NFS and CIFS are the client-server file systems used by the Linux and Windows operating systems, respectively. Adding FSGW enables COS to manage storage for existing Linux or Windows NAS media libraries directly, without the need to first convert these libraries to object data. For service providers with large existing media libraries, adding FSGW greatly improves COS utility and deployment speed.

Gateway Function

NAS filesystem access does not directly allow the ability to perform the random writes and rewrites that occur routinely with object storage access. Enabling COS to access NAS files means that some logical intermediation must occur to allow the NAS filesystem to perform random writes and rewrites.

FSGW serves this intermediation (gateway) function. FSGW uses the ZFS file system to perform file integrity checks, compression, per-user and per-group quotas and reporting, and construction of virtual device pools to provide resiliency. Additionally, by associating a virtual device to a COS container, FSGW can provide secure multi-tenancy using multiple filesystem gateways and COS containers.

Feature Summary

The FSGW option adds the following features and enhancements to compatible COS releases:

- Support for ISO installation on compatible bare metal servers
- Storage throughput of up to 15 Gbps on compatible bare metal servers
- Storage throughput of 1-6 Gbps on VM servers
- Global Namespace (GNS) option for high availability and scaling
- NFS and CIFS access for varying workloads, including small files and media objects
- Multi-tenancy and security features including administration of tenants, with the administrator having rights to only configure and administer tenant storage without access to the actual storage data, and tenants only having access to their own data
- Data resiliency with options for number of copies and choice of mirroring or erasure coding (software RAID) for storage savings, and multi-site resiliency where the number of copies is less then or equal than the number of sites
- Per-user and per-group quotas and reporting
- Ability to compress filesystem data
- Integrity checks on data retrieval
- Active Directory integration
- Ability to work with anti-virus engines
Deployment

This section provides instructions for installing and configuring the software. FSGW Release 1.4 supports ISO installation directly on bare metal servers, or OVA installation on VM servers. This section describes both options.

- **Bare Metal Installation**, page 2-1
- **Installation on the FSGW VM**, page 2-5
- **Configure FSGW on the COS PAM and Tenant PAM**, page 2-8
- **Adding a Cache and Log to a Zpool (Optional)**, page 2-8

Bare Metal Installation

FSGW Release 1.4 supports two approaches to bare metal installation:

- Automated installation using the FSGW ISO image
- Manual installation on other compatible hardware using RPMs

This section includes procedures for both installation methods.

**Note**

Automated installation requires the recommended hardware described below. Manual installation is supported on other compatible hardware. See **Hardware Prerequisites**, page 2-5 for details.

Recommended Hardware

The following hardware is recommended for FSGW Release 1.4, and is required for automated installation from the ISO image:

- Cisco UCS C240 Rack Server
- 4 x 10 GB network adapters
- 264 GB RAM
- 56 virtual CPU cores
Bare Metal Installation

Note
The UCS C240 meets the requirement for 56 virtual CPU cores by having 2 CPU sockets, each with 14 physical cores and 2 threads per core available.

Automated Installation via ISO Image

Note
This procedure uses the FSGW Release 1.4 ISO image and requires the hardware configuration described in Recommended Hardware, page 2-1. If not using the recommended hardware, use the procedure described in Manual Installation via RPMs, page 2-5.

Complete the following steps for automated installation:

Step 1
Verify that all cables are connected, and that CIMC has been set for the bare metal server before starting the installation.

Step 2
Open a supported web browser and navigate to https://<CIMC-IP>/login.html, where <CIMC-IP> is the CIMC IP address. The CIMC login page opens.

Step 3
Log in to CIMC using appropriate credentials.

Note
See the CIMC documentation for supported browsers and login credentials.

Step 4
From the CIMC main menu, navigate to the Server > Summary page and launch KVM Console.

Note
Use Java 6 Update 45 to launch KVM if higher Java versions cause failure to launch.

Step 5
Navigate to the Server > BIOS page and confirm that Virtual CD/DVD ROM is first in the boot order.

Step 6
Activate Virtual Devices, and then map the FSGW ISO file to Virtual CD/DVD ROM.

Step 7
Apply power to the server and confirm that it boots the ISO image.

When bootup is complete, the following installation options appear onscreen:

- Automated Kickstart Installation – the default option; requires no user intervention
- Manual Installation – allows the user to define the partition, time zone, and so on
- Boot from local drive – boots from the existing installation

Step 8
Choose Automated Kickstart Installation, or wait 30 seconds for automated installation to begin.

Note
If necessary to interrupt installation, wait for 30 seconds following bootup for the interrupt option.

The following packages are installed during automated installation.

- % packages
- @base - Base utilities
- @core - Core Utilities
- @cos-fsgw - COSFSGW packages
Step 9  When installation is finished, reboot the server.

Step 10 When prompted, log in to the server using the root user name and password.

The Post Install First Boot Configuration utility launches and prompts for configuration information, as shown in the following example:

**Example: Configuration Utility Main Menu**

CentOS Linux 7 (Core)
Kernel 3.10.0-327.10.1.e17.x86_64 on an x86_64

localhost login: root
Password:

Attention!!!
cosfsgw-config script should be run only to configure the device after image installation.

This script modifies network configurations. Improper use of this script may result in mis-configuring the device or making it inaccessible.

Looks like this is the first boot after installation. Please configure the following to proceed further.

1. Host Name
2. Management IP
3. COS PAM IP
4. NTP server IP
5. Bonding if required (reboot required)
6. IP for remaining NICs if any

Please reboot the server once post install configuration is over.

Do you want to configure hostname? [Y/N]

Step 11  Type Y and enter configuration information when prompted, as shown in the following examples.

**Configure Host Name and Management Interface**

Do you want to configure hostname? [Y/N]
Enter the hostname: fsgw248
1-G NIC enp1s0f0 is chosen for Management
Please assign IP for Management NIC enp1s0f0

Enter the IP address: 10.10.10.248
Enter netmask: 255.255.255.0
Enter gateway: 10.10.10.1
Enter dns server ip: 10.10.10.242
Restarting network services, please wait for prompt ...

