Democratic and Popular Algerian Republic
Ministry of Higher Education and Scientific Research
National School of Computer Science and Technology

Project Report: Network Services and Infrastructure

Chapter 06 : FOG Troubleshooting and Optimization

Members

- Soum Mohamed Islam
- Bahloul Rami
- Hadjoudj Charafeddine
- Youcefi Mohamed
- Gouhmaz Mohamed

Supervisor

Dr.Allama

Submission date : 12/05/2025

1. Introduction

In modern IT infrastructures, particularly in businesses that deal with enormous numbers of workstations, the ability to automate OS installation is crucial. Manually installing or configuring OSs on every machine is truly time-consuming. That is where tools like FOG and OpenMediaVault (OMV) are essential components of an efficient infrastructure.

FOG Project is a free, open source tool that provides a centralized platform for disk imaging, cloning, and deployment. it helps allowing administrators to deploy pre configured operating system images to multiple computers without any manual intervention on the client side. This kind of automation is especially useful in setting enterprise environments where machines need to be uniformly configured.

OpenMediaVault (OMV) is a Debian Linux based open source network attached storage solution. Most commonly, it is utilized as a backend storage repository for servers such as FOG, which need reliable and scalable access to huge data sets.
FOG and OMV make a great deployment and storage combination. FOG handles imaging and deployment, and OMV hosts the actual image files and serves them up on the network. When using FOG with OMV in a network services situation, it offers:

- Centralized image deployment and management.
- The computerized installation of numerous systems.
- An adaptable and expandable storage system.
- Reduced manual effort for IT administrators

Learning Objectives

This report focuses on the troubleshooting and optimization of FOG when integrated with OMV. The key learning objectives include:

- Understanding the integration of FOG and OMV
- Identifying common issues during setup or operation
- Applying optimization techniques for performance and security

2. Conceptual Background

To understand the troubleshooting and optimization of a FOG and OMV deployment setup, it's essential to first understand the foundational technologies within a networked environment.

What is FOG?

FOG is a Linux-based, free and open source computer imaging solution for various versions of Windows (XP, Vista, 7, 8/8.1, 10), Linux and Mac OS. It ties together a few open source tools with a PHP-based web interface. The key feature that sets FOG apart is its ability to deploy images over a network using PXE boot, eliminating the need for physical boot media like USBs or DVDs. Your PCs boot via PXE and automatically downloads a small linux client doing all the hard work of imaging your machine. Also with FOG many network drivers are built into the client's kernel (vanilla linux), so you don't really need to worry about network drivers (unless there isn't kernel support for it yet). FOG also supports putting an image that came from a computer with a 80GB partition onto a machine with a 40GB hard drive as long as the data is less than 40GB. FOG supports multicasting, meaning that you can image many PCs from the same stream. So it should be as fast whether you are imaging 1 PC or 20 PCs.

Features

FOG is more than just an imaging solution, FOG has grown into an imaging/cloning and network management solution.

- PXE boot environment (DHCP, iPXE, TFTP, fast HTTP download of big boot files like kernel and initrd)
- Imaging of Windows (XP, Vista, 7, 8/8.1, 10), Linux and Mac OS X
- Partitions, full disk, multiple disks, resizable, raw
- Snapins to install software and run jobs/scripts on the clients
- Printer management
- Change hostname and join domain
- Track user access on computers, automatic log off and shutdown on idle timeouts
- Disk wiping

What is OpenMediaVault (OMV)?

Openmediavault is the next generation network attached storage (NAS) solution based on Debian Linux. It contains services like SSH, (S)FTP, SMB/CIFS, RSync and many more ready to use. Thanks to the modular design of the framework it can be enhanced via plugins. Openmediavault is primarily designed to be used in small offices or home offices, but is not limited to those scenarios. It is a simple and easy to use out-of-the-box solution that will allow everyone to install and administer a Network Attached Storage without deeper knowledge.

In the context of FOG, OMV is typically used as the **centralized storage backend** housing the system images that FOG accesses during deployment tasks. By using OMV as a separate storage server, organizations can keep deployment logic (FOG) and image storage (OMV) modular and scalable.

Core Protocols and Technologies

A number of core network technologies and protocols are underlying the functioning of FOG and OMV together:

- **PXE (Preboot Execution Environment):** Allows client computers to be booting off the network instead of a local hard disk. PXE boots down instructions from the FOG server to initiate the deployment.

- **TFTP (Trivial File Transfer Protocol):** Employed by the PXE client to transfer bootloader files such as pxelinux.0 or FOG's iPXE binary from the FOG server. It is a very minimal protocol that performs best for early-boot small file transfers.

- **HTTP/FTP:** Both can be used towards the end of deployment for transferring files of additional files, like the FOG imaging kernel or other scripts and utilities. HTTP is generally faster and more reliable than TFTP on newer networks with greater payload.

