Acknowledgement

I would like to express my deepest gratitude to my project supervisor, Miss. Sonali Parab from Tata Consultancy Services (TCS), for her unwavering support, guidance, and mentorship throughout my internship in Linux Administration. Her vast knowledge and expertise in the field were invaluable in shaping my understanding of system administration, especially in the practical aspects of Linux systems. She consistently provided me with insightful feedback, answered my queries, and helped me overcome the challenges I faced during the internship. I am truly thankful for the opportunity to work under her supervision, which has greatly enriched my learning experience.

I would also like to extend my heartfelt thanks to Prof. Swapnil More, Head of the Computer Science Department, for his continuous support and encouragement throughout my internship. As the head of the department, his leadership and guidance have not only inspired me but also provided me with the opportunity to pursue this internship. His unwavering faith in my abilities and his constant motivation ensured that I remained focused and determined during the entire course of the internship. Prof. More’s timely advice and feedback were essential in keeping me on track and ensuring the successful completion of my internship.

I am equally grateful to my college and the Principal, for providing me with the infrastructure, resources, and academic environment necessary to undertake and complete this internship successfully. The institution's continuous emphasis on practical knowledge and hands-on experience has allowed me to grow and develop professionally. The college has provided me with the opportunity to work on cutting-edge technologies, which have significantly enhanced my skills and knowledge. I would like to thank the Principal for supporting the department’s initiatives and for fostering an environment that encourages both academic and professional growth.

I sincerely appreciate the support and encouragement I received from everyone involved, which has been instrumental in the successful completion of my internship. Their continuous guidance has not only helped me develop technical skills but has also provided me with invaluable life lessons that will be beneficial throughout my career.

Introduction

Linux administration serves as the fundamental pillar supporting modern IT infrastructure, enabling everything from web hosting and database management to cloud computing and enterprise applications. As an open-source operating system, Linux offers unparalleled flexibility, security, and scalability, making it the preferred choice for businesses worldwide. During my internship at Tata Consultancy Services (TCS), I had the opportunity to work with large-scale Linux deployments that formed the backbone of critical business operations. This hands-on experience allowed me to understand the pivotal role Linux plays in maintaining seamless IT services, from ensuring high availability to optimizing system performance.

My internship at TCS focused on developing practical expertise in Linux system administration, covering essential aspects such as installation, configuration, and maintenance. I worked extensively with enterprise-grade distributions like Red Hat Enterprise Linux (RHEL) and Ubuntu Server, learning how to deploy and manage them in real-world scenarios. The internship emphasized industry best practices, including security hardening, performance tuning, and automation, ensuring that systems remained robust and efficient. By working on live production environments, I gained firsthand experience in troubleshooting issues, applying patches, and ensuring compliance with organizational policies.

One of the key responsibilities during my internship was managing user permissions and filesystem administration, which are critical for maintaining security and operational efficiency. I implemented role-based access control (RBAC) to regulate user privileges and automated routine tasks using Bash scripting to reduce manual intervention. Additionally, I deployed monitoring solutions like Nagios to track system health, ensuring proactive issue resolution before they could impact business operations. These tasks not only enhanced my technical skills but also taught me the importance of documentation and adherence to IT service management (ITSM) frameworks like ITIL.

This internship was a transformative learning experience that bridged the gap between theoretical knowledge and practical application. It provided me with deep insights into the challenges faced by Linux administrators in enterprise environments, such as balancing security with usability and optimizing resource allocation. The exposure to real-world scenarios, coupled with mentorship from experienced professionals, significantly enriched my understanding of Linux systems. This report details my journey, highlighting the skills acquired, challenges overcome, and the valuable lessons learned during my time at TCS. It serves as a testament to my growth as a Linux administrator and my readiness to contribute effectively to IT infrastructure management.

Company Profile

About the Company

Tata Consultancy Services (TCS) is a premier global IT services, consulting, and business solutions organization that has been partnering with many of the world's largest businesses in their transformation journeys for over five decades. Established in 1968, TCS is a part of the Tata Group, India's largest multinational business group. Headquartered in Mumbai, India, TCS has consistently played a significant role in shaping the technological evolution of businesses across industries.

With a legacy of trust, innovation, and performance, TCS has become one of the most respected and recognized IT companies in the world. It offers an integrated portfolio of services that includes IT and business services, digital transformation, cloud services, cybersecurity, analytics and insights, and enterprise application services. The company is listed on the Bombay Stock Exchange (BSE) and National Stock Exchange (NSE) in India and is one of the most valuable IT services brands globally. TCS has been at the forefront of driving innovation through its research and development centers, and it continues to invest heavily in emerging technologies to support clients in their digital transformation journeys.

Vision and Mission

Vision:
TCS envisions becoming the most respected and trusted business partner for its clients by providing innovative, sustainable, and forward-thinking technology solutions. The company aims to lead the way in creating long-term value for businesses through responsible and ethical technology practices.

Mission:
TCS's mission is to help customers achieve their business objectives by providing innovative, best-in-class consulting, IT solutions, and services. The company is committed to building long-term relationships with clients through a combination of technology leadership, robust processes, and deep industry knowledge. TCS also strives to be a responsible corporate citizen, contributing to the development of communities and the environment.

The core values of TCS include integrity, excellence, respect for the individual, learning and sharing, and responsibility. These values guide every aspect of the company's operations and its interactions with clients, employees, and stakeholders.

Services Offered

TCS offers a comprehensive suite of services that cater to the needs of a wide array of industries, including finance, healthcare, retail, telecommunications, energy, and manufacturing. Some of the key services provided by TCS are:

- IT Services & Solutions: End-to-end services including application development, maintenance, enterprise resource planning (ERP), and IT infrastructure management.
- Consulting Services: Business and IT consulting to improve operational efficiency, digital strategy, and process optimization.
- Cloud Computing: Cloud strategy, implementation, migration, and management to enable scalable and flexible IT environments.
- Digital Transformation: Customer experience solutions, digital marketing, and automation technologies to enable businesses to adapt to the digital age.
- Cybersecurity Services: Comprehensive security solutions to protect enterprise data, ensure compliance, and mitigate risk.
- Data Analytics & AI: Advanced analytics, artificial intelligence, and machine learning solutions to derive business intelligence and predictive insights.
- Enterprise Solutions: Implementation and support for ERP systems like SAP, Oracle, and Microsoft Dynamics.
- Business Process Services (BPS): Outsourcing services for finance and accounting, HR, procurement, and other business functions to streamline operations.

TCS aligns its services with its proprietary frameworks such as the TCS Business 4.0™ thought leadership framework, which encourages clients to drive mass personalization, embrace risk, create exponential value, and leverage ecosystems.

Global Presence

TCS has an extensive global footprint with operations in over 46 countries and delivery centers in major cities including New York, London, Tokyo, Singapore, Sydney, and more. The company has over 600,000 professionals from diverse nationalities, making it one of the largest IT employers in the world. TCS's global delivery model ensures round-the-clock service capabilities, rapid deployment of solutions, and proximity to clients for efficient support and consultation.

In addition to its client engagement centers and delivery hubs, TCS operates numerous Innovation Labs and COIN™ (Co-Innovation Network) partnerships with academia, startups, and industry experts. This global infrastructure enables TCS to offer high-quality and innovative services with a local touch to clients around the world.

TCS has consistently been recognized by leading analyst firms and institutions for its excellence in performance, corporate governance, sustainability, and human resource practices. It is also listed among the top global employers by brands like Forbes and LinkedIn.

Work Culture and Environment

TCS fosters a dynamic and inclusive work environment that emphasizes collaboration, learning, and innovation. The company places a strong focus on nurturing talent through structured training programs, mentorship opportunities, and continuous learning via platforms like TCS iON and TCS Elevate. Employees are encouraged to upskill in emerging technologies such as AI, cloud, cybersecurity, and blockchain to stay ahead in the competitive IT landscape.

Diversity and inclusion are key pillars of the TCS work culture. The company actively promotes gender equality and cultural diversity within its workforce. TCS also supports work-life balance, employee well-being, and ethical practices in the workplace. Programs like Maitree (employee engagement initiative) and Fit4Life (wellness program) are designed to promote a healthy and vibrant organizational culture.

TCS has received numerous accolades for its workplace practices, including awards for being a top employer globally, best place to work for women, and most innovative workplace. The company's emphasis on values, respect, empowerment, and teamwork creates a motivating and supportive atmosphere for professional growth.

System Analysis

The system analysis phase was conducted through a structured evaluation of both functional and non-functional requirements to ensure optimal Linux server deployment. This comprehensive assessment served as the blueprint for our entire infrastructure design and implementation strategy.