Enter the IP address of the COS PAM server:

**Configure Interface Bonding**

********************* WARNING *********************
Ensure that link aggregation is enabled on the switch for the interfaces
If link aggregation is not enabled BONDING will not work as expected
*****************************************************************

Modifying the existing bond configurations ...
Bonding module not loaded yet !!!
Restarting network services, please wait for prompt ...
Enter the name for the bond interface (or) Q to quit : bond0

Enter the IP address: 10.10.10.88

Enter netmask: 255.255.255.0
Do you want to add enp3s0f1 as slave for bond0 [Y/N]n
Do you want to add enp3s0f0 as slave for bond0 [Y/N]y
Do you want to add enp130s0f0 as slave for bond0 [Y/N]y
Do you want to add enp130s0f1 as slave for bond0 [Y/N]n
************************************************************************
** Please REBOOT the server for bonding configurations to take effect **
************************************************************************
Enter the name for the bond interface (or) Q to quit :

**List Configurations**

Restarting network services, please wait for prompt . . .

fsgw-config> list

*************** Listing NIC Configurations **********************
=============> Management ==============
 *** Interface : enp1s0f0 IP : 10.10.10.248

==============> Existing bond configuration(s) ===============
 *** Interface : bond0 IP : None

================> IN-MEM Bond configuration(s) =================
 *** Interface : bond0 IP : 10.10.10.88
 Slaves : ['enp3s0f1', 'enp3s0f0']

===============> Individual NICs ===============
 *** Interface : enp130s0f0 IP : None

 *** Interface : enp3s0f1 IP : None

 *** Interface : enp1s0f1 IP : None

fsgw-config> list_all
Device : bond0 IP assigned : None
Device : enp130s0f0 IP assigned : None
Device : enp130s0f1 IP assigned : None
Device : enp3s0f0 IP assigned : 10.10.10.248
Device : enp1s0f1 IP assigned : None
Device : enp3s0f1 IP assigned : None
Device : enp3s0f0 IP assigned : None
Device : lo IP assigned : 10.10.10.1

fsgw-config>

**Step 12** After entering the appropriate configuration options, choose **Reboot** to reboot the server.
Changing Configuration Settings

To change any of these configuration settings later, enter `cosfsgw-config` to invoke the configuration utility. The utility supports the following command line options:

- `bconfig` – to configure bonding
- `hconfig` – to configure host name
- `nconfig_by_name` – to configure IP for a particular NIC
- `list` – to list all the configurations with bond related bindings
- `list_all` – to list all NICs without bond related bindings
- `Reboot` – to reboot the server
- `quit` – to exit configuration shell

Manual Installation via RPMs

If the installation is not on recommended hardware, complete the following steps to install and configure FSGW Release 1.4 on a bare metal server:

1. Step 1: Install the CentOS7 operating system, kernel version 3.10.0-327.10.1.el7.x86_64, on the server.
2. Step 2: Download the current FSGW Release 1.4 RPM package from the Cisco software download page.
3. Step 3: At the server prompt, enter the command `rpm -i <rpm-path>` to install the RPMs:
4. Step 4: Configure FSGW Release 1.4 as described in Configure FSGW on the COS PAM and Tenant PAM, page 2-8.

Installation on the FSGW VM

These instructions apply only for installing FSGW Release 1.4 on a VM.

Hardware Prerequisites

FSGW Release 1.4 supports installation on any server hardware meeting the following minimum requirements:

- 8 x vCPU
- vmxnet3
- 64 GB memory
- 40 GB system disk (including log)
- 2 x 100 GB SSDs for log and cache (optional but recommended)
Chapter 2      Deployment

Installation on the FSGW VM

– 20 GB total allocated for ZIL log
– 180 GB total allocated for L2ARC cache

• 1 x 1G NIC for management
• 1 x 10G NIC for SMB/NFS clients
• 1 x 10G NIC for COS internal

Note
FSGW Release 1.4 was tested on a Cisco UCS-C Series Rack Server with 10G network adapters, or a Cisco UCS-B Series Blade Server with 10G network adapters.

Software Prerequisites

FSGW Release 1.4 has the following software prerequisites:

• VMware vSphere Hypervisor 5.5.0 installed on UCS server
  – Three vSwitch virtual switches vSwitch0 (1G) for management network, vSwitch1 (10G) for COS data network, and vSwitch2 (10G) for client (NFS and Samba) network
  – 250 GB minimum free space in Storage Datastore

• DNS server for PAM
  – Named **dns-1**
  – See the *Cisco Cloud Object Storage Release 3.8.1 User Guide* for installation instructions

• COS PAM and Tenant PAM
  – COS configured on the COS PAM
  – COS configured on the Tenant PAM
  – See the *Cisco Cloud Object Storage Release 3.8.1 User Guide* for installation instructions

• COS cluster
  – See the *Cisco Cloud Object Storage Release 3.8.1 User Guide* for installation instructions

• NTP server
• Win2008R2 for AD authentication and DNS service
  – For DNS service, named as **dns-2**
  – Set AD server as DNS server on FSGW to use AD authentication.
  – Set AD server as DNS server in gateway resolv.conf file.
  – For DNS setting, add dns forwarder as **dns-1**.

Note
The dns-2 server can resolve all dns-1 hosts.

Deploy the FSGW OVA

The FSGW OVA is an archive file containing the FSGW virtual machine. Confirm that you have the latest OVA file (for example, cisco_cos_fsgw_1.4-148.ova) before proceeding.
Chapter 2      Deployment

Step 1  Confirm that the COS cluster, COS-PAM, Tenant-PAM, Windows AD server, NTP server, and DNS server are installed and configured correctly.

Step 2  Log in to the ESXi host using vCenter.

Step 3  Check the ESXi host hardware and software for the following:
- Storage – At least 300 GB free space
- Network – Three vSwitch virtual switches:
  - vSwitch0(1G) for management network
  - vSwitch1(10G) for COS data network
  - vSwitch2(10G) for client (NFS and Samba) network
- Host NTP setting

Step 4  Deploy the FSGW OVA file and complete the following steps in the installation wizard:
   a. Accept the license agreement, then click **Next**.
   b. On the Name and Location page, enter the name of the VM and select its installation location, then click **Next**.
   c. On the Storage page, select the storage to be used (at least 280 GB free space required), then click **Next**.
   d. On the Disk Format page, choose **Thin Provision** as the disk format option, then click **Next**.
   e. On the Network Mapping page, choose the corresponding network from the drop-down list, then click **Next**.
   f. On the Properties page, enter the following parameters:
      - Hostname
      - System Password (enter twice to confirm)
      - COS PAM Server IP address
      - Network Time Server IP address
      - Domain Name Server IP addresses (separated by commas or spaces)
      Recheck your entries, then click **Next**.
   g. On the Ready to Complete page, recheck all settings, then click **Finish**.

**Note**  If you check **Power on after deployment**, the VM starts after you click Finish.

Step 5  Start the FSGW VM, if not started automatically through the wizard.

