**Package Updates**

* **Purpose:** Keep the system and installed software up-to-date to ensure stability, new features, and security patches.
* **Commands:**

bash

Copy code

# Update all installed packages

sudo yum update -y

# Upgrade specific packages

sudo yum upgrade httpd -y

# List installed packages

yum list installed

# Install a new package (e.g., nginx)

sudo yum install nginx -y

# Remove a package

sudo yum remove nginx -y

* **Example:** To update the system and install the latest Apache HTTP server:

bash

Copy code

sudo yum update -y

sudo yum install httpd -y

**2. Service Management**

* **Purpose:** Start, stop, enable, or check the status of services running on the system.
* **Commands:**

bash

Copy code

# Start a service (e.g., Apache)

sudo systemctl start httpd

# Stop a service

sudo systemctl stop httpd

# Restart a service

sudo systemctl restart httpd

# Check service status

sudo systemctl status httpd

# Enable service to start on boot

sudo systemctl enable httpd

# Disable service from starting on boot

sudo systemctl disable httpd

* **Example:** To ensure the Apache server starts automatically after a reboot:

bash

Copy code

sudo systemctl start httpd

sudo systemctl enable httpd

**3. System Security**

* **Purpose:** Protect the system from unauthorized access and ensure compliance with security best practices.
* **Tasks and Commands:**

**a. User Management**

bash

Copy code

# Add a new user

sudo useradd username

# Set a password for the user

sudo passwd username

# Delete a user

sudo userdel username

**b. SELinux (Security-Enhanced Linux)**

bash

Copy code

# Check SELinux status

sestatus

# Temporarily disable SELinux (for troubleshooting)

sudo setenforce 0

# Permanently disable SELinux

sudo sed -i 's/SELINUX=enforcing/SELINUX=disabled/' /etc/selinux/config

**c. Firewall Management**

bash

Copy code

# List active firewall rules

sudo firewall-cmd --list-all

# Add a service (e.g., HTTP)

sudo firewall-cmd --permanent --add-service=http

# Reload the firewall

sudo firewall-cmd --reload

**d. SSH Security**

bash

Copy code

# Restrict SSH root login

sudo sed -i 's/^PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd\_config

# Restart SSH service to apply changes

sudo systemctl restart sshd

# Generate SSH key

ssh-keygen -t rsa -b 4096

* **Examples:**
  1. **Harden SSH Access:** Restrict root login and enforce key-based authentication:

bash

Copy code

sudo sed -i 's/^PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd\_config

sudo systemctl restart sshd

* 1. **Configure Firewall for Apache:** Allow HTTP traffic and reload the firewall:

bash

Copy code

sudo firewall-cmd --permanent --add-service=http

sudo firewall-cmd --reload

**Workflow Example:**

1. **Update the System and Software:**

bash

Copy code

sudo yum update -y

sudo yum install httpd -y

1. **Start and Enable Apache Service:**

bash

Copy code

sudo systemctl start httpd

sudo systemctl enable httpd

1. **Secure the System:**
   * Restrict SSH root login:

bash

Copy code

sudo sed -i 's/^PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd\_config

sudo systemctl restart sshd

* + Enable firewall for HTTP traffic:

bash

Copy code

sudo firewall-cmd --permanent --add-service=http

sudo firewall-cmd --reload

By following these commands and tasks, you can effectively manage RHEL systems while ensuring their security and functionality.