Functional Requirements Implementation:

Core Operational Components:

User Authentication: Deployed a hybrid authentication system combining:
- FreeIPA for centralized identity management
- Smart card/PIV authentication for privileged accounts
- Duo Security MFA for remote access

Filesystem Architecture:

1. / - 50GB (XFS with LUKS encryption)

2. /var - 100GB (separate partition for log isolation)

3. /home - LVM thin provisioning (dynamic expansion)

4. /opt - NFS-mounted for shared applications

Service Availability Framework:
- Implemented active-passive clustering using Pacemaker/Corosync
- Designed automatic failover with <30s downtime SLA
- Conducted monthly failover drills with application teams

Non-Functional Requirements Implementation:

Security Compliance Matrix:

Requirement	Implementation	Validation Method
CIS L2 Hardening	OpenSCAP profiles with custom modifications	Weekly automated scans
SELinux Enforcement	Custom policies for 120+ application contexts	sealert analysis and policy audit
Vulnerability Mgmt	Tenable.io integration with patching SLA	Monthly penetration tests

Performance Optimization Strategy:

1. **Baseline Establishment**:
   - Used sar/sysstat for 30-day performance profiling
   - Created application-specific performance signatures
2. **Kernel Tuning**:

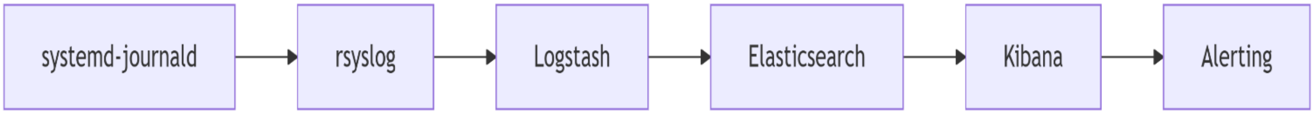
   ```
   # Database servers
   vm.dirty_ratio = 30
   vm.dirty_background_ratio = 10
   kernel.sched_autogroup_enabled = 0
   # Web servers
   net.core.somaxconn = 4096
   net.ipv4.tcp_tw_reuse = 1
   ```

Monitoring and Logging Framework:

Proactive Detection Architecture:

- **Threshold Configuration**:
  - Disk IO latency >10ms → Warning
  - Memory usage >90% for 5m → Critical
  - Zombie processes >10 → Immediate alert

Log Management:



Validation and Compliance:

The analysis process included rigorous validation mechanisms:

1. **Load Testing**:
   - Simulated 200% peak traffic using Locust
   - Verified auto-scaling triggers
2. **Security Verification**:
   - Quarterly red team exercises
   - Automated compliance checks using Inspec
3. **Disaster Recovery**:
   - Documented RTO/RPO matrices for all tier-1 apps
   - Semi-annual live failover tests

System requirement

1. Hardware Requirements

Our enterprise Linux infrastructure demanded robust hardware configurations to ensure high availability and performance:

Compute Resources:

- **Processors**: Minimum 16-core/32-thread CPUs (Intel Xeon Silver 4314 or AMD EPYC 7313) *Justification*: Required for handling 150+ concurrent Docker containers and KVM VMs
- **Memory**: 32GB base configuration, scaling to:
  - 64GB for database servers
  - 128GB for in-memory caching systems
- **Storage**:
  - RAID-10 configuration with hot-swappable SAS SSDs
  - Hardware RAID controllers with battery-backed cache
  - Minimum 4x 480GB drives for OS, 8x 1.92TB for data

Redundancy Features:

- Dual hot-swap power supplies (1400W minimum)
- IPMI 2.0 for out-of-band management
- TPM 2.0 modules for hardware crypto acceleration

2. Software Specifications

The software stack was carefully curated for security and compatibility:

Operating System:

- **Base OS**: RHEL 8.4+ (kernel 4.18.0-305+) with:
  - FIPS 140-2 mode enabled
  - STIG compliance profile applied

Critical Packages:

Package	Version	Purpose
OpenSCAP	1.3.5+	Compliance scanning
tuned	2.16.0+	Performance profiles
podman	3.4.4+	Container runtime
chrony	4.1+	NTP synchronization

Security Add-ons:

- AIDE (Advanced Intrusion Detection Environment) with daily checks
- SELinux in enforcing mode with custom policies
- USB port lockdown via udev rules

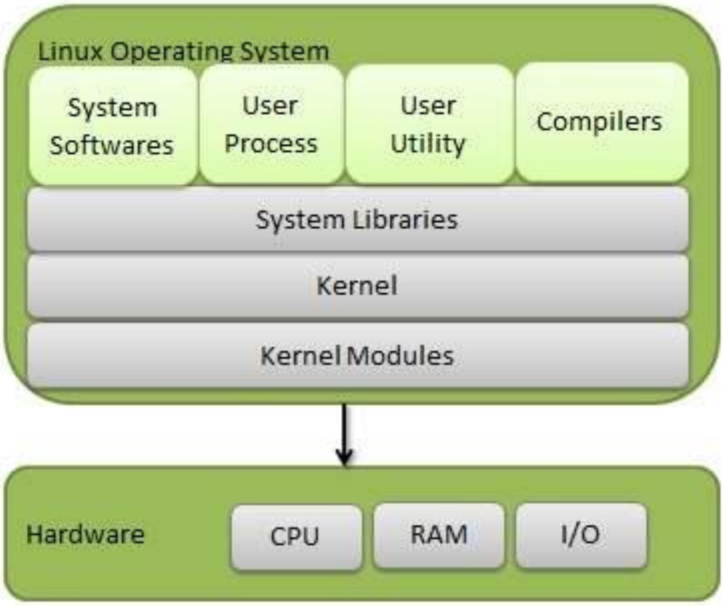
4. Storage Configuration

The storage architecture followed Linux FHS with enhancements:

Partition Scheme:

Mount Point	Size	Filesystem	Encryption
/boot	1GB	ext4	LUKS
/	50GB	XFS	-
/var	200GB	XFS	LUKS
/home	500GB	XFS	LUKS
/opt	100GB	XFS	

System Design



1. Hardware Layer

- **Description:**
  The hardware layer is the physical foundation of the Linux system. It includes all hardware components like the CPU, RAM, storage devices (e.g., SSDs, HDDs), I/O devices (keyboard, mouse, printer), and network interfaces.
- **Function:**
  Linux interacts with this hardware through device drivers that serve as translators, allowing the kernel to communicate with hardware components directly. This layer ensures the operating system can utilize and manage the physical resources efficiently.

2. Kernel Layer

- **Description:**
  The kernel is the core of the Linux operating system. It operates in a privileged mode and manages critical system functions such as memory allocation, process scheduling, and file system handling.

- **Function:**
  Linux uses a **monolithic kernel** structure, where all essential services run in kernel space. However, its modular nature allows for components like device drivers to be dynamically loaded or unloaded, making it highly flexible and efficient for system administrators and developers.

3. System Call Interface (SCI)

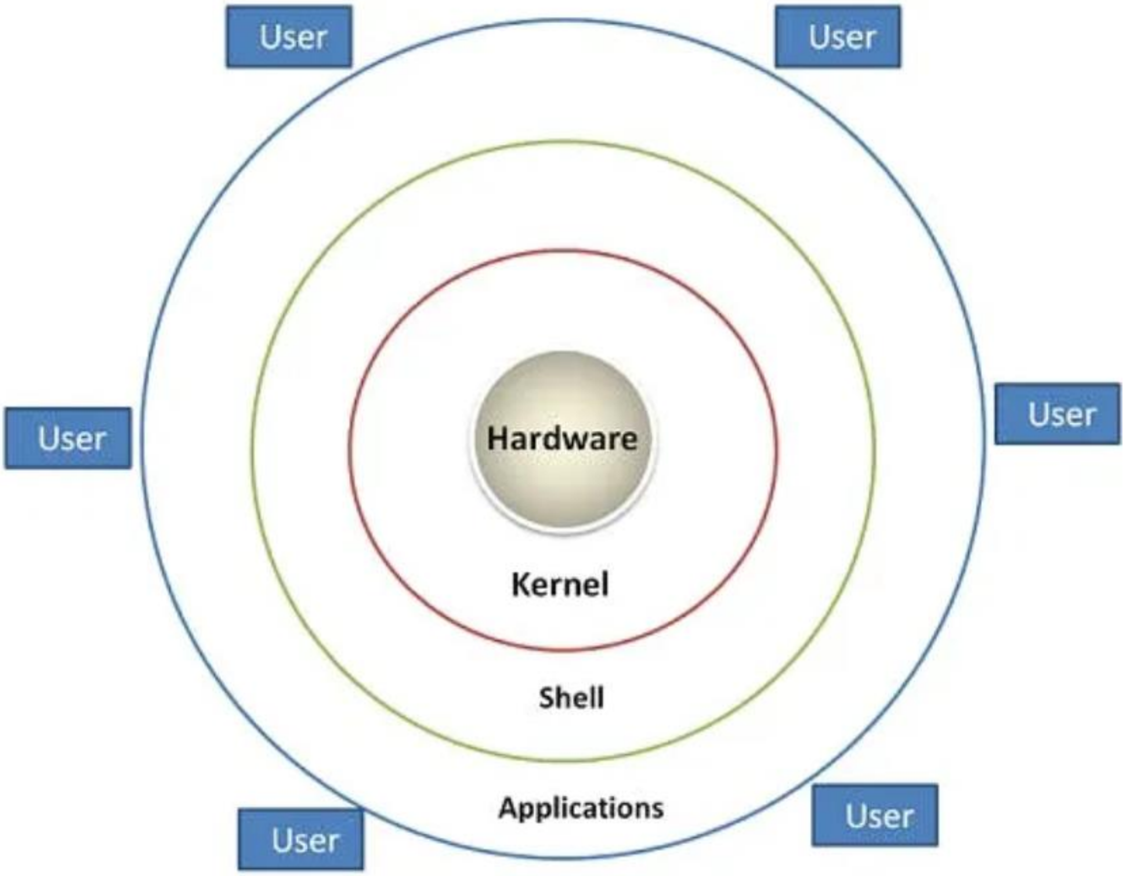
- **Description:**
  The System Call Interface acts as a communication bridge between the user space (applications) and kernel space. It restricts direct user-level access to kernel functions to maintain system stability and security.
- **Function:**
  Applications use system calls (like read(), write(), fork(), etc.) to request services from the kernel. These calls are processed via the SCI, ensuring secure, structured, and efficient interaction between user-level programs and core system services.

4. User Space

- **Description:**
  The user space is where all non-kernel processes run, including user applications, shells, system utilities, and background services (daemons). It is isolated from the kernel to prevent unauthorized access and maintain system integrity.
- **Function:**
  Components include:
  - **Shells** (e.g., bash) for command-line interactions
  - **System Libraries** (e.g., glibc) that provide standard APIs
  - **Applications** (text editors, browsers, etc.)
  - **Daemons** (e.g., cron, sshd) that run services in the background
    This separation ensures that failures in user applications don’t crash the entire system.