- **NFS/SMB:** Used by FOG to read image files from OMV. FOG can mount image storage based on configuration either using NFS (usually used in Unix/Linux environments) or SMB (usually used in Windows networks). The protocol impacts performance and access permissions.

Real world applications

In an IT manufacturing environment, FOG Optimization and Troubleshooting are required to enable proper system deployment environments. FOG (Free and Open-source Ghost) is commonly used to image and deploy an operating system across numerous machines, normally in educational or business networks. Troubleshooting on OMV/FOG provides uniformity with mass deployment by identifying faults in terms of imaging failure, failure to network boot, or insufficient permission. Storage and network optimization improves performance, reduces downtime, and increases scalability, and as such is an essential element of IT support services and systems administration.

3 - System requirements

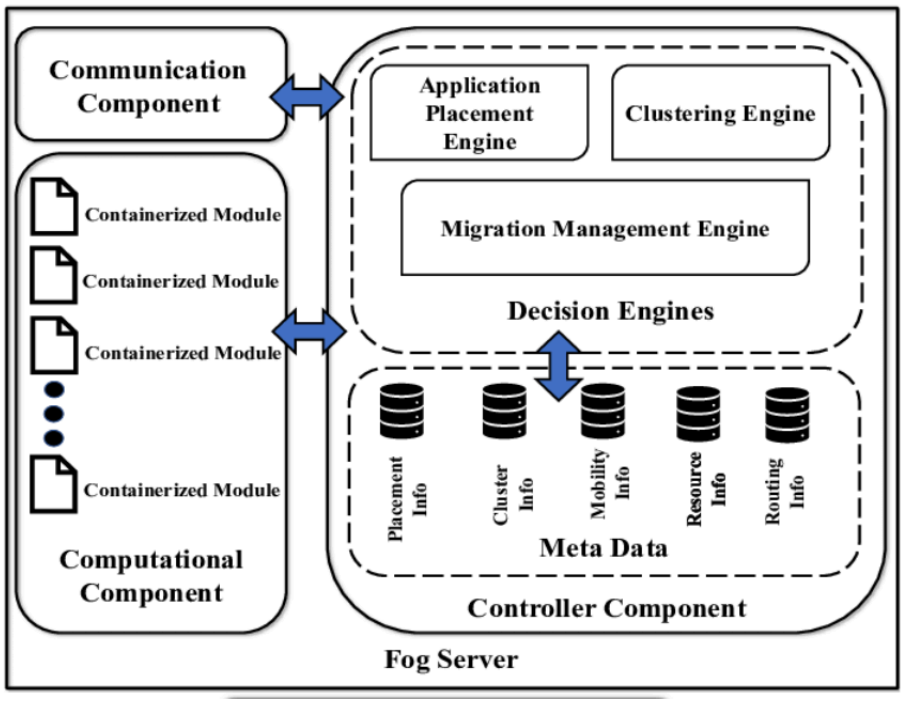
In the successful deployment and hosting of a FOG server, the procedure should begin with a system environment well defined for addressing hardware as well as software requirements. Either on physical devices or virtual configurations is the deployment option with regards to the needs of scalability and flexibility.

Ordinarily, the best suggested is

- a mid-range server
- a dual processor at least
- 4GB of RAM
- Plenty of disk space (**1 TB or more** is strongly recommended)

Particularly if the system needs to be able to host several deployments simultaneously. Operating systems also come into play, FOG itself likes to run most natively under Linux distributions such as Debian or Ubuntu and depends on services like DHCP, TFTP, and Apache in order to run efficiently.

- Ubuntu 16 or higher
- Debian 8 or higher
- CentOS 7 or higher
- Red Hat 6 or higher
- Fedora 22 or higher
- Any version of Arch.



FOG Server Architecture

The FOG server is a multi-component system built on a traditional LAMP stack:

- **Apache Web Server:** Hosts the FOG management interface and handles HTTP requests from clients during deployment.
- **MySQL/MariaDB:** Stores metadata about hosts, images, deployment history, and task scheduling.
- **PHP:** Powers the server-side logic behind the web interface and API.
- **DHCP Server (optional):** FOG can either use an external DHCP server or run its own to assign IP addresses and point clients to the PXE boot files.
- **PXE/iPXE Boot Service:** Facilitates initial network booting by delivering the necessary bootloaders and kernels to the client machine.

These components work together to coordinate image deployment, manage client information, and interface with the storage backend.

