QRADAR SIEM INSTALLATION GUIDE

IBM QRadar

Table of Contents

1. Introduction:

This guide provides a step-by-step walkthrough for setting up IBM QRadar Community Edition V7.5.0 in a home lab environment using VMware. QRadar CE is a great option for students, researchers, and cybersecurity enthusiasts who want to explore SIEM (Security Information and Event Management) capabilities in a controlled, non-production environment.

The deployment guide includes hardware requirements, ISO download instructions, VMware virtual machine setup, installation, and the configuration of a useful dashboard extension (Pulse app). By the end of this guide, you'll have a functional QRadar instance running locally and accessible via a web interface.

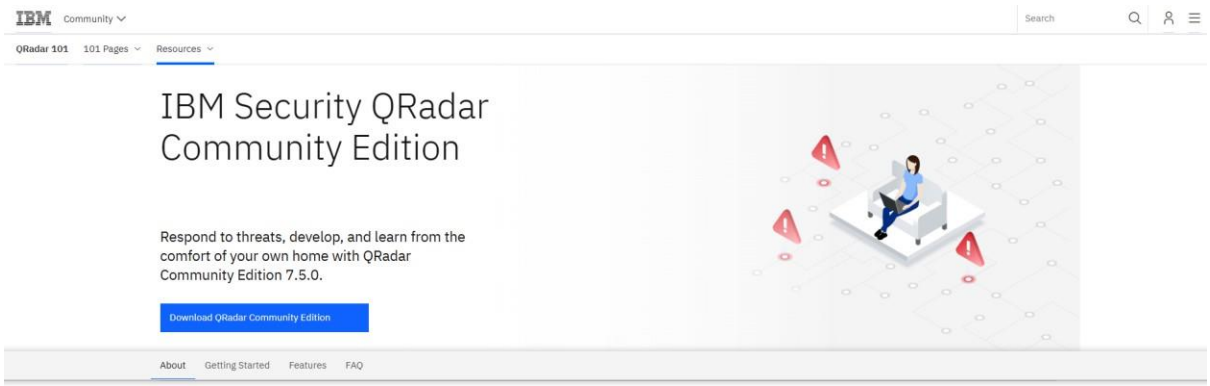
2. Hardware Requirements:

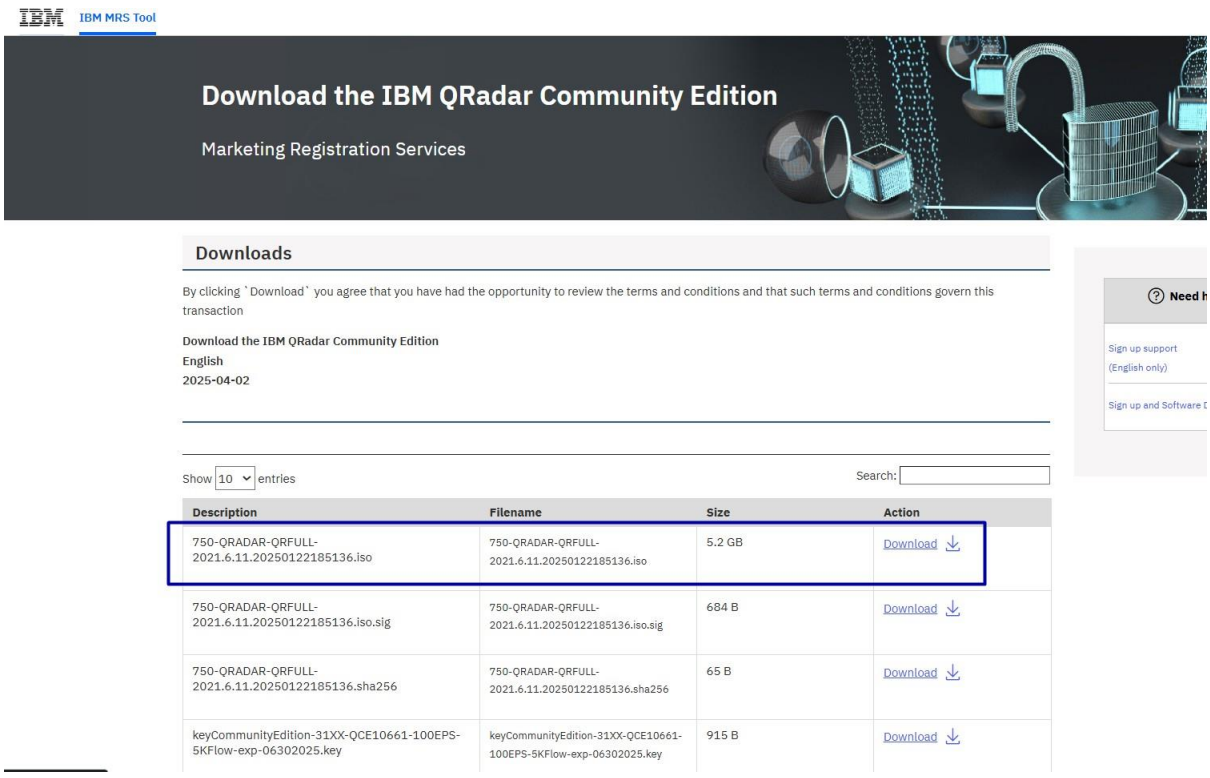
To install QRadar Community Edition V7.5.0 Update Package 11, your system must meet the following minimum hardware specifications:

- **Memory:** 24 GB RAM (minimum)
- **Disk Space:** 250 GB (minimum)
- **CPU:** 4 cores (minimum), 6 cores recommended
- **Network:** One network adapter with Internet access
- **IP Address:** Static IP required
- **Hostname:** Fully Qualified Domain Name (FQDN) must be used

3. Downloading the ISO:

- Visit the official IBM QRadar Community Edition page.
- Download the ISO file from:
  - https://www.ibm.com/community/101/qradar/ce/



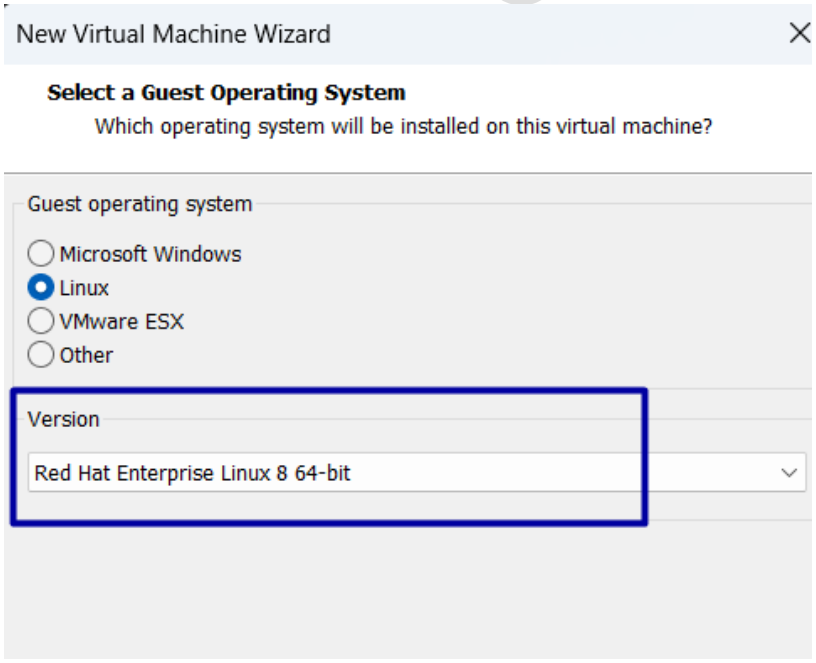


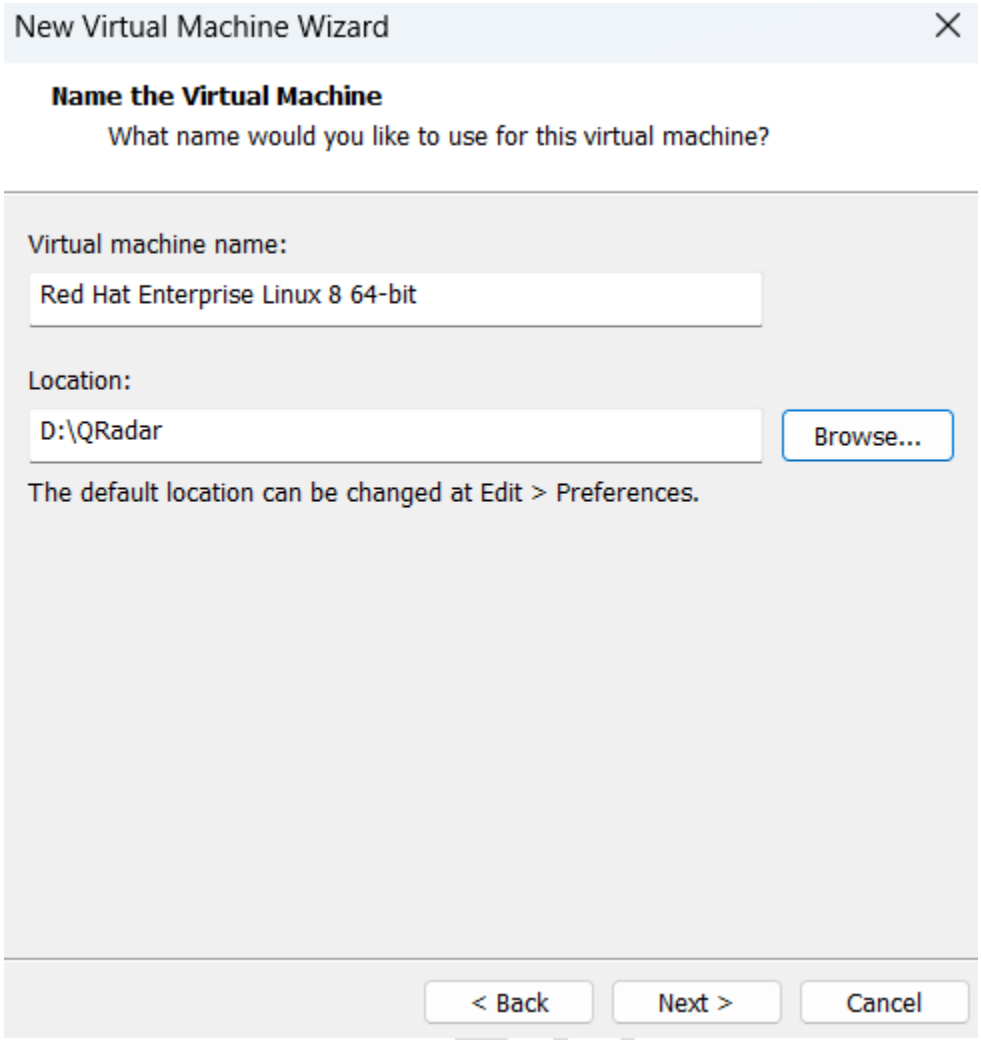
4. VMware Setup:

Create a New Custom VM:

- In VMware, create a new custom virtual machine.
- Select **Red Hat Enterprise Linux 8 (64-bit)** as the guest operating system.