Step 6  Confirm that the VM is registered to the COS PAM as follows:
   a. Log in to the COS Service Manager GUI as described in the *Cisco Cloud Object Storage Release 3.8.1 User Guide*.
   b. Choose **Infrastructure > Storage > FSG Tenant** in the GUI navigation panel.
   c. On the FSG Tenant page, open the **Filesystem Gateway Nodes** drop-down list and confirm that the name of the deployment just deployed appears in the list.
   d. In the GUI navigation panel, choose **Service Domain Object > Profiles > Auth Profiles**.
   e. On the Auth Profiles page, create a user account using the default name **auth-1**.
Configure FSGW on the COS PAM and Tenant PAM

To configure the FSGW tenant on the COS and Tenant PAMs:

Step 1 Log on to the COS PAM as described in the Cisco Cloud Object Storage 3.8.1 User Guide.
Step 2 In the Service Manager GUI navigation panel, select Panel Infrastructure > Storage > FSG Tenant.
Step 3 On the FSG Tenant page, create a new tenant (or update an existing one) with the following parameters:
   - Tenant Name – use the Tenant PAM GUI user name
   - Auth Profile – Tenant PAM authorization profile
   - Tenant Domain – Tenant PAM domain FQDN or IP address
   - Initial Password – Current password for the Tenant PAM GUI
   - COS Cluster – Cluster to which the Tenant PAM is assigned
   - FSG Nodes – FSGW nodes of the Tenant PAM
Step 4 Find the FSGW VM host, select its COS cluster, and save the configuration.
Step 5 Log in to the Tenant PAM, edit the FSGW VM configuration as described in Configuration Using the Tenant PAM GUI, page 3-1, and save the changes.
Step 6 Log in to the FSGW VM via SSH and confirm that all of these configuration settings are in effect:
   - zpool status or zpool list
   - cat /etc/samba/smb.conf
   - cat /etc/exports
   - realm list
Step 7 Access the FSGW shared folder using the NFS or SMB client.

Adding a Cache and Log to a Zpool (Optional)

FSGW Release FSGW supports adding a Level 2 Adjustable Replacement Cache (L2ARC) virtual drive and a ZFS Intent Log (ZIL) virtual drive to a Linux Z file system (ZFS) virtual storage pool (zpool). If the node on which you install FSGW uses SSD drives, we recommend adding both a cache and a log to a zpool, as they will greatly improve performance.

To add a cache and log to a zpool:
Step 1
Confirm that the FSGW VM was deployed on SSD storage. See step 4c of Deploy the FSGW OVA, page 2-6.

Step 2
Confirm that the FSGW includes three virtual disks (vDisks):
- One 40 GB disk (sda) for system use
- Two 100 GB disks (sdb, sdc) for cache and logging

Step 3
Format the sdb and sdc virtual disks into two partitions, one 10 GB and the other 90 GB, to create four virtual disks total: sdb1 and sdc1 at 10 GB each, and sdb2 and sdc2 at 90 GB each.

```
[root@cosgateway186 ~]# fdisk -1 /dev/sdb
WARNING: fdisk support is currently new, and therefore in an experimental phase. Use at your own discretion.

Disk /dev/sdb: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimal/optimal): 512 bytes / 512 bytes
Disk label type: gpt

# Start   End   Size  Type      Name
1  2048  20973567  10G   Linux filesystem
2 20973568 209715166  90G   Linux filesystem
```

```
[root@cosgateway186 ~]# fdisk -1 /dev/sdc
WARNING: fdisk support is currently new, and therefore in an experimental phase. Use at your own discretion.

Disk /dev/sdc: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimal/optimal): 512 bytes / 512 bytes
Disk label type: gpt

# Start   End   Size  Type      Name
1  2048  20973567  10G   Linux filesystem
2 20973568 209715166  90G   Linux filesystem
```

Step 4
Use the `zpool status` command to check the current zpool status.

```
[root@cosgateway186 ~]# zpool status
pool: test
state: online
scan: none requested
config:

NAME       STATE      READ  WRITE  CKSUM
math       ONLINE     0      0      0
/root/mount/auth05.fsgw.com#container6 ONLINE     0      0      0
logs
mirror-1   ONLINE     0      0      0
  sdb1      ONLINE     0      0      0
  sdc1      ONLINE     0      0      0
  cache
  sdb2      ONLINE     0      0      0
  sdc2      ONLINE     0      0      0
errors: No known data errors
```

Step 5  Run the command:

```
zpool add <zpool_name> log mirror /dev/sdb1 /dev/sdc1 cache /dev/sdb2 /dev/sdc2
```

This defines sdb1 as the log mirror for sdc1, and sdb2 as the cache mirror for sdc2.
Operation and Routine Maintenance

FSGW operation and routine maintenance consists mainly of updating the FSGW node configuration as needed through the Tenant PAM GUI, and periodically monitoring FSGW node status by reviewing statistics and log files through the GUI or the FSGW CLI. This section describes both GUI and CLI operations.

- Configuration Using the Tenant PAM GUI, page 3-1
- Checking Statistics on the Tenant PAM, page 3-2
- Configuration Using the CLI, page 3-7
- Recommended Routine Maintenance, page 3-8
- File Locations, page 3-8

Configuration Using the Tenant PAM GUI

To update the FSGW node configuration, log in to the Tenant PAM GUI and navigate to Infrastructure > File System Gateway to open the File System Gateway page.

Figure 3-1 Tenant PAM GUI - File System Gateway Page

Use this page to check the configuration of the FSGW node and update the configuration as needed.
Creating or Updating a COS Device Pool

You can use the File System Gateway page to create a new COS device pool (zpool) or update an existing device pool as needed.

- To create a new device pool, click the Add button.
- To edit an existing device pool, highlight the pool in the list and click the Edit button.

The COS Device Pool(s) dialog opens as shown in the following example.

*Figure 3-2 Creating or Updating a COS Device Pool*

When creating a new device pool, you supply basic parameters such as pool name, pool type, pool size, and whether compression is used. When assigning a pool name, be sure to observe the following naming conventions:

- A device pool name can only contain alphanumeric characters and the following special characters:
  - Underscore
  - Hyphen
  - Colon
  - Period
- Dev pool names must begin with a letter, but with the following restrictions:
  - The beginning sequence c[0-9] is not allowed.
  - The name log is reserved.
  - A name that begins with mirror, raidz, raidz1, raidz2, raidz3, or spare is not allowed because these names are reserved.
  - Pool names must not contain a percent sign (%).

*Note*

The compression option is a zpool configuration parameter, and is set to Disabled by default. To check the current status of this option via the FSGW CLI, use the command `zfs get compression <poolname>`.
Adding a Cluster

To add a cluster the device pool, click the Cluster button that is active with the device pool in Edit mode. The Cluster dialog opens as shown in the following example.

**Figure 3-3   Adding a Cluster**

Select a cluster from the drop-down list, and then click the Add button to add the cluster to the pool.

Updating NFS Options

To update the NFS options for the device pool, click the NFS button that is active with the device pool in Edit mode. The NFS Options dialog opens as shown in the following example.

**Figure 3-4   Updating NFS Options**

Change the configuration as needed, and then click Save.
Updating SMB Options

To update the SMB options for the device pool, click the **SMB** button that is active with the device pool in Edit mode. The SMB Options dialog opens as shown in the following example.

**Figure 3-5 Updating SMB Options**

![SMB Options dialog](image)

Change the configuration as needed, and then click **Save**.

Updating Quotas

To update the Quotas for the device pool, click the **Quotas** button that is active with the device pool in Edit mode. The Quotas dialog opens as shown in the following example.

**Figure 3-6 Updating Quotas**

![Quotas dialog](image)

Change the configuration as needed, and then click **Save**.

Updating Device Pool Resiliency

You can configure resiliency at the level of the device pool (via the FSGW node) or the COS cluster, or both, as best meets the needs of the deployment. Resiliency at the device pool level applies across COS clusters, while resiliency at the COS cluster level applies to the nodes in that particular COS cluster.
Note

See the Cisco Cloud Object Storage Release 3.8.1 User Guide for details on configuring resiliency within a COS cluster.