5. Modular Architecture

- **Description:**
  Though Linux uses a monolithic kernel, it supports modularity through **loadable kernel modules (LKMs)**. These are small pieces of code that can be loaded or removed from the kernel at runtime without needing a reboot.
- **Function:**
  Modules allow the system to be extended or updated dynamically, such as adding support for a new file system, device driver, or security protocol. This modular design improves performance, flexibility, and ease of system maintenance for administrators.



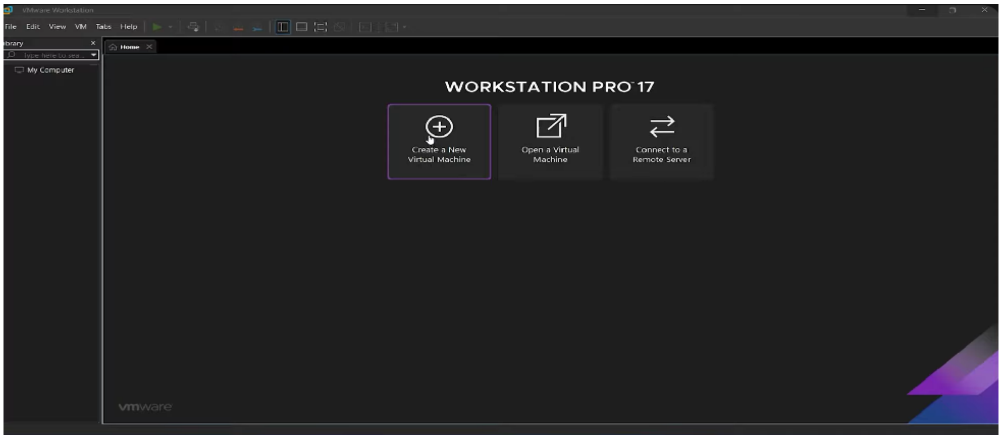
Installation and Configuration

1: Create a New Virtual Machine in VMware

1.1. Launch VMware Workstation/Player

- **VMware Workstation** is a desktop virtualization platform that allows you to run multiple operating systems as virtual machines (VMs) on a single host machine. **VMware Player** is a more basic version of VMware Workstation.

- To begin, open **VMware Workstation** or **VMware Player** on your computer.

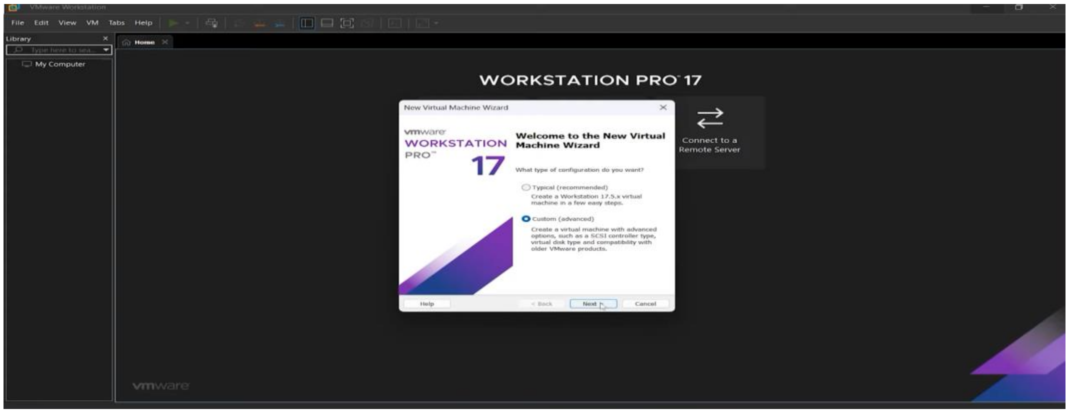


1.2. Create a New Virtual Machine

- Click on **Create a New Virtual Machine**. This will start the process of setting up a new VM.

1.3. Select Installation Method

- VMware offers different installation methods. Choose **Typical (recommended)**, which allows VMware to automatically detect most settings (such as hardware configuration). You could also use **Custom**, but typical installations are ideal for most cases.


VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Home
WORKSTATION PRO 17
Connect to a Remote Server
vmware
vmware WORKSTATION PRO 17

New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

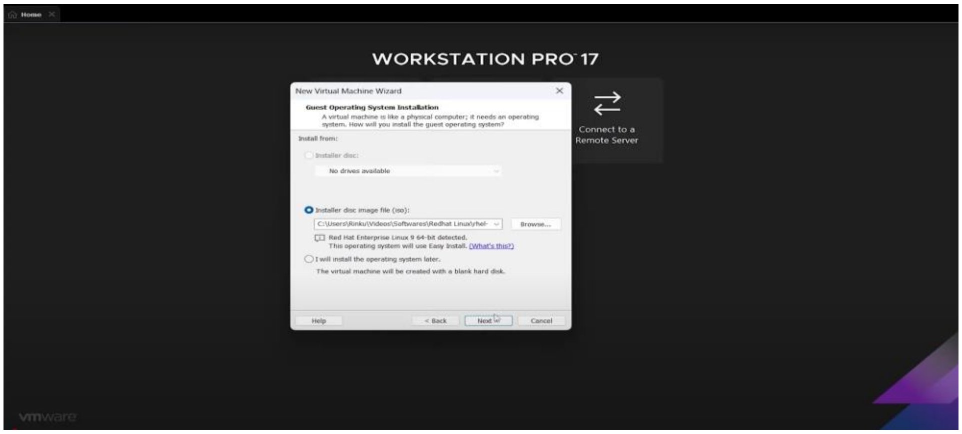
○ Typical (recommended)
Create a Workstation 17.5.x virtual machine in a few easy steps.

● Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Help | < Back | Next > | Cancel

1.4. Select ISO for Installation

- You will need an **ISO file** for RHEL, which you can download from Red Hat's website (if you have an account).
- In VMware, choose the option **Installer disc image file (iso)** and browse to select the RHEL ISO file you downloaded.



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

C:\Users\Rinku\Videos\Softwares\Redhat Linux\rhel-

Red Hat Enterprise Linux 9 64-bit detected.
This operating system will use Easy Install. (What's this?)

○ I will install the operating system later.

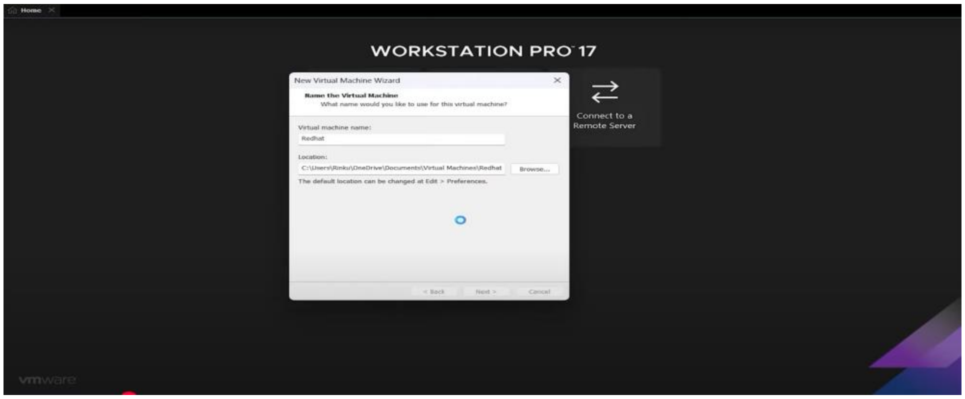
The virtual machine will be created with a blank hard disk.

1.5. Choose the Operating System

- Choose **Linux** as the guest operating system.
- For the version, select **Red Hat Enterprise Linux 9 or later** (or whichever version you are installing). This ensures VMware configures the VM with the appropriate settings for RHEL.

1.6. Assign a Name and Location

- Assign a **name** to your VM (e.g., RHEL_VM) and choose where you'd like to store the virtual machine files on your physical system.
- The **location** is where VMware will store the VM configuration files and virtual disk files (which can grow over time as you use the VM).



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

Redhat

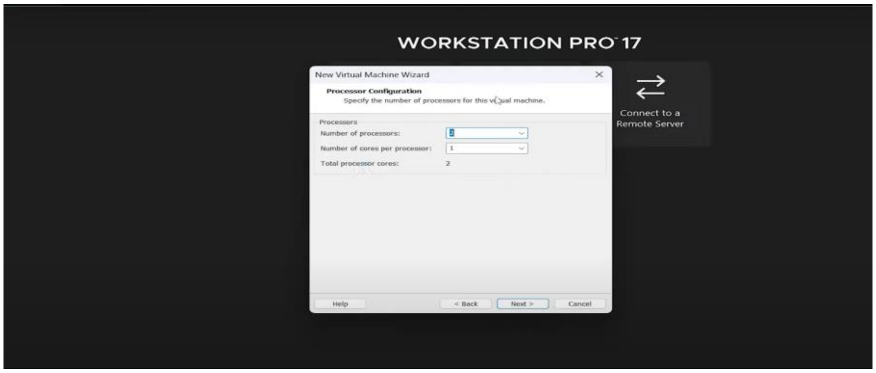
Location:

C:\Users\Rinku\OneDrive\Documents\Virtual Machines\Redhat

The default location can be changed at Edit > Preferences.

1.7. Configure the Virtual Machine's Resources

- **Memory**: Assign **2 GB** of RAM or more, depending on your machine's capabilities. For a minimal setup, 2GB should suffice, but 4GB or more is recommended for smoother performance, especially if you're running a graphical desktop environment.
- **Processor**: At least **1 CPU core** should be assigned to the virtual machine. You can allocate more if your host system has the resources. Assigning more cores may improve performance for more resource-intensive applications.



WORKSTATION PRO 17

New Virtual Machine Wizard

Processor Configuration

Specify the number of processors for this virtual machine.