4-Installation

After you have taken your Snapshot, start up the machine again and log in with your credentials. Before we can Install FOG Server on Ubuntu Server, we are going to update our system to make sure everything is on the latest patch level.Code language is always Bash.

```
sudo apt-get update
sudo apt-get dist-upgrade -y
```

After you finished the update, let's run:

```
sudo -i
```

So we don't always need to put sudo in front of our commands for now

```
cd /opt/
```

First, navigate to the */opt/* folder so we are not using the root home for downloading and unzipping our FOG Server.
Now we are going to download FOG:

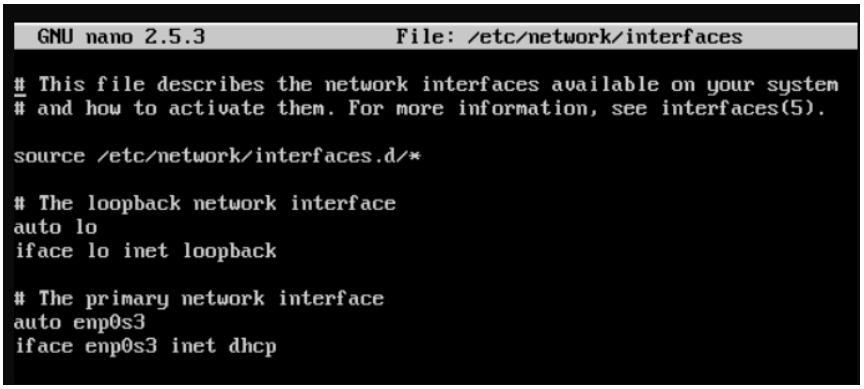
```
git clone https://github.com/fogproject/fogproject.git fogproject-master
```

Now before we are going to Install FOG Server, we are going to change our IP Address, because it gets significantly harder to do that after FOG is installed. Way more things you need to change. If we do it now, we just do it once and the FOG Installation takes over the IP.

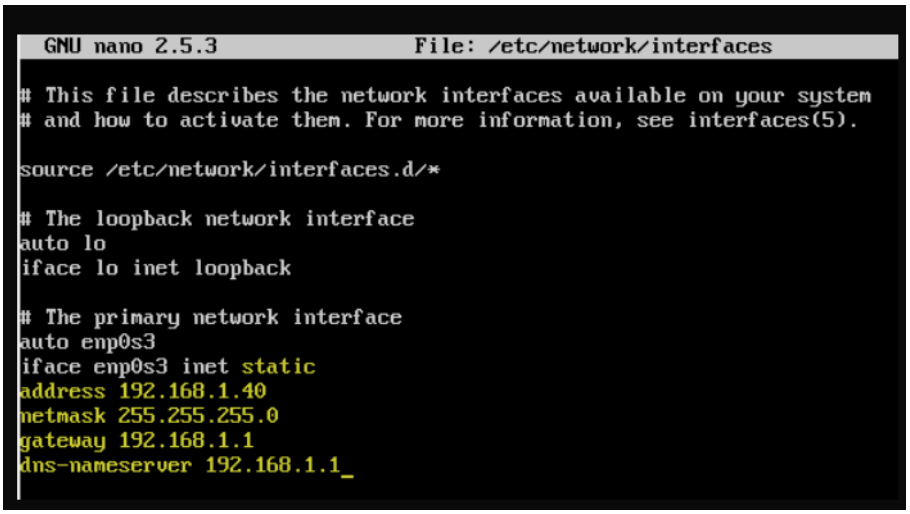
We do this by typing:

```
nano /etc/network/interfaces
```

If you have DHCP activated, you should see something along those lines:



Which we are going to change to look like this:



Of course, adjust according to whatever IP Addresses you are using. Change all the stuff in yellow.

Now press CTRL + O and confirm with Enter to save the file, hit CTRL + X to leave the editor.

Now reboot the Server by typing:

```
reboot now
```

I know you could just restart the networking services, but that failed on me a few times so let's restart to be sure.

After logging back in with your credentials type:

```
sudo -i
cd /opt/fog-master/bin
```

If all is good, we are now ready to Install our FOG Server.

I recommend you take another Snapshot of your VM now while it's running. Just to be safe. Follow through the Snapshot process we covered earlier again and take a new one.

I call it something like: "Before FOG Installation, everything prepared". Simple.