The Pool Resiliency section of the COS Device Pool(s) dialog lets you choose the desired type of resiliency for the device pool as well as the maximum number of failures permitted.

Figure 3-7  Updating Device Pool Resiliency

Choose one of the following resiliency methods:

- Mirroring – Each COS cluster has an identical copy of the data in the device pool.
- Erasure Coding – Data and parity are distributed across COS clusters using dynamic stripe width to guarantee the ability to recover both data and resiliency for up to the specified maximum failures.

Note

- With either Mirroring or Erasure Coding resiliency, the device pool must have at least two associated COS clusters.
- The number of associated COS clusters must be at least one greater than the specified Max Failures.

Checking Statistics on the Tenant PAM

The FSG Statistics page of the FSGW SM GUI lists all existing FSGW nodes and displays a wealth of information about the Tenant PAM, including:

- Storage usage
- Bandwidth
- Operations
- COS cluster containers
- FSG services
- Zpool status

In addition, this page displays any active alarms and their severity levels to help identify any issues with the FSGW.

To access the FSG Statistics page, open the FSGW Service Manager GUI navigation panel and choose **Infrastructure > FSG Statistics**. The page appears as shown in the example of Figure 3-8.

**Figure 3-8  FSG Statistics Page, Top**

The bottom of the page provides details on Cluster, Service, and Device pools, as shown in the example of Figure 3-9.

**Figure 3-9  FSG Statistics Page, Bottom**
Configuration Using the CLI

The FSGW CLI lets you check services and configuration manually. To access the CLI, log into the FSGW node of interest via SSH using the following credentials:

- Username: root
- Password: rootroot

To check the FSGW network, use `ifconfig`. For example:

```
ifconfig ens35, ens160, ens192
```

There are three network adapters on the FSGW VM: Management network, COS data network, and Client data network. Be sure that each NIC is up and running and has a valid IP address.

To test each network, use `ping <gateway>`.

To check each FSGW service, use `lsmod | grep` as follows:

```
lsmod | grep zfs
lsmod | grep cosdevfs
lsmod | grep dns Resolver
```

To check FSGW communication and configuration services:

```
systemctl status cosfsgw
systemctl status cosfsgwpam
```

To check and then test the DNS service:

```
cat /etc/resolv.conf
nslookup <cos_auth_fqdn>
```

To check the NTP configuration and status:

```
cat /etc/chrony.conf
chronyc sources
```

To check the COS container mount status:

```
ls /var/cisco/cosfsgw/mnt
cat /sys/cosdevfs/gateway_config
```

To check the zpool status:

```
zpool scrub <zpool_name>
zpool status -v
```

To check the SMB configuration and services:

```
cat /etc/samba/smb.conf
systemctl status smb
```

To check the NFS configuration and services:

```
cat /etc/exports
systemctl status nfs
```

To check the AD status:

```
realm list
```
Recommended Routine Maintenance

Daily Tasks

- Check the Tenant PAM GUI to be sure that there are no major alarms or errors displayed.
- Check the COS PAM to be sure that there are no major issues on the COS side.

Weekly Tasks

- Run the `zpool scrub <zpool_name>` CLI command on FSGW to be sure that zpool is in good state after running for a week.

File Locations

The FSGW logs are at the following locations:

- `/var/log/`
- `/var/log/cisco/cosfsgw/`

The configuration files are at the following location:

- `/etc/cisco/cosfsgw/`

Usage Example

[root@cosgateway_4_720 ~]# cd /etc/cisco/cosfsgw/
[root@cosgateway_4_720 cosfsgw]# l1
    total 20
    -rw-r--r-- 1 root root 239 Jul 20 22:03 announce.json
    -rw-r--r-- 1 root root 2912 May 19 15:04 current.pam.json
    -rw-r--r-- 1 root root 111 Jul 20 19:59 events_monitoring.json
    -rw-r--r-- 1 root root 107 Jul 21 00:32 init.json
    -rw-r--r-- 1 root root 190 Jul 18 21:03 stats_monitoring.json

To check the FSGW version, check the FSGW rpm as follows:

[root@cosgateway_4_720 ~]# rpm -qa | grep cosfsgw-aic
cosfsgw-aic-client-1.2.1-164.el7.centos.x86_64
[root@cosgateway_4_720 ~]#
Troubleshooting

This section identifies some common issues you may encounter with FSGW Release 1.4, and provides suggestions for diagnosing and resolving these issues.

- Modules are Loaded Properly, page 4-1
- Configuring Support to Add or Delete a Container, page 4-1
- Reading or Writing to a Pool, page 4-2

Modules are Loaded Properly

The `zpool list` command should list the pool created. If the pool is not listed:

- Check to see if the zfs, cosdevfs, and dns_resolver modules are loaded.
  
  ```bash
  [root@cosgateway1 cosdevfs]# lsmod | grep "zfs\| dns_resolver\|cosdevfs"
  tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=800768k,mode=700)
  ```

- Check to see if the cosdevfs is mounted.
  
  ```bash
  [root@cosgateway1 cosdevfs]# mount | grep cosdevfs
  cosdevfs on /home/dinesh/queue_metastab/fs_gateway/cosdevfs/mount type cosdevfs (rw,relatime)
  ```

  Or, check to see if the default mount point have the following file:
  
  ```bash
  [root@cosgateway1 cosdevfs]# ls -lh ./mount/ total 0
  c--x--x--x 1 root root 0, 0 Jul 19 07:28 cosdev_data
  ```

- The following message in the cosdevfs log indicates that the cosdevfs module is loaded.
  

Configuring Support to Add or Delete a Container

A command to add or delete a container object may result in an error message like that shown in the following example.

```bash
[root@cosgateway1 cosdevfs]# zpool create -f -O recordsize=2M raidtst /home/dinesh/queue_metastab/fs_gateway/cosdevfs/mount/auth02.p2.cisco.com#donald
Cannot resolve path /home/dinesh/queue_metastab/fs_gateway/cosdevfs/mount/auth02.p2.cisco.com#donald
```
Reading or Writing to a Pool

In the example above, the error message indicates that the configuration is not added and that vdev is not available in the mount path.

A command to create or delete a container object also may result in an error message like that shown in the following example:

```
[root@cosgateway1 ~]# echo
"cmd:add,cluster:auth02.p2.cisco.com,container:donald,size:300,account:test:eric,key:eric"
> /sys/cosdevfs/gateway_config
-bash: /sys/cosdevfs/gateway_config: No such file or directory
```

In this case, the error message indicates that the cosdevfs module is not loaded.