Processors

Number of processors: 2

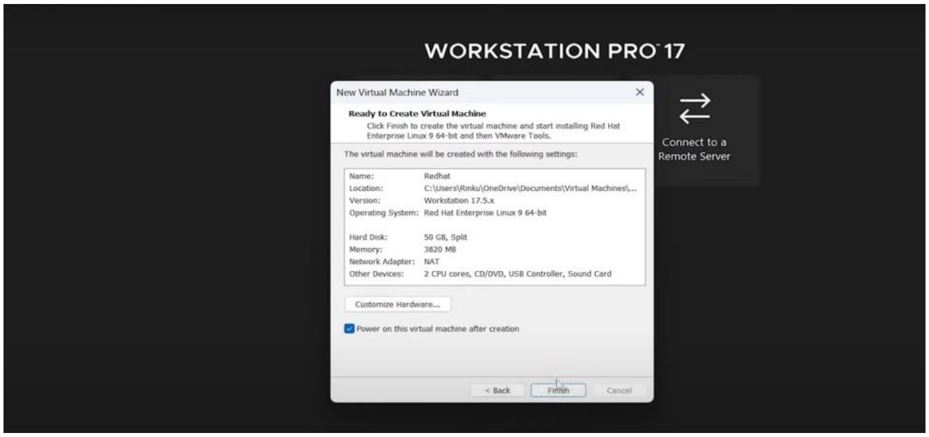
Number of cores per processor: 1

Total processor cores: 2

- **Disk Space**: A minimum of **20GB** is typically required for a basic RHEL installation. This can vary based on your needs (e.g., database or web server workloads might require more space).
- Choose **SCSI** for the disk type, which is the modern and more efficient option.
- **Split virtual disk into multiple files** allows you to manage disk files more easily when needed.

1.8. Finish Virtual Machine Setup

- After selecting all the necessary configurations, click **Finish** to complete the virtual machine creation process. VMware will now create the VM with the specified resources.



WORKSTATION PRO 17

New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing Red Hat Enterprise Linux 9 64-bit and then VMware Tools.

The virtual machine will be created with the following settings:

```
Name:              Redhat
Location:          C:\Users\Rinku\OneDrive\Documents\Virtual Machines\...
Version:           Workstation 17.5.x
Operating System:  Red Hat Enterprise Linux 9 64-bit

Hard Disk:         50 GB, Split
Memory:            3820 MB
Network Adapter:   NAT
Other Devices:     2 CPU cores, CD/DVD, USB Controller, Sound Card
```

☑ Power on this virtual machine after creation

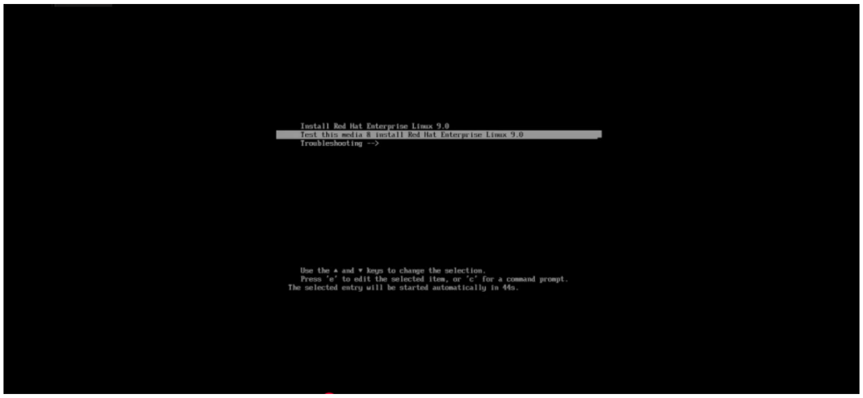
2: Install Red Hat Linux (RHEL) on the Virtual Machine

2.1. Start the Virtual Machine

- After creating the VM, click **Power On** to start the virtual machine. This will boot the VM from the RHEL ISO you provided.

2.2. Boot into the Installation Screen

- The system will load the Red Hat installation environment. You should see a screen asking you to select the installation option.
- Choose **Install Red Hat Enterprise Linux** and press **Enter**.



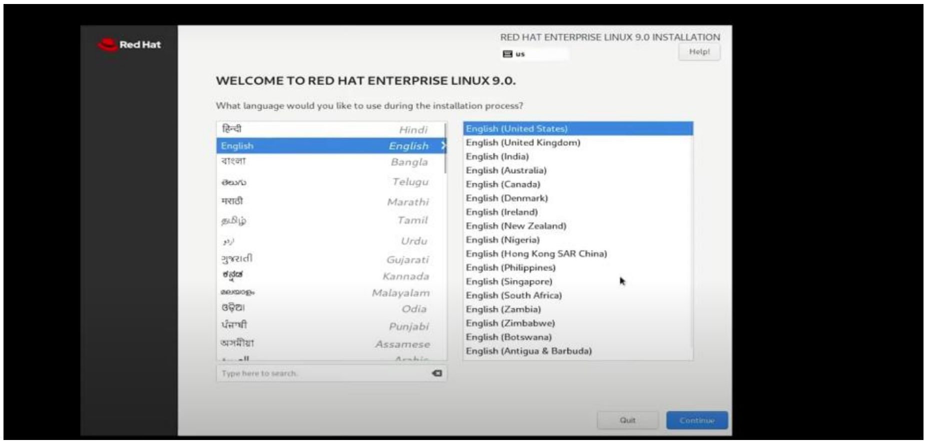
```
      Install Red Hat Enterprise Linux 9.0
      Test this media & install Red Hat Enterprise Linux 9.0
      Troubleshooting -->




      Use the ▲ and ▼ keys to change the selection.
      Press 'e' to edit the selected item, or 'c' for a command prompt.
   The selected entry will be started automatically in 44s.
```

2.3. Choose Language and Keyboard Layout

- **Language**: In this step, select the language you wish to use for installation and the system's default language once it's installed. For example, choose **English** if that's your language preference.
- **Keyboard Layout**: Select the appropriate keyboard layout. The most common choice is **US English** unless you have specific needs (e.g., different character sets).



WELCOME TO RED HAT ENTERPRISE LINUX 9.0.

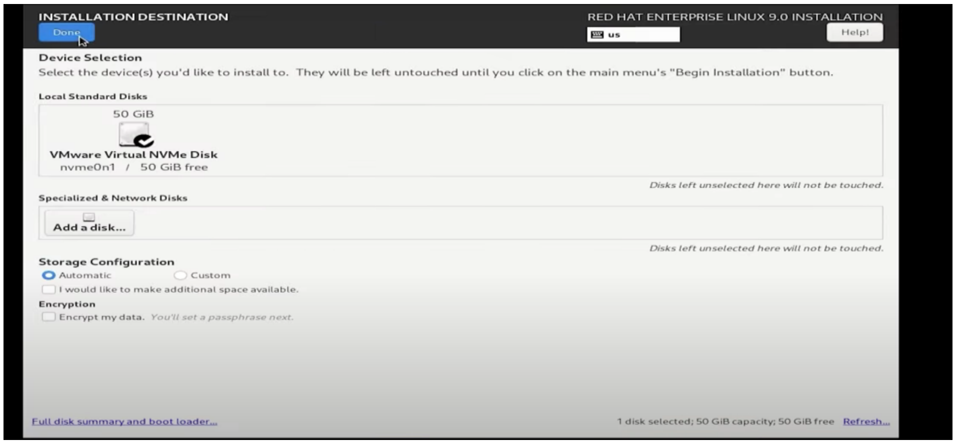
What language would you like to use during the installation process?

हिन्दी	Hindi
English	English
বাংলা	Bangla
తెలుగు	Telugu
मराठी	Marathi
தமிழ்	Tamil
اردو	Urdu
ગુજરાતી	Gujarati
ಕನ್ನಡ	Kannada
മലയാളം	Malayalam
ଓଡ଼ିଆ	Odia
ਪੰਜਾਬੀ	Punjabi
অসমীয়া	Assamese
العربية	Arabic

English (United States)
English (United Kingdom)
English (India)
English (Australia)
English (Canada)
English (Denmark)
English (Ireland)
English (New Zealand)
English (Nigeria)
English (Hong Kong SAR China)
English (Philippines)
English (Singapore)
English (South Africa)
English (Zambia)
English (Zimbabwe)
English (Botswana)
English (Antigua & Barbuda)

2.4. Select Installation Destination (Disk)

- In this section, you will be asked to choose the virtual disk (the hard drive) where Red Hat Linux will be installed.
- Select the **Virtual Disk** (it will usually be named something like sda).
- Choose either **Automatic Partitioning** (recommended for beginners) or **Manual Partitioning** if you have advanced disk configuration needs.



INSTALLATION DESTINATION

RED HAT ENTERPRISE LINUX 9.0 INSTALLATION

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

50 GiB
VMware Virtual NVMe Disk
nvme0n1 / 50 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Disks left unselected here will not be touched.

Storage Configuration

● Automatic ○ Custom

□ I would like to make additional space available.

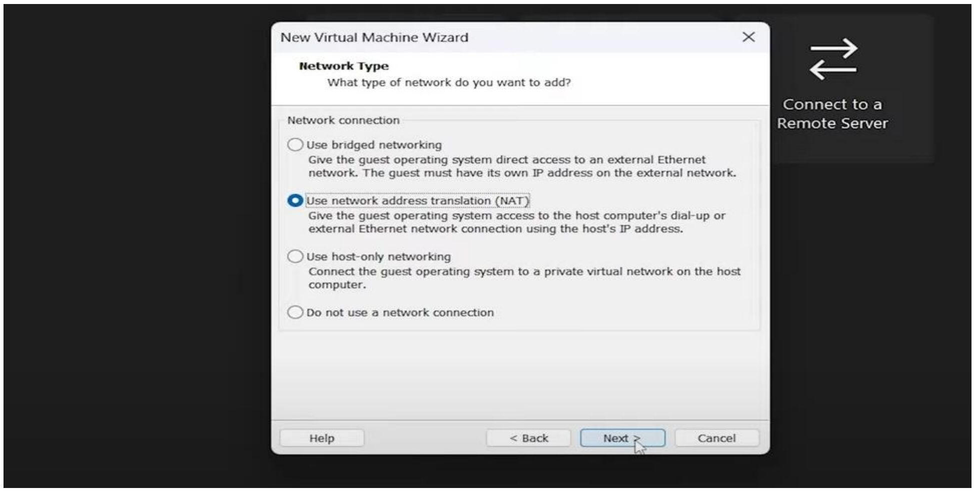
Encryption

□ Encrypt my data. *You'll set a passphrase next.*

1 disk selected; 50 GiB capacity; 50 GiB free

2.5. Configure Network and Hostname

- **Network Configuration**: Enable networking by toggling the **ON/OFF** switch for the network adapter. If your VMware setup uses **NAT** or **Bridged** networking, it will automatically get an IP address from your host network.
- **Hostname**: Set the **hostname** for the system (e.g., rhel-server). The hostname is used to identify the system within a network.



