Linux Tips and Tricks

The Linux Tips and Tricks section is a valuable resource for enhancing your Linux operating system knowledge, which is essential for optimizing your experience with FileWave Server, Boosters, and IVS. This section provides a wide range of tips and tricks that cover various aspects of Linux, including system administration, command-line usage, package management, troubleshooting, and security. By familiarizing yourself with Linux best practices, customization options, and efficient workflows, you can improve your proficiency in managing and maintaining your Linux-based FileWave infrastructure. Discover valuable insights to maximize the performance, security, and efficiency of your Linux environment, ultimately enhancing your FileWave deployment.

- How to Disable Apache Version Number Disclosure on FileWave Server
- How to Setup a LAMP Server on a Ubuntu Linux system
- Mount macOS & Windows shares on Debian
- Upgrading or Updating MariaDB on AlmaLinux 9
- Updating CentOS Repo Files After Mirrorlist End of Life

How to Disable Apache Version Number Disclosure on FileWave Server

What

The Apache instance in FileWave can sometimes disclose version numbers in its HTTP response headers. This article outlines the steps to disable this disclosure, thereby enhancing the security of the FileWave Server.

When/Why

This action is recommended when your goal is to improve the security of your FileWave instance. Initially, Apache may disclose specific version information in its responses, like in the example below:

```
Date: Fri, 14 Jul 2023 00:05:55 GMT
Server: Apache/2.4.57 (Unix) OpenSSL/3.0.9 mod_wsgi/4.9.4 Python/3.10
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
Content-Length: 362
```

This information is disclosed when the `HEAD / HTTP/1.0` command is sent to the server (using telnet on port 443). Revealing version numbers can potentially expose the server to targeted attacks, as this information helps attackers focus their efforts. Disabling this function is a recommended best practice in the security community.

How

Please follow the steps below to disable Apache version number disclosure:

1. SSH into your FileWave server. If you are unsure how to do this, please request assistance from FileWave Technical Support.
2. Use a command like `sudo vi /usr/local/filewave/apache/conf/httpd_custom.conf` to open the Apache configuration file in a text editor.
3. Insert these two lines into the configuration file:

   ```
   ServerTokens Prod
   ServerSignature Off
   ```

4. Save the file with the updated lines.
5. Restart Apache with the following command: `fwcontrol apache restart`.

After following these steps, if you run the `HEAD / HTTP/1.0` test (using telnet on port 443), the response from Apache will no longer include specific version numbers. It will look similar to the following:

```
HTTP/1.1 400 Bad Request
Date: Fri, 14 Jul 2023 00:11:38 GMT
Server: Apache
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
Content-Length: 362
```

Related Links:

- FileWave Technical Support

Remember to always prioritize the security of your FileWave instance. If you have further queries or concerns, please don't hesitate to reach out to our Technical Support Team.

How to Setup a LAMP Server on a Ubuntu Linux system

The purpose of this brief guide is to take you through the process of setting up a LAMP (Linux, Apache, MySQL, PHP) server on a local Ubuntu Linux machine or virtual machine.

This will allow you to develop using PHP and MySQL (with phpMyAdmin). This is a common stack that is necessary for Wordpress development.

Install the necessary packages

You will need to install the following packages for the LAMP server. You can install them all at once by separating each package by a space, or one at a time like shown.

I prefer to download one at a time because it is easier to see if there were any errors.

Enter the terminal and type the following:

- `sudo apt-get install apache2`
- `sudo apt-get install php`
- `sudo apt-get install php-mysql`
- `sudo apt-get install mysql-server`

You should then be prompted to set a password for the MySQL root user. After setting the password continue to install:

- `sudo apt-get install libapache2-mod-php`
- `sudo apt-get install php-mcrypt`
- `sudo apt-get install phpmyadmin`

You should then be prompted which server to use. Select Apache by pressing enter. Select no for advanced server setup.

Change permissions to the /var/www/html

In order for PHP scripts and files to be run by the LAMP server they need to be saved in the /var/www/html directory. You can think of this location as your local server.

In order to make changes to this directory we need to change the permissions on it. In the terminal enter the command:

`sudo chown {your ubuntu username} /var/www/html`

Create a symbolic link to phpMyAdmin

By default, phpMyAdmin is installed in the /usr/share/ directory. We need to move it to our local server directory.

We navigate to the server directory that we want the link in by: `cd /var/www/html`

Then create the link by entering the command `ln -s /usr/share/phpmyadmin phpmyadmin`.

Restart Apache and test

Run the following command to restart Apache, setting the changes that were made:

`sudo systemctl restart apache2`

You should then be able to create an info.php file in the /var/www/html directory with this command: `touch /var/www/html/info.php`

In the file type the following php code:

`<?php phpinfo(); ?>`

Then, open a browser and type in localhost/info.php You should see a page from the php file you just wrote that gives you information about php.