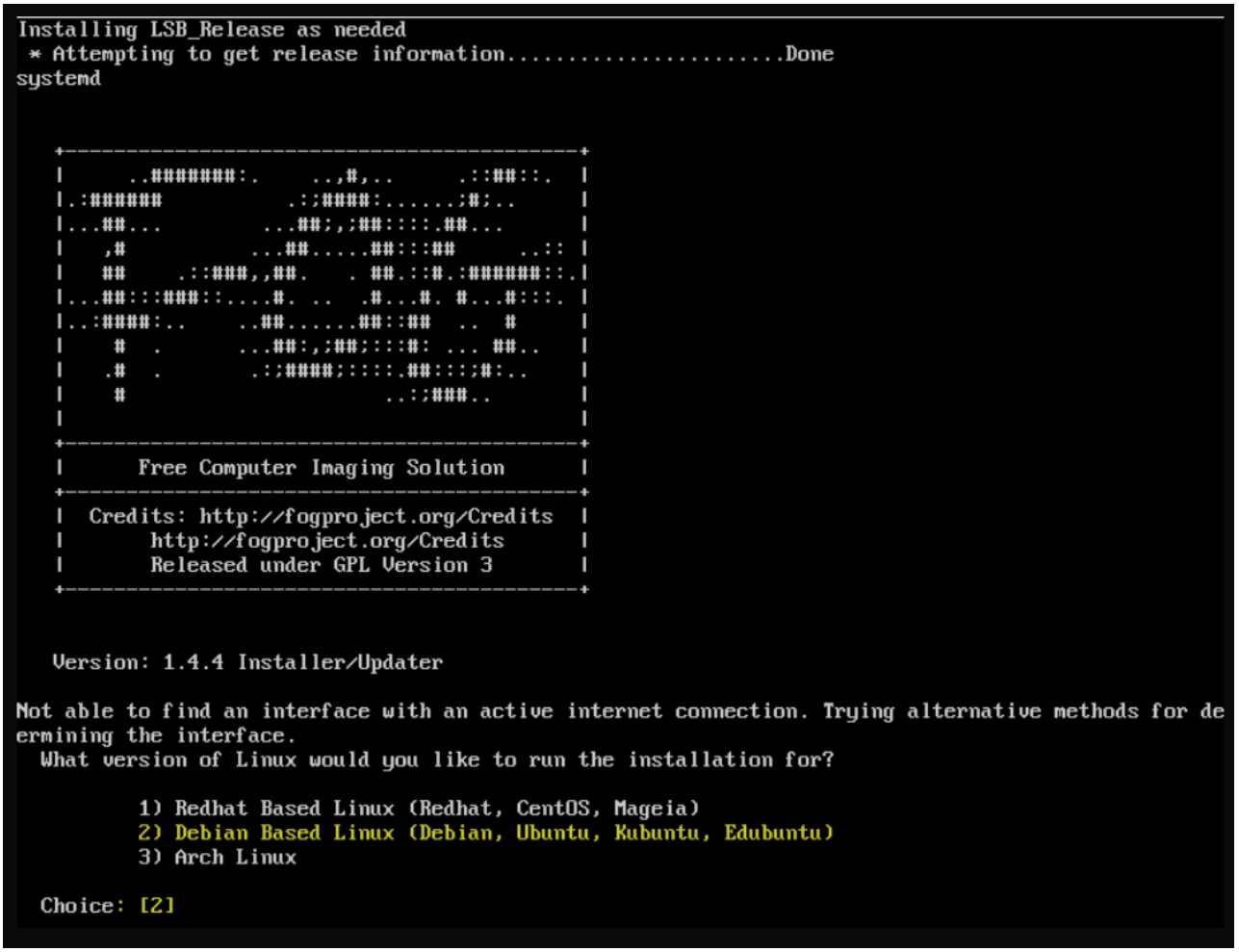
Install FOG Server on Ubuntu Server

As I mentioned in the beginning, our FOG-Server will NOT be installed as a DHCP Server, because our pfSense Firewall will still handle DHCP for us. The setup routine will ask you a few questions and I will exactly tell you what to choose. Follow along carefully as this is a crucial step.

Inside of your `/opt/fog-master/bin` folder type:

`./installfog.sh`

On the first prompt you make the obvious choice: 2 – for Debian Based Linux – Hit Enter.



Next, in my case, I will follow the recommendation of a potential reinstall of Apache and PHP files. So, agree with Y.

Stopping Web Services will likely fail, don't worry about it now.

Now I'll give you a list of questions and answers that the routine will ask you.

- What type of installation would you like to do? [N/s (Normal/Storage)]
- Choose: N
- What is the IP address to be used by this FOG Server? [TheIpYouSetUpEarlier]
- Confirm with Enter
- Would you like to change the default network interface from [YourNetworkInterfaceName]?
- Choose: N
- Would you like to setup a router address for the DHCP Server? [Y/n]
- Choose: Y and enter the IP Address of your Router / DHCP Server
- Would you like DHCP to handle DNS?
- Choose: Y
- What DNS address should DHCP allow? [IP of your Router or DNS Server you use]
- Confirm with Enter or Change the IP Accordingly
- Would you like to use the FOG Server for DHCP Service? [y/N]
- Choose: N
- This version of FOG has internationalization support, would you like to install the additional language packs? [y/N]
- Choose: N, or Yes if you need it.
- Are you sure you wish to continue (Y/N)
- Check if everything is correct and confirm with Y

In some older versions of Ubuntu Server, you will get asked to set a MySQL password in the installation process. I wasn't asked for it in Ubuntu. In case, you can leave it empty and just hit enter without a security risk. You can still change it later, too.

Next, before everything is finished, you get asked to update your Database.