New Virtual Machine Wizard

Network Type

What type of network do you want to add?

Network connection

○ Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

● Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

○ Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.

○ Do not use a network connection

2.6. Disk Partitioning and Filesystem Setup

- If you chose **Automatic Partitioning**, Red Hat will create the necessary partitions for you. If you chose **Manual Partitioning**, you'll need to create partitions like /, /home, and /swap yourself. For most users, **automatic partitioning** is sufficient.
- The default filesystem used by RHEL is **ext4**, but you can choose **XFS** for newer setups.

2.7. Software Selection

- Here, you can choose the type of installation. The common options are:
  - **Minimal Install**: This is a lightweight installation with just the core Linux system and essential utilities.
  - **Server with GUI**: A full server installation that also includes a graphical user interface (GUI), useful if you plan to manage the system using a graphical desktop environment.
  - Choose **Server with GUI** if you want the full installation with a GUI (this is recommended for general use).

2.8. Set Root Password

- **Root Password**: Set a secure **root** password. The root account is the administrative account for your system, so the password should be strong.
- Confirm the password to continue.

2.9. Set Time Zone

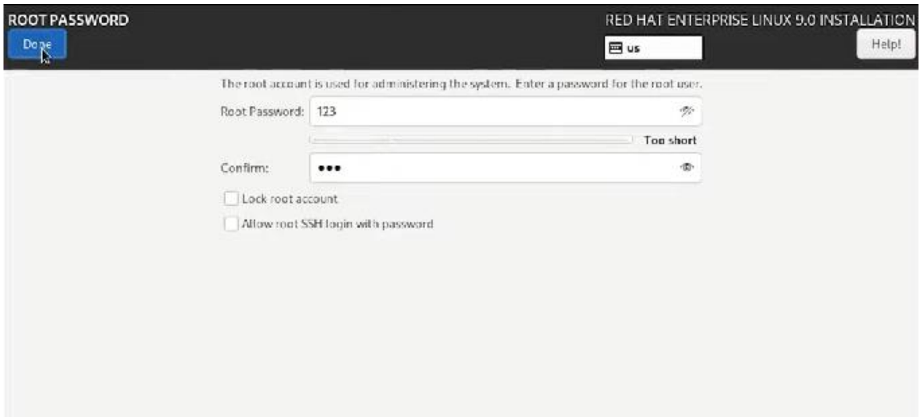
- Choose the correct **time zone** based on your geographical location to ensure that the system time is accurate.
- Once done, click **Done**.

2.10. Begin Installation

- After configuring all the settings, click **Begin Installation**. The installer will copy files to the disk and set up the system.
- This process can take some time depending on your system and network speed.

2.11. Create a User Account

- While the system is installing, you'll be prompted to create a **non-root user account**. This user will be used for daily operations.
- **Username**: Choose a username (e.g., admin or user).
- Set a password for this account.



The root account is used for administering the system. Enter a password for the root user.

Root Password: 123

Too short

Confirm: •••

□ Lock root account

□ Allow root SSH login with password

3: Post-Installation Configuration

3.1. Network Configuration

- After installation, the system should automatically configure network settings.
- To verify, use the ip a or ifconfig command to check the network interfaces and IP addresses.

Example:

ip a (This will list all network interfaces and their assigned IP addresses.)

2. System Updates

- The first thing you should do after logging in is update the system to ensure it has the latest security patches and software updates.
- sudo yum update -y
  - This will fetch and install any available updates from the Red Hat repositories.

3.3. Install Additional Software (Optional)

- If you need additional software, such as web servers or databases, use yum to install it.

Example:

sudo yum install httpd -y

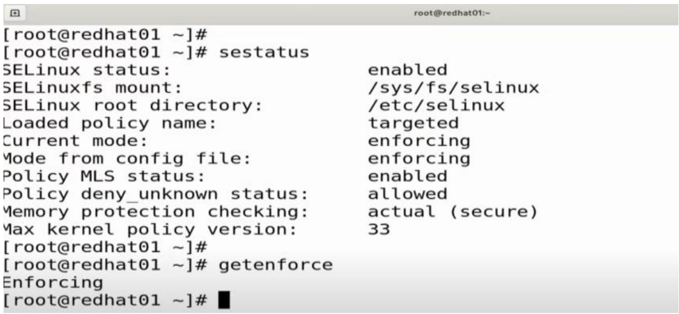
This will install Apache web server.

3.4. Configure Firewall

- Use firewalld to manage the firewall. To allow traffic on port 80 for a web server, run:
- sudo firewall-cmd --permanent --add-service=http
- sudo firewall-cmd --reload
    - This allows HTTP traffic through the firewall.

3.5. Configure SELinux

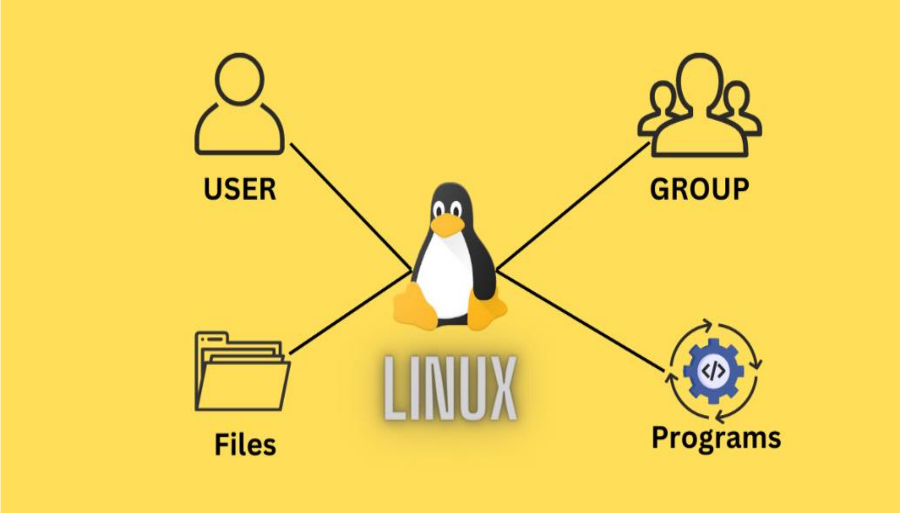
- SELinux (Security-Enhanced Linux) provides an additional layer of security by enforcing mandatory access control policies.
- To check the current status of SELinux, use:
- Getenforce or sestatus
- To set SELinux to **Enforcing** mode:
- sudo setenforce 1



```
[root@redhat01 ~]#
[root@redhat01 ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[root@redhat01 ~]#
[root@redhat01 ~]# getenforce
Enforcing
[root@redhat01 ~]# 
```

User and Group management

User and group management in Linux is crucial for controlling access to system resources and maintaining system security. In Red Hat Enterprise Linux (RHEL), user and group management is typically done through commands like useradd, usermod, userdel, groupadd, and groupdel, as well as modifying configuration files such as /etc/passwd, /etc/group, and /etc/shadow.



1. User Management

1.1. Adding a User

To add a new user to the system, you can use the useradd command. This command creates a new user account and a corresponding home directory.

- **Syntax:** sudo useradd [options] username
- **Example:** sudo useradd john

This command creates a new user named john. A home directory /home/john will be created automatically, and the default shell will be /bin/bash.

- **Assigning a Password:** After adding a user, you'll typically want to assign a password. Use the passwd command: sudo passwd john

You will be prompted to enter the new password for the user.

1.2. Modifying a User

If you need to modify a user's details, such as changing their shell, home directory, or group, use the usermod command.

- **Syntax:** sudo usermod [options] username
- **Examples:**
    - **Change the user's shell:** sudo usermod -s /bin/zsh john

This changes John's shell to zsh.

- **Change the user's home directory:** sudo usermod -d /home/johnny john
- **Add a user to an existing group:** sudo usermod -aG sudo john

This adds John to the sudo group, granting him administrative privileges.

1.3. Deleting a User

If you need to delete a user and optionally remove their home directory and files, use the userdel command.

- **Syntax:** sudo userdel [options] username
- **Example:** sudo userdel -r john

The -r option removes the user's home directory and mail spool.

1.4. Listing Users

You can view a list of all users in the system by looking at the /etc/passwd file, or you can use the getent command.

- **List users using cat:** cat /etc/passwd
- **List users using getent:** getent passwd

This will display all users, including system users.

3. Group Management

2.1. Adding a Group

To create a new group, use the groupadd command.

- **Syntax:** sudo groupadd groupname
- **Example:** sudo groupadd developers

This creates a new group called developers.

2.2. Modifying a Group

To modify a group (for example, to change the group’s name), use the groupmod command.

- **Syntax:** sudo groupmod [options] groupname
- **Example: Rename a group:** sudo groupmod -n devops developers

This renames the developers group to devops.

2.3. Deleting a Group

To delete a group, use the groupdel command.

- **Syntax:** sudo groupdel groupname
- **Example:** sudo groupdel developers

This deletes the developers group.

2.4. Viewing Group Information

To see the details about a specific group, use the getent command or view the /etc/group file.