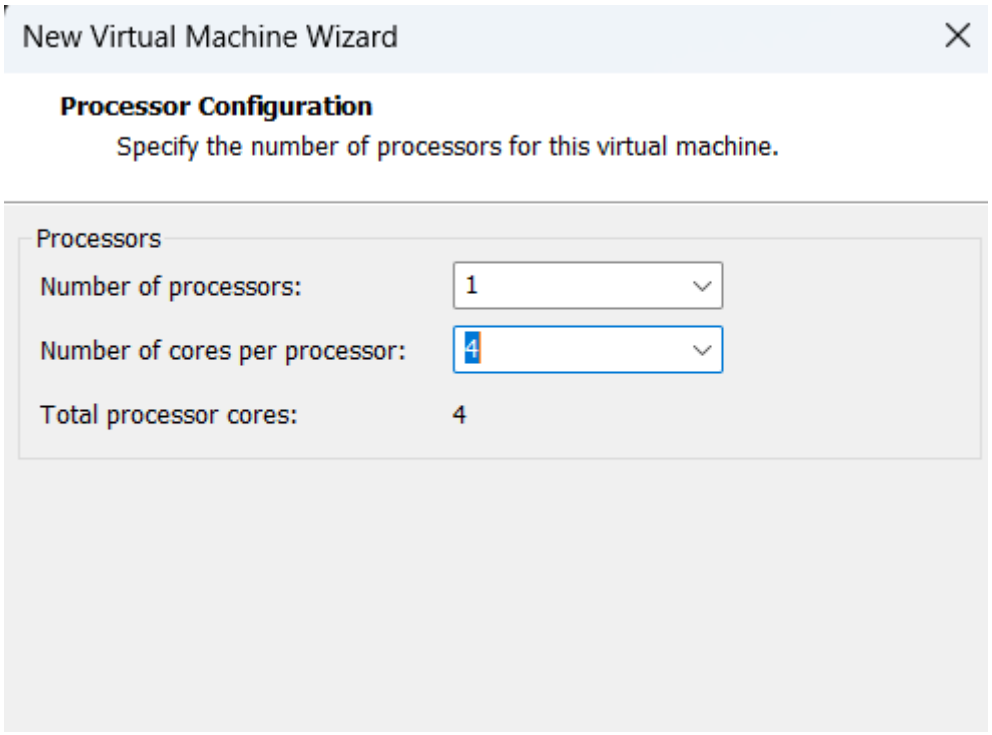
The guest operating system has to be **Red Hat Enterprise Linux 8 64-bit**