Finally, to access phpMyAdmin go to localhost/phpmyadmin in your browser. The default root username is ‘root’ and the password is the password you chose earlier for the MySQL database.

Example Script

```
#!/bin/bash
# This will install Apache / MySQL / PHP on Linux (LAMP)
# It includes ImageMagick and enables .htaccess redirect files
# Many apps use those.

# Update repositories
sudo apt-get update -y

# Upgrade packages
sudo apt-get upgrade -y

# Install packages
sudo apt-get install -y apache2
sudo apt-get install -y php
sudo apt-get install -y php-mysql
sudo apt-get install -y php-cli
sudo apt-get install -y php-gd
sudo apt-get install -y php-curl
sudo apt-get install -y php-zip
sudo apt-get install -y mysql-server
sudo apt-get install -y libapache2-mod-php
sudo apt-get install -y phpmyadmin
sudo apt-get install -y imagemagick
sudo apt-get install -y php-imagick

# Prompt for MySQL root password
echo "Please enter the new password for the MySQL root user:"
read -s root_password

# Change authentication for root user
sudo mysql <<EOF
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY '${root_password}';
FLUSH PRIVILEGES;
EOF

# Enable mod_rewrite
sudo a2enmod rewrite

# Change AllowOverride directive
sudo sed -i 's/AllowOverride None/AllowOverride All/g' /etc/apache2/apache2.conf

# Change permissions to the /var/www/html
sudo chown $USER /var/www/html

# Remove any index.html or index.htm files in /var/www/html/
rm -f /var/www/html/index.htm
rm -f /var/www/html/index.html

# Create a symbolic link to phpMyAdmin
cd /var/www/html
ln -s /usr/share/phpmyadmin phpmyadmin

# Restart Apache
sudo systemctl restart apache2

# Create index.php file
echo "<?php phpinfo(); ?>" > /var/www/html/index.php

# Output completion message
echo "Setup completed. Visit localhost/index.php to check PHP info. Access phpMyAdmin at localhost/phpmyadmin with
the root password you entered."
```

Installing SSL

```
#!/bin/bash
```

```
# Install Certbot and the Certbot Apache plugin
sudo apt-get install -y certbot python3-certbot-apache

# Prompt for the domain name
echo "Please enter the domain name for the SSL certificate:"
read domain_name

# Run Certbot for the domain
sudo certbot --apache -d $domain_name

# Test automatic renewal
sudo certbot renew --dry-run

# Check if ufw is installed
if command -v ufw &> /dev/null
then
    # Allow HTTPS through the firewall
    sudo ufw allow 'Apache Full'
else
    echo "ufw not found. If you have another firewall, please manually open port 443 (HTTPS)."
fi

# Output completion message
echo "SSL setup completed. Visit https://$domain_name to check the SSL status."
```

Mount macOS & Windows shares on Debian

Mount macOS & Windows shares on Debian e.g. in case you need to save backups on a network share.

Step-by-Step Guide for Debian

Mounting Windows Shares

1. Install CIFS Utilities: Open a terminal and install the CIFS utilities package if it's not already installed.

```
sudo apt-get update
sudo apt-get install cifs-utils
```

2. Mount the Windows Share: Use the `mount` command to mount the Windows share. Replace the placeholders with your actual values.

```
sudo mount -t cifs -o username=yourusername,password=yourpassword //yourIPAddress/yoursharedfolder
/yourfoldertomount
```

Mounting macOS Shares

1. Install CIFS Utilities: Ensure the CIFS utilities package is installed (this step is the same as above).

```
sudo apt-get update
sudo apt-get install cifs-utils
```

2. Mount the macOS Share: Use the `mount` command to mount the macOS share. Replace the placeholders with your actual values.

```
sudo mount -t cifs //yourIPAddress/yoursharedfolder /yourfoldertomount -o
username=yourusername,password=yourpassword,nounix,sec=ntlmssp
```

Creating and Sharing a Folder

1. Create a Folder: Create the folder where you want to mount the share.

```
sudo mkdir /yourfoldertomount
```

2. Replace the Placeholder: Replace `yourfoldertomount` with the actual path of the folder you created in the mount commands above.

Example

If you want to mount a Windows share with IP `192.168.1.100` and shared folder name `backup` to a local directory `/mnt/backup`:

1. Create Local Directory:

```
sudo mkdir /mnt/backup
```

2. Mount the Share:

```
sudo mount -t cifs -o username=myuser,password=mypassword //192.168.1.100/backup /mnt/backup
```

Similarly, for a macOS share:

1. Create Local Directory:

```
sudo mkdir /mnt/backup
```

2. Mount the Share:

```
sudo mount -t cifs //192.168.1.100/backup /mnt/backup -o
username=myuser,password=mypassword,nounix,sec=ntlmssp
```

Additional Tips

- FSTAB Entry for Persistent Mounts: To make the mount persistent across reboots, add an entry to `/etc/fstab`:

```
//yourIPAddress/yoursharedfolder /yourfoldertomount cifs
username=yourusername,password=yourpassword,nounix,sec=ntlmssp 0 0
```