For this you navigate to your FOG Server via a Web Browser of your choice:

http://192.168.1.40(or your FOG SERVER IP)/fog/management/

Log in with the default credentials:

- Username: fog
- Password: password

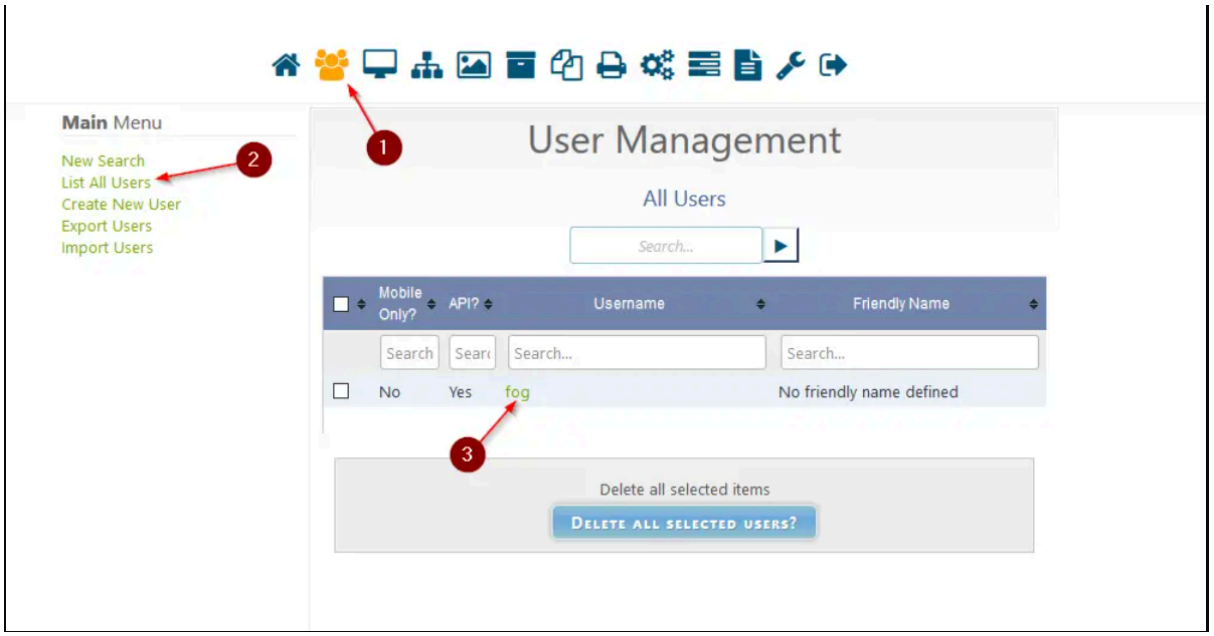
Confirm any prompts to Update the Database before or after logging in. After this is done, confirm that the installation is finished on your FOG Server by pressing Enter.

To give it a fresh start type:

```
reboot now
```

On your FOG Server.

After the Server is back up, log in with the default credentials again via your Web Browser. Navigate to your User Manager and change the default credentials of your fog user.



Congratulations, you just successfully installed your first FOG Server.

5 - Service Testing and Validation

After completing the installation and initial configuration of the FOG server, it is essential to validate that the service functions as intended. This section outlines the steps taken to test core functionalities such as image capture, deployment, and network communication. These tests help ensure system reliability and confirm that FOG can be effectively integrated into real-world IT environments

1. Capture a Base Image from a Client

- Booted the client machine via PXE.
- Selected *"Perform Full Host Registration and Inventory"* to register the device.
- Created a task on the FOG Web Interface: *"Capture Image"*.
- Rebooted the client, which booted into the FOG Preboot Environment and started capturing.

Result: Image captured successfully and saved on the FOG server.

2. Verify File Transfer and Log Outputs

firstly, Checked logs on the server:
`tail -f /opt/fog/log/fog.log`

Then monitored TFTP and NFS services using:

```
systemctl status tftpd-hpa
systemctl status nfs-kernel-server
```

Confirmed file transfers were successful with no dropped packets.

3. Review Web Interface Logs and Status

- Navigated to **FOG Dashboard > Task Management** to confirm task status.
- Checked **Storage Nodes** to verify transfer rates and completion percentages.

Result: All tasks marked as *Complete*, no errors in log summaries.

6 - Common Troubleshooting in OMV and FOG

Importance of Effective Troubleshooting

Effective troubleshooting is essential for maintaining the reliability and performance of both OMV and FOG implementations. Without a structured approach to identifying and resolving issues, organizations may experience extended downtime, data loss, or incomplete system deployments. This report emphasizes practical, experience-based strategies to diagnose and solve problems quickly and efficiently.

Systematic Approach to Problem Solving

Effective troubleshooting follows a structured methodology:

1. **Identify the Problem**: Define the issue clearly, including symptoms and scope
2. **Gather Information**: Collect relevant data, logs, and environmental factors
3. **Analyze the Data**: Look for patterns and potential causes
4. **Develop Hypotheses**: Create theories about what might be causing the issue
5. **Test Hypotheses**: Implement potential solutions one by one
6. **Implement the Solution**: Apply the fix that resolves the issue
7. **Verify the Solution**: Confirm that the problem is resolved and has not created new issues
8. **Document the Process**: Record the problem, solution, and lessons learned

This methodical approach prevents wasted time and ensures that problems are thoroughly resolved rather than temporarily masked.