The following sample error message in the cosdevfs log indicates that the cosdevfs module is not mounted:

```
```

The following sample error message indicates that the authentication failed due to an invalid user account in the configuration add command:

```
```

The following sample error message indicates that the cluster (auth07.p7.com) is either not available or is an invalid cluster name.

```
```

The following sample error message indicates that the add configuration failed due to either an invalid user account, an unavailable cluster, or an invalid cluster name.

```
```

The following sample error message indicates that the add configuration was successful.

```
Jul 20 05:30:35 cosgateway1 kernel: app-name: kern.cosdevfs, thread: conf_3, desc: completed config update successfully
```

In this successful case, the mount directory will contain a file similar to the one listed below.

```
[root@cosgateway1 cosdevfs]# ls -lh ./mount/ total 0
-rwrxr-xr-x 1 root root 300G Jul 20 05:30 auth02.p2.cisco.com#donald -> Container Name
```

Reading or Writing to a Pool

For every Read or Write transaction, each thread having a BEGIN status should be associated with a COMPLETE status, as shown in the following examples.

```
Jul 20 06:00:37 cosgateway1 kernel: app-name: kern.cosdevfs, txn: WRITE, thread: IO_3_10, object: cosdevfs-obj-399360-1024, status: BEGIN, desc: Write begining

Jul 20 06:00:37 cosgateway1 kernel: app-name: kern.cosdevfs, txn: WRITE, thread: IO_3_10, object: cosdevfs-obj-399360-1024, status: COMPLETE, desc: Write completed
```

After writing data to the container, running `zpool scrub` and checking `zpool status` should result in a report of no data errors returned, as shown in the following example.
[root@cosgateway1 raidtst]# zpool status pool: raidtst
state: ONLINE
scan: scrub repaired 0 in 0h0m with 0 errors on Wed Jul 20 06:09:27 2016

errors: No known data errors

Note: All of the log examples shown above are from /var/log/cisco/cosfsgw/cosdevfs.log. In general, you can use the Linux `grep` command to search for the status string `ERROR` as a way to track down errors.
Global Namespace Option

This section describes the Global Namespace (GNS) option available for COS Filesystem Gateway (FSGW) Release 1.4. GNS is a cost option that can be installed and configured separately following installation of FSGW to enable horizontal scalability and improve throughput.

Overview

FSGW alone supports a single virtual machine (VM) configuration that does not directly support the clustering of network resources. FSGW throughput is thus limited to the capacity of the VM, making FSGW a potential bottleneck to the performance of COS systems as they scale. Adding the GNS option creates an aggregation layer that enables clustering of FSGW servers, allowing throughput to scale horizontally. GNS provides the logical intermediation needed to coordinate a group of FSGW servers so that they operate as a cluster.

The GNS option is implemented using Red Hat GlusterFS, a scalable open-source file system that aggregates distributed network resources in a single global namespace. The GlusterFS server performs volume setup, manages the bricks (logical components) in the volume, and manages communication with the nodes. The GlusterFS Native Client also provides a proxy layer above the GlusterFS server to perform load-balancing, file locking, and failover for the FSGW cluster.

Note

See http://redhatstorage.redhat.com/products/glusterfs/ for additional information on GlusterFS and its system architecture.

Feature Summary

GNS adds the following features and enhancements to compatible FSGW releases:

- Horizontal scaling of FSGW servers
- Single FSGW node write throughput up to 5 Gbps
- Horizontal scaling of FSGW proxies
- Approximately linear increase of throughput when adding more FSGW servers and FSGW proxies to the architecture
- Automatic failover of FSGW servers
- File locking when CTDB is added in FSGW proxies
Hardware Support

GNS supports installation on server hardware meeting the following minimum requirements:

- 8 x vCPU
- vmxnet3
- 64 GB memory
- 40 GB system disk (including log)
- 2 x 100 GB SSDs for zpool log and cache (optional but recommended)
  - 20 GB total allocated for ZIL log
  - 180 GB total allocated for L2ARC cache
- 1 x 1G NIC for management
- 1 x 10G NIC for SMB/NFS clients
- 1 x 10G NIC for COS internal (not needed for FSGW Proxies)

System Requirements

GNS uses FSGW Release 1.4 and COS Release 3.8.1 (or the COS 3.10.1 pre-release) as its companion release. COS and FSGW use the same COS PAM component, with an additional Tenant PAM for FSGW.

Software Components

Table A-1 lists the software components and versions have been qualified for this release:

<table>
<thead>
<tr>
<th>Software Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSGW ISO</td>
<td>COS-FS-Gateway-x86_64-1.4-148.iso</td>
</tr>
<tr>
<td>FSGW OVA</td>
<td>cisco_cos_fsgw_1.4-148.ova</td>
</tr>
<tr>
<td>COS 3.10.1</td>
<td>cos_full-3.10.1-0b26-x86_64.iso</td>
</tr>
<tr>
<td>COS PAM</td>
<td>2.5.1-cisco-mos-mendocino.2.4.1.cos_3101.20790.ova</td>
</tr>
<tr>
<td>Tenant PAM</td>
<td>2.5.0-cisco-mos-mendocino.2.4.1.fs.gateway.tenant.20366.ova</td>
</tr>
<tr>
<td>GlusterFS</td>
<td>Customized 3.8.5-0.23</td>
</tr>
</tbody>
</table>

Installation Environment

GNS requires the following installation environment for FSGW Release 1.4:

- VMware vSphere Hypervisor 5.5.0 installed on a UCS server
- DNS server for PAM
- COS PAM and Tenant PAM
- COS Cluster and NTP Server
- Win2008R2 for AD authentication and DNS service
Restrictions and Limitations

- GNS does not provide a strictly linear performance increase when adding more nodes to a FSGW cluster.
- GNS does not support file locking for NFS v3. File locking is not supported when using Common Internet File System (CIFS) alone, but byte range locking is supported when using CIFS and Cluster Trivial Database (CTDB).

Installation and Configuration

GNS installation and configuration involves the following procedures:

- Install Filesystem Gateway (FSGW) Server, page A-3
- Install the GlusterFS Server on the FSGW Node, page A-3
- Start the GlusterFS Servers, page A-4
- Create a Zpool on the FSGW Server, page A-4
- Create the GlusterFS Volume, page A-5
- Install the FSGW Proxy, page A-5
- Mount the GlusterFS Share on the Client Server, page A-6
- Option: Using the GlusterFS Native Client as a User Client, page A-6
- Option: Using CTDB to Manage Samba Shares for GlusterFS Volumes Created using Cisco modified ZFS, page A-7
- Option: Sharing GlusterFS Volumes over NFS Ganesha, page A-11

Install Filesystem Gateway (FSGW) Server

FSGW Release 1.4 must be installed on a server before GNS can be installed and configured as a layer upon FSGW. For FSGW server installation instructions, see Deployment, page 2-1.

Install the GlusterFS Server on the FSGW Node

To install the GlusterFS server on the FSGW node, a customized GlusterFS RPM package is required to ensure compatibility with the cosdevfs component of FSGW.

Step 1: Download the customized GlusterFS RPM package from the Cisco Software Downloads site.