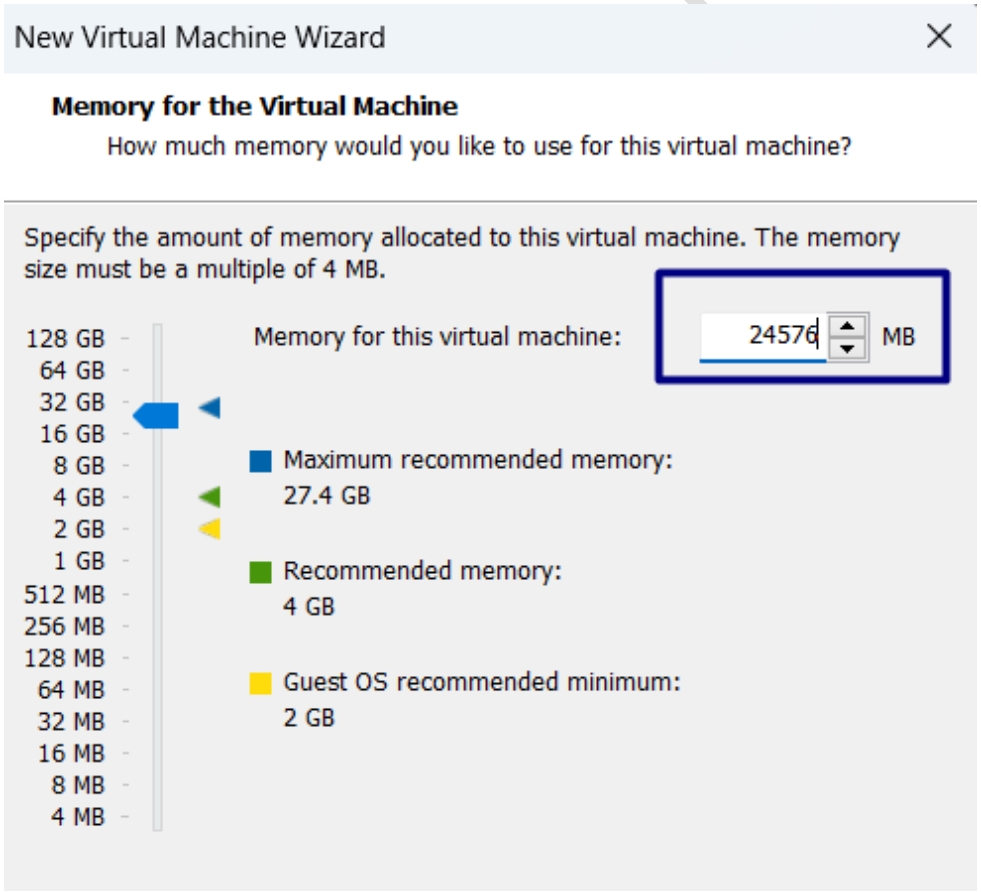