- **View all groups:** cat /etc/group
- **View a specific group:** getent group developers

3. Adding a User to a Group

You can add an existing user to a group with the usermod command.

- **Syntax:** sudo usermod -aG groupname username
- **Example:** sudo usermod -aG developers john

This command adds the user john to the developers group. The -aG option ensures that the user is added to the group without being removed from any other groups.

4. User and Group Configuration Files

4.1. /etc/passwd

This file stores information about each user account, including the username, password (encrypted), UID, GID, full name, home directory, and login shell.

- **Example entry in /etc/passwd:** john:x:1001:1001:John Doe:/home/john:/bin/bash
  - john: Username
  - x: Placeholder for password (actual password is stored in /etc/shadow)
  - 1001: User ID (UID)
  - 1001: Group ID (GID)
  - John Doe: User's full name (GECOS field)
  - /home/john: Home directory
  - /bin/bash: Default login shell

4.2. /etc/group

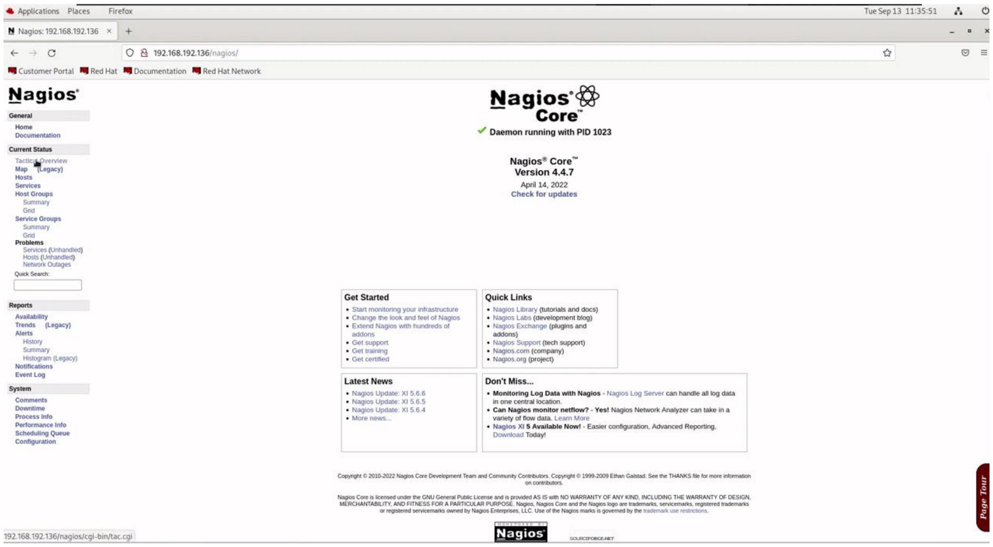
This file stores information about user groups. It lists group names, group passwords (rarely used), and the GID, along with the members of each group.

- **Example entry in /etc/group:** developers:x:1002:john,jane
  - developers: Group name
  - x: Placeholder for password
  - 1002: Group ID (GID)
  - john,jane: List of users in this group

TOOLS USED

1. System Monitoring Tool: Nagios

Nagios is an open-source IT infrastructure monitoring tool that enables system administrators to monitor servers, network devices, and services to ensure everything is functioning correctly. It helps detect problems like system crashes, high CPU usage, disk space issues, and service failures, and alerts administrators to address these issues promptly.



✓ Daemon running with PID 1023

Nagios® Core™
Version 4.4.7
April 14, 2022
Check for updates

Get Started

- Start monitoring your infrastructure
- Change the look and feel of Nagios
- Extend Nagios with hundreds of addons
- Get support
- Get training
- Get certified

Quick Links

- Nagios Library (tutorials and docs)
- Nagios Labs (development blog)
- Nagios Exchange (plugins and addons)
- Nagios Support (tech support)
- Nagios.com (company)
- Nagios.org (project)

Latest News

- Nagios Update: XI 5.6.6
- Nagios Update: XI 5.6.5
- Nagios Update: XI 5.6.4
- More news...

Don't Miss...

- **Monitoring Log Data with Nagios** - Nagios Log Server can handle all log data in one central location.
- **Can Nagios monitor netflow? - Yes!** Nagios Network Analyzer can take in a variety of flow data. Learn More
- **Nagios XI 5 Available Now!** - Easier configuration, Advanced Reporting, Download Today!

Copyright © 2010-2022 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information on contributors.

Nagios Core is licensed under the GNU General Public License and is provided AS IS with NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. Nagios, Nagios Core and the Nagios logo are trademarks, servicemarks, registered trademarks or registered servicemarks owned by Nagios Enterprises, LLC. Use of the Nagios marks is governed by the trademark use restrictions.

Key Features of Nagios:

- **Monitoring**: Nagios can monitor various network services, host resources, and applications (like HTTP, DNS, SMTP, POP3, etc.).
- **Alerting**: It provides real-time alerts via email, SMS, or other messaging platforms when a service or system goes down or experiences issues.
- **Scalability**: Nagios is highly scalable, allowing it to monitor a single machine or an entire infrastructure across multiple networks.
- **Plugin-based**: Nagios relies on plugins for monitoring specific services and resources, making it highly flexible and customizable.
- **Web Interface**: Nagios comes with a web interface that provides detailed views of all monitored hosts, services, and their status.

How Nagios Works:

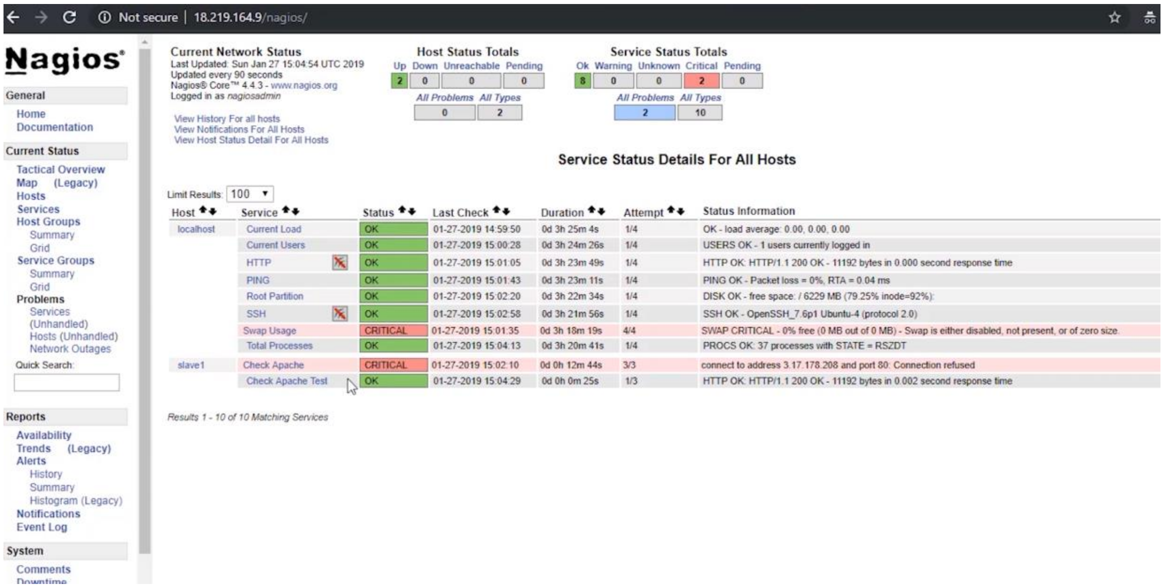
1. **Hosts and Services**: You configure Nagios to monitor a list of hosts (e.g., servers, workstations) and services (e.g., HTTP, SSH).

2. **Plugins**: Nagios uses plugins to check the status of services. These plugins gather performance metrics like CPU usage, memory usage, disk space, and network traffic.
3. **Check Intervals**: Nagios performs checks at regular intervals. If a service or host is found to be down, Nagios alerts the system administrators.
4. **Notification**: When a failure or critical condition is detected, Nagios sends notifications through email, SMS, or other communication methods, depending on the configuration.

Installation and Configuration of Nagios:

1. **Install Nagios**: sudo yum install nagios nagios-plugins-all httpd -y
2. **Start the Nagios service**: sudo systemctl start nagios

   sudo systemctl enable nagios
3. **Configure Nagios**: Configure the /etc/nagios/nagios.cfg file, specify hosts to monitor, and set up appropriate plugins for those services.



Current Network Status
Last Updated: Sun Jan 27 15:04:54 UTC 2019
Updated every 90 seconds
Nagios® Core™ 4.4.3 - www.nagios.org
Logged in as *nagiosadmin*