Step 2: Install the customized GlusterFS components as shown in the following example:

```bash
rpm -ivh glusterfs-libs-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh python-gluster-3.8.5-0.23.git494dbb8.el7.centos.noarch.rpm
rpm -ivh glusterfs-extra-xlators-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-client-xlators-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-api-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-fuse-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-cli-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
yum install centos-release-gluster
```
yum install userspace-rcu
rpm -ivh glusterfs-server-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm

Start the GlusterFS Servers

Step 1  Complete the steps described in Install the GlusterFS Server on the FSGW Node, page A-3 for each FSGW node to be included in the cluster.

Step 2  Start the GlusterFS server on all nodes to be included in the cluster as shown in the following example:
        service glusterd start
        chkconfig glusterd on

Step 3  On one of the FSGW nodes, find all other FSGW nodes and add them into the cluster as follows:
        gluster peer probe <server_data_ip>

Create a Zpool on the FSGW Server

A zpool is used as a brick of the GlusterFS volume. It can be created through the Tenant PAM GUI or using the CLI. You must create a zpool on each node in the FSGW cluster.

Using the Tenant PAM

For instructions on using the Tenant PAM to create a zpool, see Deployment, page 2-1.

Using the CLI

To create a zpool on one FSGW node through the CLI:

Step 1  Create a container on the COS cluster and mount the container on the FSGW node.

Example
echo
"cmd:add,cluster:auth12.fsgw.com,container:test12,size:20000,account:auth-1:jdoe,key:a86850deb742ec3cb4
> /sys/cosdevfs/gateway_config

Step 2  Create the zpool by mounting the container as shown in the following example.

Example
zpool create -f -O recordsize=2M test6 /var/cisco/cosfsgw/mnt/auth12.fsgw.com#test12
Create the GlusterFS Volume

**Step 1**
On each FSGW node in the cluster, create a subdirectory from the zpool mount point.

**Example**

```
mkdir -p /test6/bricks/share/brick1
```

**Step 2**
On one FSGW node in the cluster, create the GlusterFS volume.

**Example**

```
gluster vol create test6 10.10.10.58:/test6/bricks/share/brick1
10.10.10.53:/test6/bricks/share/brick1 10.10.10.55:/test6/bricks/share/brick1
10.10.10.12:/test6/bricks/share/brick1
gluster vol start test6
```

Install the FSGW Proxy

The FSGW proxy is a server that holds the GlusterFS Native Client and mounts the GlusterFS volume as a GlusterFS share. The FSGW proxy then exports the mounted share as needed via either an NFS server or Samba server. Clients can then mount the share using the NFS or Samba protocol, as dictated by the needs of the clients.

**Note**

The FSGW proxy can be a CentOS7 server with a basic configuration.

The procedure to install the GlusterFS native client is identical to that for installing the GlusterFS server on the FSGW node. See Install the GlusterFS Server on the FSGW Node, page A-3 for instructions.

Mount the GlusterFS Volume on the FSGW Proxy

**Step 1**
On each FSGW proxy, add a new route to each FSGW node data IP address via its client IP.

**Example**

```
route add -net 10.10.10.58 netmask 255.255.255.255 gw 10.10.10.58 metric 10 dev ens192
route add -net 10.10.10.55 netmask 255.255.255.255 gw 10.10.10.55 metric 11 dev ens192
route add -net 10.10.10.53 netmask 255.255.255.255 gw 10.10.10.53 metric 12 dev ens192
route add -net 10.10.10.12 netmask 255.255.255.255 gw 10.10.10.12 metric 13 dev ens192
```

**Step 2**
Mount the GlusterFS share from one of the FSGW nodes.

**Syntax**

```
mount -t glusterfs <server_client_ip>:<glusterfs_vol_name> <mountpoint>
```
Export the Mounted GlusterFS Share

Export the mounted GlusterFS share using NFS or Samba server, according to the needs of the clients.

**Export via NFS Server**

Add an entry to `/etc/exports` and then restart nfs service, as shown in the following example:

```
/mnt/share *(rw,fsid=1,no_root_squash,async)
```

```
service nfs restart
```

**Export via Samba Server**

Add a section in `/etc/samba/smb.conf` and then restart the smb service, as shown in the following example.

```
[share]
comment = shared path = /mnt/share guest ok = yes read only = no public = yes writable = yes
hosts allow = 10.20.
valid users = root
```

```
service smb restart
```

Mount the GlusterFS Share on the Client Server

After the GlusterFS share is exported from each FSGW proxy node, it can be mounted by the NFS or Samba clients in the usual manner.

**For NFS Client**

Mount the client using the following command syntax:

```
mount <fsgw_proxy_client_ip>:<export_path> <mount_point>
```

**For Samba Client**

Create the samba user on samba client and set a password using the following command syntax:

```
mount -t cifs <fsgw_proxy_client_ip>:<export_path> <mount_point> -o user=<smb_user>,pass=<password>
```

For instructions on mounting the Samba share, see Option: Using CTDB to Manage Samba Shares for GlusterFS Volumes Created using Cisco modified ZFS, page A-7.

Option: Using the GlusterFS Native Client as a User Client

The GlusterFS Native Client and GlusterFS volume can also be installed directly on a user node. With this approach, the client acts as a user client, and there is no need for an FSGW proxy or intermediation by NFS or Samba.

Complete the following steps to install the GlusterFS Native Client on a user node:

**Step 1**
Install the customized GlusterFS RPMs on the user node as described in Install the GlusterFS Server on the FSGW Node, page A-3.

**Step 2**
On the user node, add a route to each FSGW node data IP address via its client IP address.

```
route add -net 10.10.10.58 netmask 255.255.255.255 gw 10.10.10.58 metric 10 dev ens192
```
Appendix A      Global Namespace Option

Installation and Configuration

Step 3

Mount the GlusterFS volume directly using the GlusterFS client.

**Syntax**

```
mount -t glusterfs <server_client_ip>:<glusterfs_vol_name> <mountpoint>
```

## Option: Using CTDB to Manage Samba Shares for GlusterFS Volumes Created using Cisco modified ZFS

This section describes the steps for creating GlusterFS volumes using a Cisco modified version of ZFS using Swift over Cisco Cloud Object Storage (COS). It also describes the steps for sharing such volumes over Samba or CIFS to enable clustering and high availability.

**Note**

For instructions on sharing GlusterFS volumes over NFS Ganesha, see Option: Sharing GlusterFS Volumes over NFS Ganesha, page A-11.

### GlusterFS RPMs

The GlusterFS RPMs include a patch to enable the use of a Cisco modified version of ZFS. This patch is located on the GlusterFS volume in the path /root/glusterfs-rpms.

#### Installing RPMs

Install the following RPMs in the sequence shown in the following examples:

```
rpm -ivh glusterfs-libs-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh python-gluster-3.8.5-0.23.git494dbb8.el7.centos.noarch.rpm
rpm -ivh glusterfs-extra-xlators-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-client-xlators-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-api-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-fuse-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
rpm -ivh glusterfs-cli-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
yum install centos-release-gluster
yum install userspace-rcu
rpm -ivh glusterfs-server-3.8.5-0.23.git494dbb8.el7.centos.x86_64.rpm
yum install samba-vfs-glusterfs
```

### Create ZFS Pools

The following procedure assumes two servers hosting GlusterFS volumes at IP addresses 10.10.10.5 and 10.10.10.8, and a Samba client at 10.10.10.9, and refers to them as Servers 5, 8, and 9, respectively.