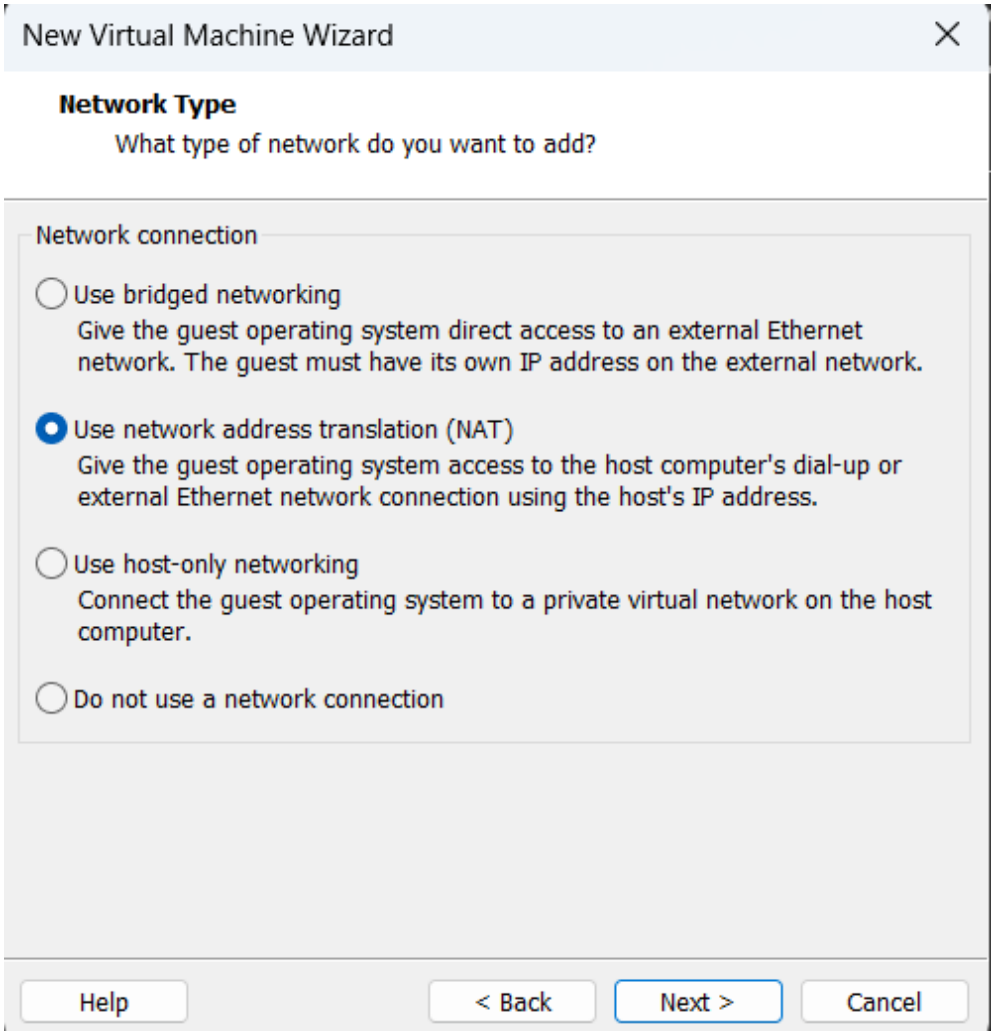
Allocate Resources:

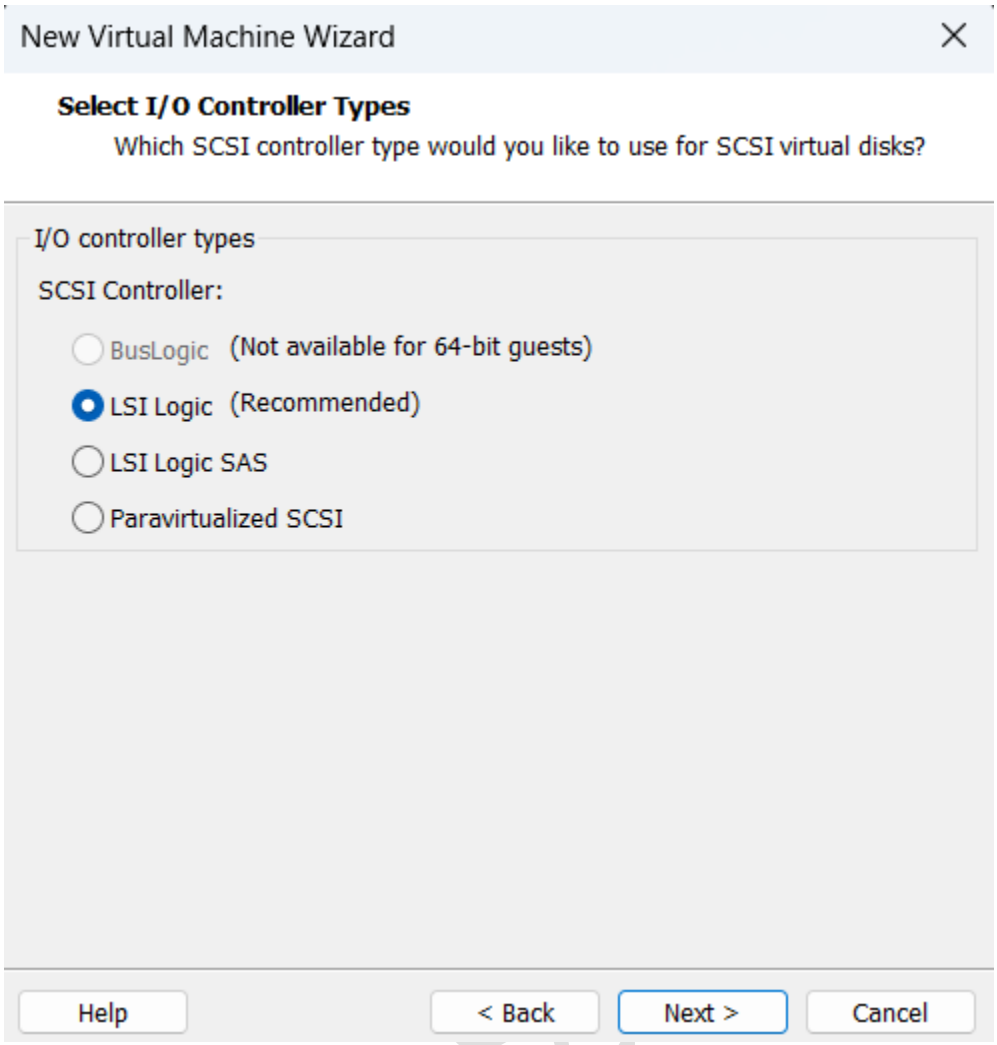
- **CPU:** 1 CPU with 4 cores
- **Memory:** 24 GB RAM
- **Disk:** 250 GB (single file, allocated upfront)