Documentation Best Practices

Proper documentation is essential for effective troubleshooting:

- **Maintain System Documentation**: Keep updated network diagrams, configuration files, and change logs
- **Issue Tracking**: Record problems, attempted solutions, and outcomes
- **Standard Operating Procedures**: Document routine maintenance and troubleshooting procedures
- **Knowledge Base**: Build a repository of common issues and their solutions
- **Recovery Documentation**: Maintain step-by-step recovery procedures for critical failures

Comprehensive documentation reduces downtime during future incidents and facilitates knowledge transfer between team members.

Backup Strategies

Before attempting any troubleshooting that could affect system configuration or data:

- **Configuration Backups**: Export system configurations regularly
- **Data Backups**: Maintain current backups of all critical data
- **System State Snapshots**: Capture system state before making changes
- **Recovery Testing**: Regularly verify that backups can be successfully restored
- **Incremental Approach**: Make small, reversible changes when possible

These precautions minimize risk and provide fallback options if troubleshooting attempts exacerbate issues.

OMV Common Issues and Solutions

Installation Problems

Common installation issues include:

Problem: Installation Fails with Hardware Detection Errors

- *Cause*: Incompatible hardware or incorrect BIOS settings
- *Solution*: Verify hardware compatibility, update BIOS/UEFI, and disable unnecessary controllers in BIOS

Problem: Web Interface Not Accessible After Installation

- *Cause*: Network configuration issues or service startup failures
- *Solution*: Check network settings, verify service status with `systemctl status nginx php-fpm`, and check logs in `/var/log/nginx/`

Problem: Insufficient Disk Space Errors

- *Cause*: System partition too small for installation requirements
- *Solution*: Ensure system partition has at least 10GB of free space or reinstall with proper partitioning

Web Interface Access Issues

Common web interface problems include:

Problem: "Connection Refused" When Accessing Web Interface

- *Cause*: Web server not running or firewall blocking access
- *Solution*: Check status of nginx and php-fpm services, verify firewall rules, and check for binding issues

Problem: SSL Certificate Warnings

- *Cause*: Self-signed certificates or expired certificates
- *Solution*: Generate new certificates or import proper certificates through the command line

Problem: Slow Web Interface Performance

- *Cause*: Resource constraints or database issues

- *Solution*: Check system resources with `top` or `htop`, optimize database, and clear browser cache

Problem: Session Timeouts

- *Cause*: PHP configuration issues or load balancing problems
- *Solution*: Adjust session timeout settings in PHP configuration or OMV settings

Plugin Installation Failures

Common plugin issues include:

Problem: "Unable to Download Package" Errors

- *Cause*: Repository connectivity issues or plugin incompatibility
- *Solution*: Verify internet connectivity, check compatibility between plugin and OMV version, and update apt repositories

Problem: Plugin Installs But Doesn't Function

- *Cause*: Missing dependencies or configuration errors
- *Solution*: Check system logs for specific errors, install missing dependencies manually, and verify plugin configuration

Problem: Plugins Disappear After System Update

- *Cause*: Version compatibility issues or plugin storage location problems
- *Solution*: Reinstall plugins after updating, verify plugin data location, and check for available updates to plugins

Storage Management Problems

Common storage issues include:

Problem: Disks Not Detected

- *Cause*: Hardware issues, driver problems, or incompatible devices
- *Solution*: Check physical connections, verify disk health with SMART tools, update drivers, and check system logs

Problem: File System Mount Failures

- *Cause*: Corrupted file systems, incorrect mount options, or permission issues
- *Solution*: Run file system checks with appropriate tools (e.g., `fsck`), verify mount options, and check system logs

Problem: RAID Degradation

- *Cause*: Disk failures, connection issues, or software problems
- *Solution*: Replace failed disks, verify connections, check RAID status with `mdadm --detail`, and monitor rebuild progress

Problem: Disk Performance Issues

- *Cause*: Fragmentation, hardware limitations, or configuration problems
- *Solution*: Check disk health, optimize file system settings, and verify proper RAID configuration

OMV Performance Optimization

Resource Monitoring

Effective performance troubleshooting requires comprehensive monitoring:

- **CPU Usage**: Monitor with **`top`**, **`htop`**, or **`mpstat`**
- **Memory Utilization**: Track with **`free`**, **`vmstat`**, or **`htop`**
- **Disk I/O**: Analyze with **`iostat`**, **`iotop`**, or **`dstat`**
- **Network Throughput**: Monitor with **`iftop`**, **`nethogs`**, or **`bmon`**
- **Process Analysis**: Identify resource-intensive processes with **`ps aux`** sorted by resource usage

Establishing baseline metrics during normal operation provides a reference for troubleshooting performance degradation.