#### Step 1

Confirm that the `lsmod` output is similar on both servers used for hosting volumes, as shown in the following example:

```
[root@gateway9_raidztest ctdb]# lsmod | grep zfs
zfs 2794315 5 cosdevfs
```
Step 2  Run the following command on both Server 5 and Server 8:

```bash
mount -t cosdevfs cosdev /var/cisco/cosfsgw/mnt
```

Step 3  Run the following command to create a ZFS pool named `glusterp` on Server 5:

```bash
zpool create -O recordsize=2M glusterp /var/cisco/cosfsgw/mnt/auth10.fsgw.com#hacluster -f
```

Step 4  Run the following command to create a ZFS pool named `glusterp` on Server 8:

```bash
zpool create -O recordsize=2M glusterp /var/cisco/cosfsgw/mnt/auth10.fsgw.com#hacluster1 -f
```

Step 5  Run the following commands on both Server 5 and Server 8:

```bash
mkdir -p /glusterp/bricks/config/brick1
mkdir -p /glusterp/bricks/config/ctdb
```

Step 6  Confirm that glusterd is now running on both Server 5 and Server 8.

Step 7  Execute `gluster peer probe 10.10.10.8` from server 5.

Step 8  Run commands on Server 5 to create GlusterFS volumes out of ZFS pools, as shown in the following example:

```bash
gluster vol create data replica 2 10.10.10.5:/glusterp/bricks/config/brick1 10.10.10.8:/glusterp/bricks/config/brick1
gluster volume set data user.smb disable
gluster volume set data server.allow-insecure on
gluster volume set data stat-prefetch off
gluster volume set data storage.batch-fsync-delay-usec 0
gluster volume set data user.smb disable
gluster volume start data
```

Volume Name: data
Type: Replicate
Volume ID: 6bc8716d-45bd-4006-8623-73a2887130b6
Status: Started
Snapshot Count: 0
Number of Bricks: 1 x 2 = 2
Transport-type: tcp
Bricks:
Brick1: 10.10.10.5:/glusterp/bricks/config/brick1
Brick2: 10.10.10.8:/glusterp/bricks/config/brick1
Options Reconfigured:
nfs.disable: on
performance.readdir-ahead: on
transport.address-family: inet
user.smb: disable
server.allow-insecure: on
performance.stat-prefetch: off
storage.batch-fsync-delay-usec: 0

Step 9  Run commands on Server 5 to create separate config volume to host lock files, as shown in the following example:

gluster volume create ctdb replica 2 10.10.10.8:/glusterp/bricks/config/ctdb 10.10.10.5:/

Step 10 Edit /etc/glusterfs/glusterd.vol on Server 5 and Server 8 to add the following setting:
option rpc-auth-allow-insecure on

Step 11 Create files on both Server 5 and Server 8 as shown in the following example:

/etc/ctdb/nodes
10.10.10.5
10.10.10.8
/etc/ctdb/public_addresses
10.10.10.10/24 ens35
10.10.10.10/24 ens35
/etc/sysconfig/ctdb
CTDB_RECOVERY_LOCK=/gluster/lock/lockfile
#CIFS only
CTDB_PUBLIC_ADDRESSES=/etc/ctdb/public_addresses
CTDB_MANAGES_SAMBA=yes
#CIFS only
CTDB_NODES=/etc/ctdb/nodes

Step 12 Confirm that /etc/samba/smb.conf on both Server 5 and Server 8 has entries for clustering and share:

[global]
map to guest = Bad User
clustering = yes
idmap backend = tdb2
kernel share modes = no
kernel oplocks = no
map archive = no
map hidden = no
map read only = no
map system = no
store dos attributes = yes
[gluster-data]
comment = For samba share of volume ctdb
vfs objects = glusterfs
glusterfs:volume = data
glusterfs:logfile = /var/log/samba/glusterfs-ctdb.%M.log
glusterfs:loglevel = 7
path = /
read only = no
guest ok = yes
writable = yes
valid users = vijay root dinesh
[gluster-ctdb] ** Not sure about this, we may omit this section, but that is not tested.
comment = For samba share of volume ctdb
vfs objects = glusterfs
glusterfs:volume = ctdb
glusterfs:logfile = /var/log/samba/glusterfs-ctdb.%M.log
glusterfs:loglevel = 7
path = /
read only = no
guest ok = yes
Step 13 On both Server 5 and Server 8, edit the ctdb startup scripts to mount a config volume in /gluster/lock. In the following files, replace all in the statement `META=ctdb`.

- `/var/lib/glusterd/hooks/1/start/post/S29CTDBsetup.sh`
- `/var/lib/glusterd/hooks/1/stop/pre/S29CTDB-teardown.sh`

**Note** Script S29CTDBsetup.sh depends on host name resolution. It can be modified to use IP addresses as shown in the following example:

```bash
parse_args $@
if [ "$META" = "$VOL" ]
then
  mkdir -p $CTDB_MNT
  sleep 5
  #mount -t glusterfs -o{MNTOPTS} $(HOSTNAME):/$VOL "$CTDB_MNT" \
  mount -t glusterfs -o{MNTOPTS} 10.74.124.8:/$VOL "$CTDB_MNT"
  \n  add_fstab_entry $VOL $CTDB_MNT
  chkconfig ctdb on
fi
```

Step 14 On Server 5, execute `gluster volume start ctdb`.

Step 15 Confirm that /gluster/lock is mounted on both Server 5 and Server 8.

**Example - Server 5**

```
[root@gateway5 glusterfs-rpms]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/centos-root 30G 2.9G 28G 10% /
devtmpfs 32G 0 32G 0% /dev
tmpfs 32G 0 32G 0% /dev/shm
tmpfs 32G 41M 32G 1% /run
tmpfs 32G 0 32G 0% /sys/fs/cgroup
/dev/sda1 497M 212M 285M 43% /boot
tmpfs 6.3G 0 6.3G 0% /run/user/0
glusterp 1.9T 0 1.9T 0% /glusterp
gateway5:/ctdb.tcp 1.9T 0 1.9T 0% /gluster/lock
```

**Example - Server 8**

```
[root@gateway8 brick1]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/centos-root 30G 2.1G 28G 7% /
devtmpfs 32G 0 32G 0% /dev
tmpfs 32G 0 32G 0% /dev/shm
tmpfs 32G 41M 32G 1% /run
tmpfs 32G 0 32G 0% /sys/fs/cgroup
/dev/sda1 497M 212M 285M 43% /boot
tmpfs 6.3G 0 6.3G 0% /run/user/0
glusterp 1.9T 0 1.9T 0% /glusterp
gateway8:/ctdb.tcp 1.9T 0 1.9T 0% /gluster/lock
```