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

All Problems	All Types
0	2

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
8	0	0	2	0

All Problems	All Types
2	10

Service Status Details For All Hosts

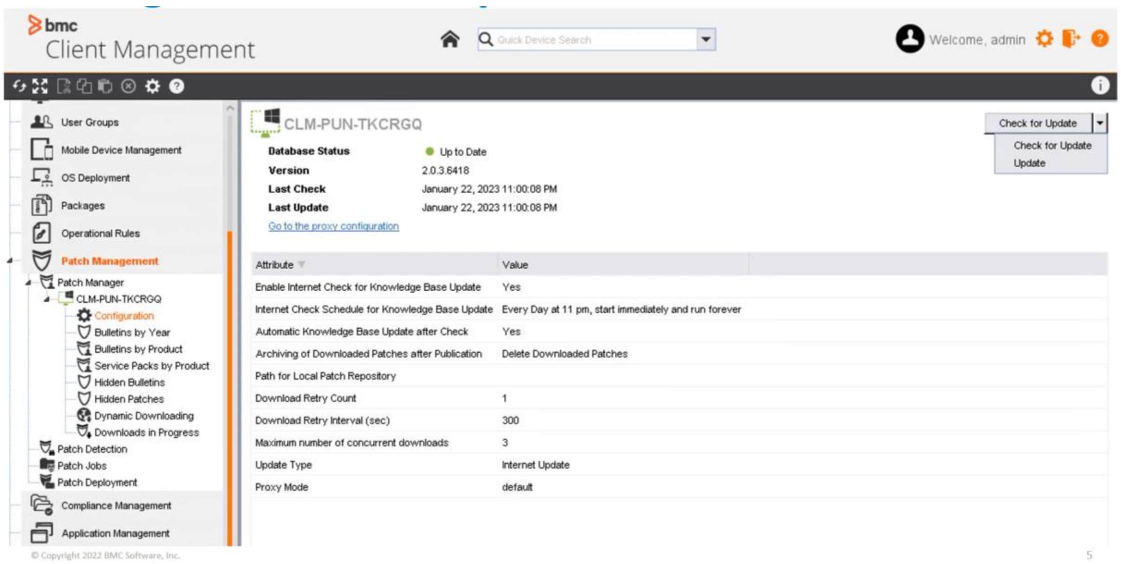
Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	01-27-2019 14:59:50	0d 3h 25m 4s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	01-27-2019 15:00:28	0d 3h 24m 26s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	01-27-2019 15:01:05	0d 3h 23m 49s	1/4	HTTP OK: HTTP/1.1 200 OK - 11192 bytes in 0.000 second response time
	PING	OK	01-27-2019 15:01:43	0d 3h 23m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.04 ms
	Root Partition	OK	01-27-2019 15:02:20	0d 3h 22m 34s	1/4	DISK OK - free space: / 6229 MB (79.25% inode=92%):
	SSH	OK	01-27-2019 15:02:58	0d 3h 21m 56s	1/4	SSH OK - OpenSSH_7.6p1 Ubuntu-4 (protocol 2.0)
	Swap Usage	CRITICAL	01-27-2019 15:01:35	0d 3h 18m 19s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
	Total Processes	OK	01-27-2019 15:04:13	0d 3h 20m 41s	1/4	PROCS OK: 37 processes with STATE = RSZDT
slave1	Check Apache	CRITICAL	01-27-2019 15:02:10	0d 0h 12m 44s	3/3	connect to address 3.17.178.208 and port 80: Connection refused
	Check Apache Test	OK	01-27-2019 15:04:29	0d 0h 0m 25s	1/3	HTTP OK: HTTP/1.1 200 OK - 11192 bytes in 0.002 second response time

Results 1 - 10 of 10 Matching Services

2. Patching Tool: BMC

BMC (formerly known as BMC Software) is a tool designed for patch management, automating the process of applying patches and updates to systems, software, and applications to keep them secure and functioning optimally. BMC helps IT teams stay up-to-date with security patches, bug fixes, and performance enhancements, reducing the risk of system vulnerabilities.



CLM-PUN-TKCRGQ

Database Status ● Up to Date
Version 2.0.3.6418
Last Check January 22, 2023 11:00:08 PM
Last Update January 22, 2023 11:00:08 PM
Go to the proxy configuration

Attribute	Value
Enable Internet Check for Knowledge Base Update	Yes
Internet Check Schedule for Knowledge Base Update	Every Day at 11 pm, start immediately and run forever
Automatic Knowledge Base Update after Check	Yes
Archiving of Downloaded Patches after Publication	Delete Downloaded Patches
Path for Local Patch Repository	
Download Retry Count	1
Download Retry Interval (sec)	300
Maximum number of concurrent downloads	3
Update Type	Internet Update
Proxy Mode	default

© Copyright 2022 BMC Software, Inc. 5

Key Features of BMC:

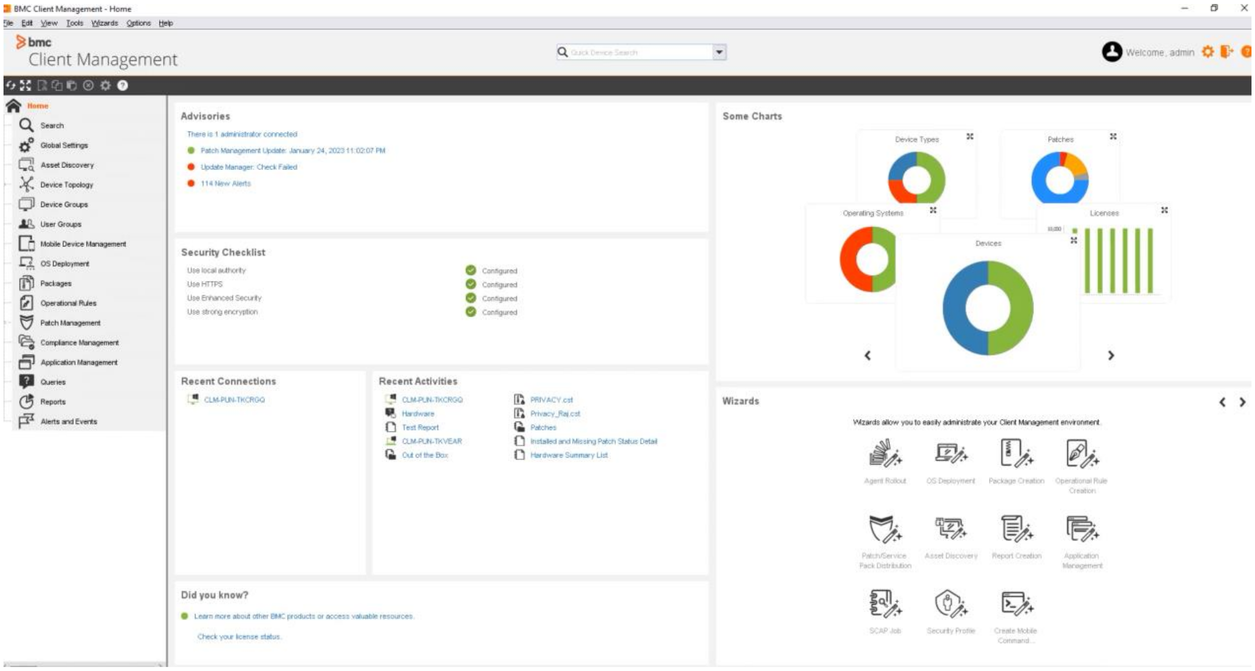
- **Automated Patch Management**: BMC automates the process of identifying, deploying, and verifying patches on a variety of systems.
- **Comprehensive Coverage**: It supports patching for multiple platforms, including Linux, Windows, and macOS.
- **Compliance Reporting**: It provides detailed reports and dashboards on patch deployment status, helping organizations ensure compliance with internal policies and external regulations.
- **Risk Assessment**: BMC can perform vulnerability scans to assess whether a patch is needed or if the system is at risk.
- **Integration**: It can integrate with other IT management tools and enterprise systems for streamlined workflows.

How BMC Works:

1. **Scan for Patches**: BMC scans the systems to identify missing patches or vulnerabilities that require attention.
2. **Deployment**: After identifying missing patches, BMC automatically deploys patches to the appropriate systems.
3. **Compliance and Reporting**: BMC tracks patch compliance and generates reports to demonstrate that all patches have been successfully applied.

Patching Process:

1. **Define Patch Policies**: You can define patch policies, such as patch deployment schedules (e.g., once a week or after security updates are released).
2. **Testing**: It's important to test patches in a staging environment before deploying them to production systems.
3. **Patch Installation**: Once the patches are validated, they are deployed to all relevant systems automatically.



Advisories

There is 1 administrator connected
● Patch Management Update: January 24, 2023 11:02:07 PM
● Update Manager: Check Failed
● 114 New Alerts

Security Checklist

Use local authority ✓ Configured
Use HTTPS ✓ Configured
Use Enhanced Security ✓ Configured
Use strong encryption ✓ Configured

Recent Connections

CLM-PUN-TKCRGQ

Recent Activities

CLM-PUN-TKCRGQ
Hardware
Test Report
CLM-PUN-TKVEAR
Out of the Box
PRIVACY.cst
Privacy_Raj.cst
Patches
Installed and Missing Patch Status Detail
Hardware Summary List

Wizards allow you to easily administrate your Client Management environment.

Did you know?

● Learn more about other BMC products or access valuable resources.

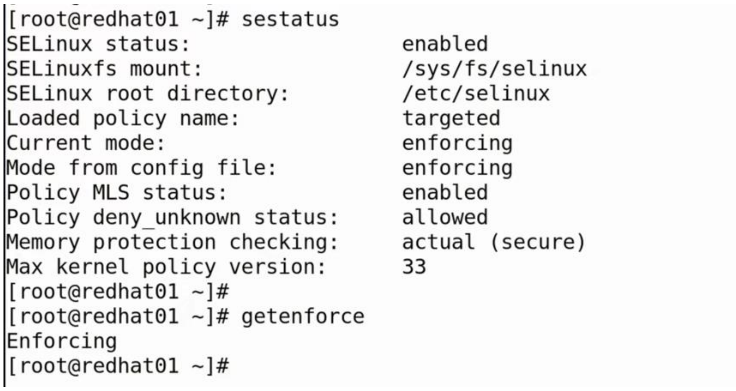
Check your license status.

3. Security Tool: SELinux

SELinux (Security-Enhanced Linux) is a security feature of the Linux kernel that enforces mandatory access control (MAC). SELinux adds an additional layer of security on top of traditional discretionary access control (DAC) by defining and enforcing security policies for access to files, processes, and network resources.

Key Features of SELinux:

- **Mandatory Access Control (MAC)**: SELinux ensures that even users with root privileges cannot access certain resources unless explicitly permitted by the security policy.
- **Fine-grained Security**: SELinux allows you to define detailed security rules for processes, files, devices, and other system resources.
- **Enforcement**: SELinux can run in **Enforcing**, **Permissive**, or **Disabled** mode.
  - **Enforcing**: SELinux enforces the security policies, denying access to unauthorized users or processes.
  - **Permissive**: SELinux logs access violations but doesn't deny access.
  - **Disabled**: SELinux is turned off completely.



```
[root@redhat01 ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[root@redhat01 ~]#
[root@redhat01 ~]# getenforce
Enforcing
[root@redhat01 ~]#
```

How SELinux Works:

1. **Labels and Contexts**: SELinux uses labels and contexts to assign security attributes to files, processes, and resources. Each file or resource has an associated security context.
2. **Policies**: SELinux operates based on policies that define what actions can be performed by which users, processes, or applications. These policies can be very specific, down to the file level.