New Virtual Machine Wizard
Processor Configuration
Specify the number of processors for this virtual machine.
Processors
Number of processors:
1
Number of cores per processor:
4
Total processor cores:
4

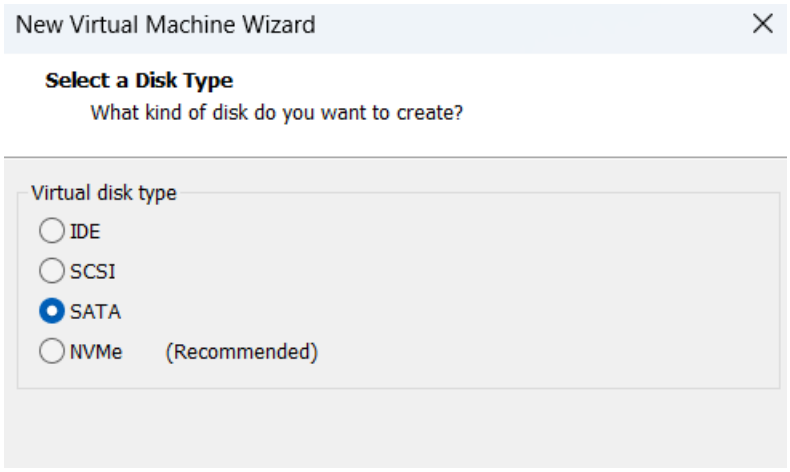

New Virtual Machine Wizard
Memory for the Virtual Machine
How much memory would you like to use for this virtual machine?
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine:
24576
MB
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended memory:
27.4 GB
Recommended memory:
4 GB
Guest OS recommended minimum:
2 GB