System Tuning

Common system tuning strategies include:

Problem: High CPU Usage

- *Cause*: Resource-intensive services, inefficient configurations, or background processes

- *Solution*: Identify high-CPU processes, optimize service configurations, disable unnecessary services, and consider hardware upgrades

Problem: Memory Exhaustion

- *Cause*: Memory leaks, insufficient physical memory, or excessive caching
- *Solution*: Adjust service memory limits, optimize PHP and MySQL memory settings, and consider hardware upgrades

Problem: High Load Average

- *Cause*: I/O bottlenecks, CPU contention, or runaway processes
- *Solution*: Identify bottlenecks with `iotop` and `htop`, optimize I/O operations, and schedule resource-intensive tasks during off-hours

Storage Performance Optimization

Storage optimization techniques include:

Problem: Slow Disk I/O

- *Cause*: Fragmentation, hardware limitations, or configuration issues
- *Solution*: Implement RAID for performance, use SSDs for cache, adjust mount options, and optimize file system parameters

Problem: Slow USB Storage

- *Cause*: USB bus limitations or driver issues
- *Solution*: Use USB 3.0 or higher ports, update drivers, and consider direct SATA connections for critical storage

OMV Security Troubleshooting

Authentication Issues

Common authentication problems include:

Problem: Failed Login Attempts

- *Cause*: Incorrect credentials, account lockouts, or authentication service issues

- *Solution*: Reset passwords, verify account status, and check authentication service logs

Problem: SSH Authentication Failures

- *Cause*: Key permission issues, configuration errors, or service problems
- *Solution*: Verify key permissions, check SSH configuration, and validate user accounts

Problem: Two-Factor Authentication Problems

- *Cause*: Time synchronization issues, configuration errors, or plugin problems
- *Solution*: Verify time synchronization, check plugin configuration, and test with alternate authentication methods

Permission Problems

Common permission issues include:

Problem: Access Denied to Shared Resources

- *Cause*: Incorrect file permissions, ACL issues, or configuration errors
- *Solution*: Verify file system permissions, check ACL settings, and validate share configurations

Problem: Group Permission Issues

- *Cause*: Incorrect group assignments, nested group problems, or configuration errors
- *Solution*: Verify group memberships, check group settings, and validate group-based access controls

SSL/TLS Configuration

Common SSL/TLS issues include:

Problem: SSL Certificate Errors

- *Cause*: Expired certificates, misconfiguration, or trust chain issues
- *Solution*: Renew certificates, verify configurations, and ensure proper certificate chains

Problem: Certificate Verification Failures

- *Cause*: Self-signed certificates, hostname mismatches, or trust issues
- *Solution*: Implement proper certificates, ensure hostname matching, and configure trust relationships

Firewall Configuration

Common firewall issues include:

Problem: Services Inaccessible Due to Firewall

- *Cause*: Restrictive firewall rules or configuration errors
- *Solution*: Verify and adjust firewall rules, check service ports, and test with temporarily disabled firewall

Problem: Port Forwarding Not Working

- *Cause*: Misconfiguration, NAT issues, or upstream firewalls
- *Solution*: Verify port forwarding rules, check NAT configuration, and test with external validators

Problem: IP Blocking Issues

- *Cause*: Overly restrictive rules, fail2ban configurations, or blacklisting
- *Solution*: Audit IP blocking rules, verify fail2ban settings, and implement whitelist exceptions

FOG Common Issues and Solutions

Installation and Setup Problems

Common installation issues include:

Problem: Installation Script Fails

- *Cause*: Missing dependencies, network issues, or permission problems

- *Solution*: Verify prerequisites, check network connectivity, and run with appropriate permissions

Problem: Web Interface Inaccessible After Installation

- *Cause*: Web server configuration, PHP issues, or network problems
- *Solution*: Check web server status, verify PHP configuration, and validate network settings

Problem: Database Connection Errors During Installation

- *Cause*: MySQL/MariaDB configuration issues or credential problems
- *Solution*: Verify database service, check credentials, and validate database permissions

Problem: Missing Dependencies

- *Cause*: Incomplete system preparation or repository issues
- *Solution*: Install required packages, update repositories, and check for compatibility issues

Image Capture Failures

Common image capture issues include:

Problem: Client Cannot Boot to FOG

- *Cause*: PXE configuration issues, DHCP problems, or hardware compatibility
- *Solution*: Verify PXE configuration, check DHCP settings, and test with compatible hardware

Problem: Captured Image Is Incomplete

- *Cause*: File system errors, space limitations, or compression issues
- *Solution*: Check source system file system, ensure adequate storage space, and verify compression settings

Problem: FOG Client Cannot Initiate Capture

- *Cause*: Client configuration issues, communication problems, or permission errors

- *Solution*: Verify client configuration, check connectivity to FOG server, and validate permissions

7 - Best Practice and Security Issues

Secure Configuration Best Practices

- Change Default Credentials: Alter the default FOG web interface login (fog/password) during install time to a secure one-time password.