Step 16 Execute `systemctl restart ctdb` on both Server 5 and Server 8, as shown in the following example:

```
[root@gateway5 glusterfs-rpms]# ctdb status
Number of nodes:2
pnn:0 10.10.10.5 OK (THIS NODE)
pnn:1 10.10.10.8 OK
```
### Appendix A      Global Namespace Option

#### Installation and Configuration

**Generation:** `1100789658`

**Size:** `2`

**hash:** `0` **lmaster:** `0`

**hash:** `1` **lmaster:** `1`

**Recovery mode:** `NORMAL (0)`

**Recovery master:** `0`

```
[root@gateway5 glusterfs-rpms]# ctdb ip
Public IPs on node 0
10.10.10.11 1
10.10.10.113 0
```

---

**Step 17** Create Samba users and add permissions to the added users, as shown in the following example:

- `smbpasswd -a root`
- `smbpasswd -a vijay`
- `smbpasswd -a dinesh`
- `sudo chown vijay: /glusterp`
- `sudo chown dinesh: /glusterp`
- `sudo chmod u+w /glusterp`
- `sudo chmod -R ugo+rw /glusterp`

**Step 18** Mount the share `gluster-data` over CIFS by loading it from Server 9, as shown in the following example:

```
mount -t cifs //10.10.10.11/gluster-data /mnt/ctdb/ -o user=dinesh,pass=dinesh
```

---

**Option: Sharing GlusterFS Volumes over NFS Ganesha**

This section describes the steps to set up ZFS, GlusterFS, CTDB, the Samba-gluster vfs Plugin, and NFS Ganesha for sharing GlusterFS volumes.

The following procedure assumes two servers hosting GlusterFS volumes at IP addresses 10.10.10.5 and 10.10.10.8, and a Samba client at 10.10.10.9, and refers to them as Servers 5, 8, and 9, respectively.

#### Prepare the Nodes

**Step 1** Run `glusterfs cluster:` on both Server 5 and Server 8 to install native ZFS at IP addresses 10.10.10.5 and 10.10.10.8. The client node IP addresses are 10.10.10.41 (Windows) and 10.10.10.9 (Linux).

**Step 2** Use the command `zpool create -f gluster /dev/sdc` on both nodes to create a zpool on each node.

**Step 3** Install GlusterFS on both nodes as shown in the following example:

```
yum install glusterfs-server -y
chkconfig glusterd on
service glusterd start
mkdir -p /gluster/bricks/share/brick1
```

**On One Node**

```
gluster peer probe 10.10.10.5
gluster vol create share replica 2 10.10.10.5:/gluster/bricks/share/brick1
10.10.10.8:/gluster/bricks/share/brick1
gluster vol start share
```

**On Both Nodes**

```
mkdir -p /gluster/bricks/config/brick1
```
### Installation and Configuration

#### On One Node

```bash
gluster vol create config replica 2 10.10.10.5:/gluster/bricks/config/brick1
10.10.10.8:/gluster/bricks/config/brick1
gluster vol start config
```

#### On Both Nodes

```bash
mkdir /opt/samba-config
mount -t glusterfs localhost:config /opt/samba-config
echo "localhost:config /opt/samba-config glusterfs defaults,_netdev 0 0" >>/etc/fstab
```

### Configuring Samba and CTDB

Complete the following steps to configure Samba and CTDB:

#### Step 1

Use the following commands to configure Samba and CTDB:

```bash
yum -y install ctdb samba samba-common samba-winbind-clients samba-client
samba-vfs-glusterfs
```

#### Step 2

Edit the `ctdb` file in `/opt/samba-config` as follows:

```bash
vi /opt/samba-config/ctdb:
CTDB_RECOVERY_LOCK=/opt/samba-config/lockfile
#CIFS only
CTDB_PUBLIC_ADDRESSES=/etc/ctdb/public_addresses
CTDB_MANAGES_SAMBA=yes
#CIFS only
CTDB_NODES=/etc/ctdb/nodes
```

#### Step 3

Enter `rm /etc/sysconfig/ctdb` to remove this directory.

#### Step 4

Link the Samba and System `ctdb` files as follows:

```bash
ln -s /opt/samba-config/ctdb /etc/sysconfig/ctdb
service smb stop
chkconfig smb off
chkconfig ctdb on
```

#### Step 5

Edit the `public_addresses` and `nodes` files as follows:

```bash
vi /opt/samba-config/public_addresses:
10.10.10.11/24 ens35
10.10.10.113/24 ens35
vi /opt/samba-config/nodes:
10.10.10.5
10.10.10.8
ln -s /opt/samba-config/nodes /etc/ctdb/nodes
ln -s /opt/samba-config/public_addresses /etc/ctdb/public_addresses
```

#### Step 6

Open the SMB configuration file and add lines to the Global section, as shown in the following example:

```bash
vi /opt/samba-config/smb.conf
map to guest = Bad User
clustering = yes
idmap backend = tdb2
```

#### Step 7

Add the following lines at the end of the SMB configuration and then save the changes.

```bash
[share]
comment = gluster vfs share
path = /
read only = No
```
Appendix A      Global Namespace Option

Installation and Configuration

guest ok = Yes
kernel share modes = No
create mask = 777
directory mask = 777
writable = yes
force user = nobody
vfs objects = glusterfs
glusterfs:loglevel = 9
glusterfs:logfile = /var/log/samba/glusterfs-testvol.log
glusterfs:volume = share

cp /opt/samba-config/smb.conf /etc/samba/
service ctdb start

Mount the Samba Share on the Client

**Step 1** Mount the Samba share using the following virtual IP addresses:
- 10.10.10.11
- 10.10.10.113

**Step 2** On Windows client 10.10.10.41, open a web browser and navigate to `\10.10.10.11\share`.

**Step 3** On Linux client 10.10.10.9, mount the share as follows:

**Syntax**

```bash
mkdir /opt/gluster-share
mount -t cifs //10.10.10.11/share /opt/gluster-share -o user=guest,guest
```

Configure NFS Ganesha on CTDB

Configure NFS Ganesha on CTDB as follows:

```bash
gluster volume set all cluster.enable-shared-storage enable
gluster nfs-ganesha enable
gluster vol set share ganesha.enable on vi /etc/ganesha/ganesha.conf:
EXPORT
{
    # Export Id (mandatory, each EXPORT must have a unique Export_Id) Export_Id = 2;
    # Exported path (mandatory)
    Path = /share;
    # Pseudo Path (required for NFS v4)
    Pseudo = /share;
    # Required for access (default is None)
    # Could use CLIENT blocks instead Access_Type = RW;
    # Exporting FSAL FSAL {
    Name = GLUSTER; Hostname = localhost;
    Volume = share;
    }
}
%include "/etc/ganesha/exports/export.share.conf"
service nfs-ganesha restart
```
Mount NFS Share on Linux Clients

Use the following command to mount the NFS share on all Linux clients:

```
mount 10.10.10.113:/share /opt/nfstest/
```