3. **Role-based Access Control (RBAC)**: SELinux uses roles to determine what actions users and processes can perform on system resources.

Managing SELinux:

- **Check SELinux status**: sestatus
- **Switch between modes**:

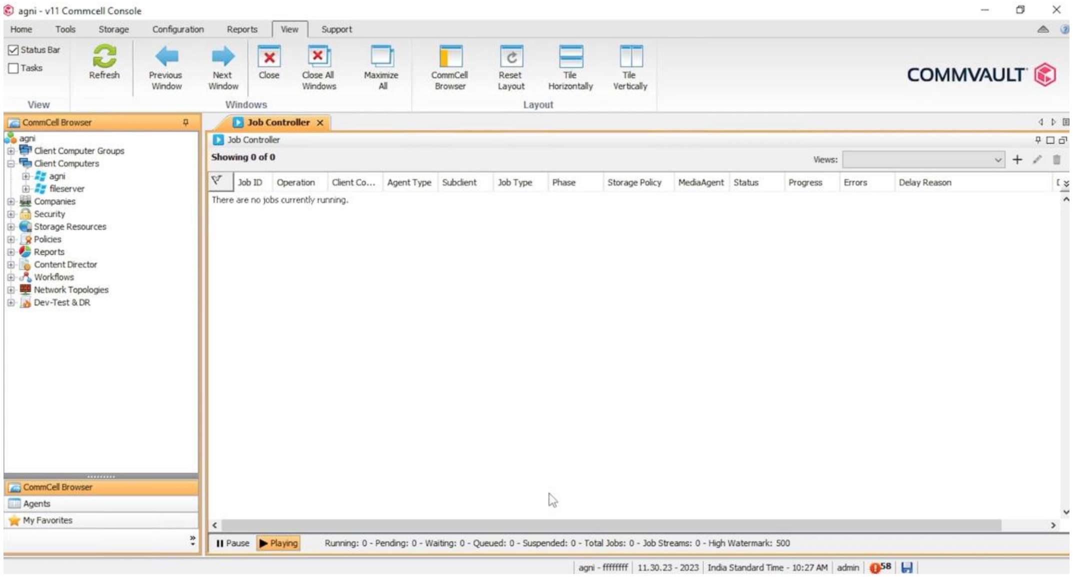
```
sudo setenforce 1  # Enforcing mode

sudo setenforce 0  # Permissive mode
```

- **Configure SELinux**: The main configuration file for SELinux is /etc/selinux/config. You can change the default mode of SELinux (Enforcing, Permissive, Disabled) in this file.

4. Backup Tool: Commvault

Commvault is an enterprise-level data protection and backup software suite designed to back up, restore, and manage data across various environments, including physical, virtual, and cloud infrastructures. It is widely used for its scalability, reliability, and automation in backing up large volumes of data.



Showing 0 of 0

There are no jobs currently running.

Running: 0 - Pending: 0 - Waiting: 0 - Queued: 0 - Suspended: 0 - Total Jobs: 0 - Job Streams: 0 - High Watermark: 500

agni - ffffffff | 11.30.23 - 2023 | India Standard Time - 10:27 AM | admin | 58

Key Features of Commvault:

- **Automated Backups**: Commvault automates backup operations, allowing users to schedule regular backups for data protection.
- **Cross-Platform Support**: It supports backups for multiple platforms, including databases (e.g., SQL Server, Oracle), virtual machines (e.g., VMware, Hyper-V), and cloud environments.
- **Incremental Backups**: Commvault can perform incremental backups, which only back up changes made since the last backup, saving time and storage space.
- **Data Deduplication**: Commvault uses deduplication technology to minimize redundant data, improving backup efficiency and reducing storage requirements.
- **Disaster Recovery**: Commvault supports disaster recovery scenarios by enabling fast restoration of critical data and systems.

Backup and Restore Process:

1. **Create Backup Jobs**: Define backup jobs by selecting data sources, backup frequency, and destination.
2. **Backup Execution**: Commvault will automatically back up the selected data to a predefined destination, either on-premises or in the cloud.
3. **Restore Data**: In case of data loss or system failure, Commvault allows you to restore data quickly from the backup.

5. Log Management Tool: rsyslog and systemd-journald

5.1. rsyslog

rsyslog is an open-source logging system used to collect, store, and forward log messages from various sources. It supports advanced features like log filtering, remote logging, and log forwarding to other systems for centralized logging.

Key Features of rsyslog:

- **Remote Logging**: You can configure rsyslog to forward log messages to a remote server.
- **Log Filtering**: rsyslog allows you to filter log messages based on severity, facility, or other criteria.
- **File-based Logging**: Logs can be stored in specific files, such as /var/log/messages, /var/log/auth.log, etc.

Configuration:

- The main configuration file for rsyslog is /etc/rsyslog.conf.
- You can define rules to direct log messages from specific facilities to specific files.

Example of rsyslog Configuration:

```
# Store authentication logs

authpriv.* /var/log/auth.log

# Forward logs to a remote server

*.* @192.168.1.100:514
```

5.2. systemd-journald

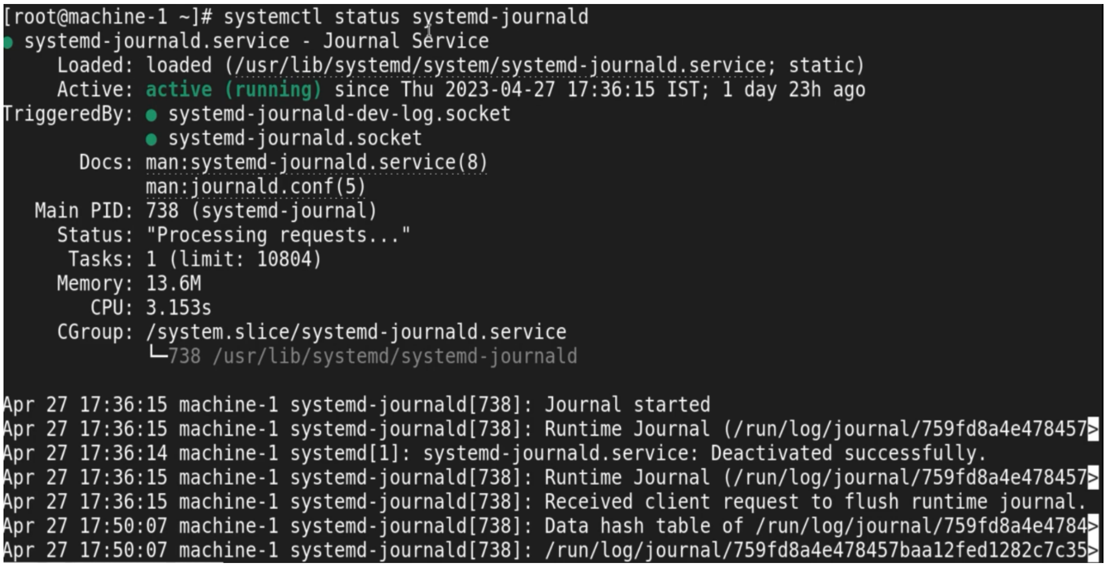
systemd-journald is the logging component of systemd, the system and service manager for Linux systems. It collects and manages log data, particularly for system services and application logs, and stores logs in a binary format for faster access.

Key Features of systemd-journald:

- **Centralized Logging**: Journald collects logs from systemd services and other sources and stores them in a central location.
- **Efficient Querying**: It uses a binary format for logs, which can be queried using the journalctl command.
- **Persistent Logging**: Journald can store logs persistently in /var/log/journal, allowing logs to survive reboots.
- **Log Filtering and Searching**: Logs can be filtered by service, date, severity, or other criteria.

Log Management with systemd-journald:

- **View logs**: journalctl
- **Filter logs**: journalctl -u apache2.service
- **View logs for a specific time**: journalctl --since "2023-04-15" --until "2023-04-16"



```
[root@machine-1 ~]# systemctl status systemd-journald
● systemd-journald.service - Journal Service
     Loaded: loaded (/usr/lib/systemd/system/systemd-journald.service; static)
     Active: active (running) since Thu 2023-04-27 17:36:15 IST; 1 day 23h ago
TriggeredBy: ● systemd-journald-dev-log.socket
             ● systemd-journald.socket
       Docs: man:systemd-journald.service(8)
             man:journald.conf(5)
   Main PID: 738 (systemd-journal)
     Status: "Processing requests..."
      Tasks: 1 (limit: 10804)
     Memory: 13.6M
        CPU: 3.153s
     CGroup: /system.slice/systemd-journald.service
             └─738 /usr/lib/systemd/systemd-journald

Apr 27 17:36:15 machine-1 systemd-journald[738]: Journal started
Apr 27 17:36:15 machine-1 systemd-journald[738]: Runtime Journal (/run/log/journal/759fd8a4e478457>
Apr 27 17:36:14 machine-1 systemd[1]: systemd-journald.service: Deactivated successfully.
Apr 27 17:36:15 machine-1 systemd-journald[738]: Runtime Journal (/run/log/journal/759fd8a4e478457>
Apr 27 17:36:15 machine-1 systemd-journald[738]: Received client request to flush runtime journal.
Apr 27 17:50:07 machine-1 systemd-journald[738]: Data hash table of /run/log/journal/759fd8a4e4784>
Apr 27 17:50:07 machine-1 systemd-journald[738]: /run/log/journal/759fd8a4e478457baa12fed1282c7c35>
```