- Lock Down Web Interface Access: Use firewall config or web server config (such as.htaccess or nginx.conf) to restrict access to the FOG management interface to known trusted IP addresses only.

- Enable HTTPS: Secure the web interface with a Let's Encrypt SSL certificate or an Apache/NGINX self-signed certificate.

- Regular Updates: Update the OS, FOG software, and all dependencies (apache2, php, mysql, etc.) on a regular basis to implement known patch vulnerabilities.

- Disable Unused Services: If your FOG server is not being used as a DHCP server, disable that feature during installation and through system services.

Maintenance Tips

- Take Scheduled Backups: Back up FOG config files, images, and MySQL databases from time to time. Automate backups using mysqldump and rsync.

- Monitor Disk Usage: As imaging is space-intensive, utilize df -h or enable logrotate and notifications for full partitions.

- Check Logs Regularly: Employ tail -f /opt/fog/log/fog.log or read logs from the web UI to identify issues early.

Performance Optimization Notes

- Use SSDs or RAID Storage: For faster imaging and deployment, use SSDs or create software/hardware RAID on the FOG server.

- Enable Multicast Deployments: In large-scale client deployment, use multicast mode to reduce bandwidth usage and accelerate mass deployments.

- Segment Network Traffic: Where feasible, isolate PXE/FOG traffic from production traffic using VLANs or separate switches.

- Adjust TFTP Parameters: Set TFTP block size in /etc/default/tftpd-hpa higher to make PXE boot faster.

Common Nature Misconfigurations in Security to be Remediated

- Failure to update default fog credentials.

- Wide open open access to management portal from any network.
- Running FOG server with excessive root privileges or enabling idle features like built-in DHCP as another server (e.g., pfSense) does it already.
- Saving sensitive images insecurely and unencrypted or unprotected with access controls.

8- Case Study

Enterprise Deployment Issues

Environment:

- 500 node corporate network across multiple buildings
- OMV serving as central file repository and backup target
- FOG managing Windows and Linux workstation deployment
- 10 Gbps core network with 1 Gbps to endpoints

Issues Encountered:

1. Multicast deployments failing across subnets
2. Sporadic image corruption during high-volume deployment
3. Performance degradation on OMV during peak deployment periods
4. Client registration failures in specific network segments

Analysis Process:

1. Network traffic analysis revealed improper multicast forwarding configuration
2. Storage performance monitoring showed I/O contention during parallel operations
3. Network packet capture identified MTU inconsistencies causing fragmentation
4. Service logs revealed resource exhaustion during peak operations

Solutions Implemented:

1. Reconfigured routers and switches for proper multicast forwarding across subnets
2. Implemented I/O scheduling to prioritize critical operations
3. Standardized MTU settings across network infrastructure
4. Added server resources and optimized service configurations
5. Established deployment windows to avoid resource contention

Outcomes:

- Successful multicast deployment across all subnets
- 99.8% deployment success rate for imaging operations

- Minimal impact on OMV performance during deployments
- Consistent client registration across all network segments
- 40% reduction in total deployment time

9 - Conclusion

In this task, we installed, set up, and tested a FOG image server in a physical host machine with Ubuntu 22.04. We initiated system preparation, setting static IP addresses, and installation of FOG through official step-by-step procedure. We tested the service further by imaging and deploying disk images onto client stations, verifying logs, and examining the result from the FOG web interface. We also went over some of the most critical best practices for securing and optimizing the FOG environment. The topic extends to overall network service management since FOG is a key element in centralized client system provisioning, maintenance, and recovery in an IT infrastructure. Proficiency in these tools makes system administrators better equipped to deal with large-scale deployments, with the promise of consistency and reduced downtime—key elements of well-executed and secure enterprise network administration.

References

1. **FOG Project. (n.d.). *FOG Project Wiki*. Retrieved May 12, 2025, from https://wiki.fogproject.org/wiki/index.php?title=Main_PageFOG Project**

2. **FOG Project. (n.d.). *FOG Project GitHub Repository*. GitHub. Retrieved May 12, 2025, from https://github.com/FOGProject/fogproject**

3. **Canonical Ltd. (n.d.). *Configuring networks - Ubuntu Server documentation*. Retrieved May 12, 2025, from https://ubuntu.com/server/docs/configuring-networksUbuntu Documentation+2Ubuntu+2Ubuntu Documentation+2**

4. **Debian Documentation Project. (n.d.). *Debian Reference Manual*. Retrieved May 12, 2025, from https://www.debian.org/doc/manuals/debian-reference/**

5. **Ceos3c. (2022). *Install FOG Server on Ubuntu Server – Ultimate Guide*. Retrieved May 12, 2025, from https://www.ceos3c.com/linux/install-fog-server-ubuntu-server/Ceos3c**