- Security Note: Storing passwords in plain text can be a security risk. Consider using a credentials file:

```
//yourIPAddress/yoursharedfolder /yourfoldertomount cifs credentials=/etc/cifs-
credentials,nounix,sec=ntlmssp 0 0
```

And create `/etc/cifs-credentials` with the following content:

```
username=yourusername
password=yourpassword
```

Ensure the credentials file has appropriate permissions:

```
sudo chmod 600 /etc/cifs-credentials
```

CentOS Details

If you are on CentOS and are migrating off of it and need to do it here is the old documentation on this same process:

1. For Linux to Windows:
    1. mount -t cifs -o username=yourusername,password=yourpassword //yourIPAdress/yoursharedfolder /yourfoldertomount
2. For Linux to macOS
    1. sudo yum install cifs-utils
    2. mount -t cifs //yourIPAddress/yoursharedfolder /yourfoldertomount -o username=yourusername,password=yourpassword,nounix,sec=ntlmssp

> Create a folder and share it then replace this value "yourfoldertomount" with the right shared folder name.

Related Content

- FileWave Server Backup and Restore

Upgrading or Updating MariaDB on AlmaLinux 9

What

This article provides a step-by-step guide to upgrading or updating MariaDB on AlmaLinux 9. MariaDB is a popular open-source database management system. Updating to the latest version will ensure optimal performance, security, and compatibility.

When/Why

Updating or upgrading MariaDB on AlmaLinux 9 should be performed when a newer version is available, to improve database operations, add new features, or patch potential vulnerabilities.

How

1. Check Current MariaDB Version on AlmaLinux 9

Check the current MariaDB version and AlmaLinux OS version using the following commands:

```
mysql -V
cat /etc/almalinux-release
```

2. Create a Backup of Existing MariaDB Databases

Create a backup of existing databases:

```
mysqldump -u root -p --all-databases > /tmp/database-backup.sql
cp -a /var/lib/mysql /var/lib/mysql.backup
cp -a /etc/my.cnf /etc/my.cnf_bk
```

3. Uninstall Old MariaDB Repositories

Uninstall the old MariaDB repositories:

```
systemctl stop mariadb
mv /etc/yum.repos.d/mariadb.repo /etc/yum.repos.d/mariadb_bk
dnf update
```

4. Add the new MariaDB Repository on AlmaLinux 9

Create a new repo file for the latest version:

```
vi /etc/yum.repos.d/MariaDB.repo
```

Paste the following contents into the file:

```
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.11/rhel9-amd64
module_hotfixes=1
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

5. Remove Old MariaDB Server

Remove the old MariaDB version:

```
dnf remove mariadb-server
dnf clean all
```

6. Upgrade and Install Latest MariaDB

Install the latest version of MariaDB on your server:

```
dnf install MariaDB-server
dnf install MariaDB-server galera-4 MariaDB-client MariaDB-shared MariaDB-backup MariaDB-common
systemctl start mariadb
systemctl enable mariadb
mysql_upgrade -u root -p
```

Verify your MariaDB version and status:

```
mysql -V
systemctl status mariadb
```

Related Links

- MariaDB Documentation page: https://mariadb.com/kb/en/library/systemd/
- AlmaLinux OS Documentation: https://wiki.almalinux.org/documentation.html

Updating CentOS Repo Files After Mirrorlist End of Life

What

CentOS reached the end of life on June 30, 2024. This will cause issues when attempting to download install packages from repositories. The CentOS mirror list feature allows yum, the package manager, to find and use the nearest and fastest mirror automatically. However, there can be circumstances where disabling this feature is necessary, such as:

Mirror Issues: Sometimes, specific mirrors can be slow, outdated, or unreliable, causing issues with package installations and updates.

When/Why

Since mirrorlist.centos.org no longer exists, you will need to update the repo files on your CentOS server. Follow the steps below to update the repo file accordingly.

How

To resolve the issue, you can mass update all .repo files with the following commands run as root or with sudo when SSH'd to your Server, IVS or Booster:

```
sed -i s/mirror.centos.org/vault.centos.org/g /etc/yum.repos.d/*.repo
sed -i s/^#.*baseurl=http/baseurl=http/g /etc/yum.repos.d/*.repo
sed -i s/^mirrorlist=http/#mirrorlist=http/g /etc/yum.repos.d/*.repo
yum clean all && yum -y update
```

Explanation: The commands provided will perform the following actions:

1. Replace all instances of mirror.centos.org with vault.centos.org in the .repo files.
2. Uncomment (sed -i s/^#.*baseurl=http/baseurl=http/g) the baseurl lines in the .repo files.
3. Comment out (sed -i s/^mirrorlist=http/#mirrorlist=http/g) the mirrorlist lines in the .repo files.

Related Content

- mirrorlist.centos.org error
- FileWave Server on CentOS - EOL