The network adapter has to be NAT

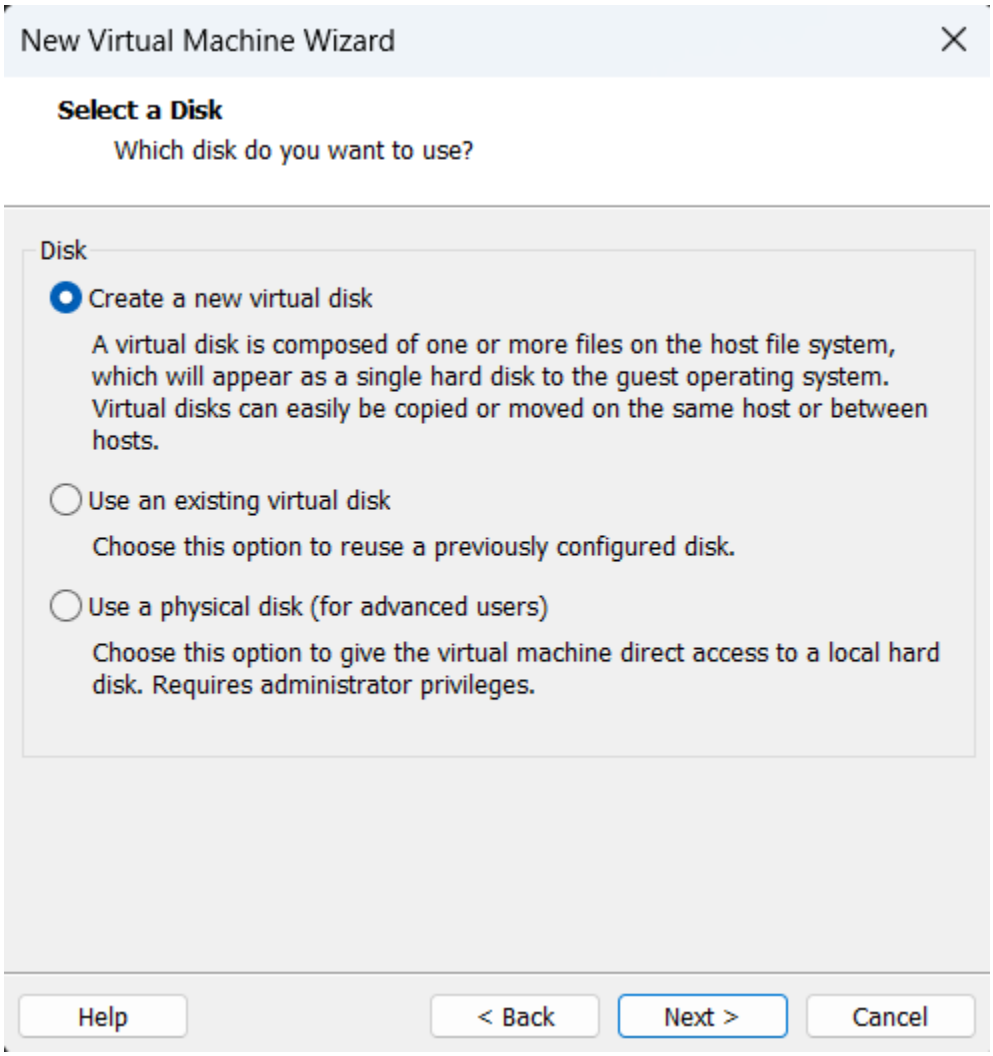




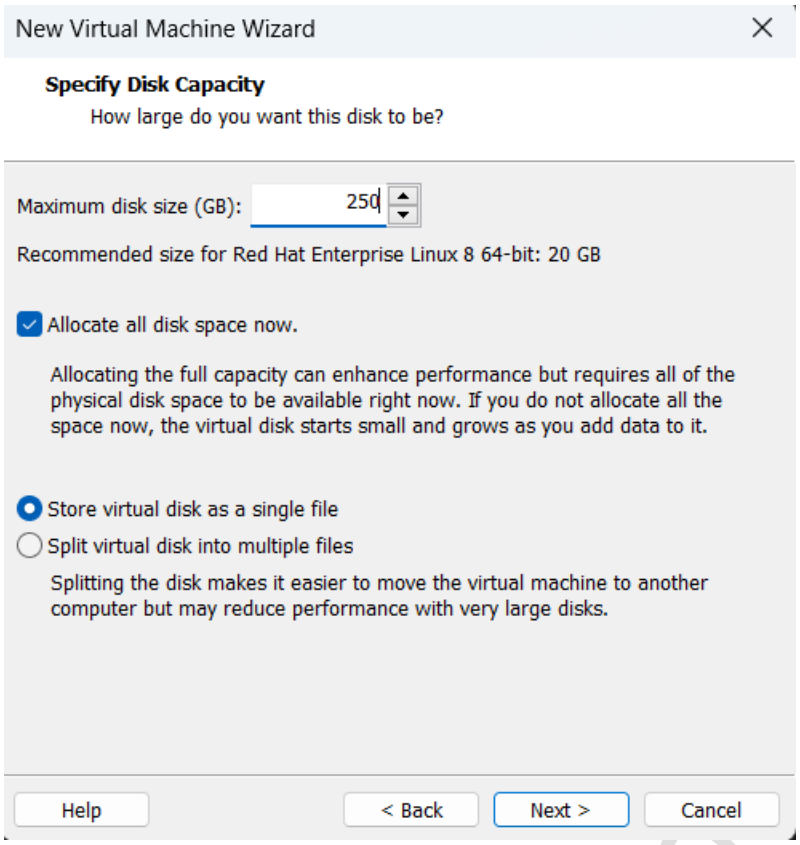
Use **SATA** instead of NVMe for disk type. NVMe may not allocate all required resources properly.

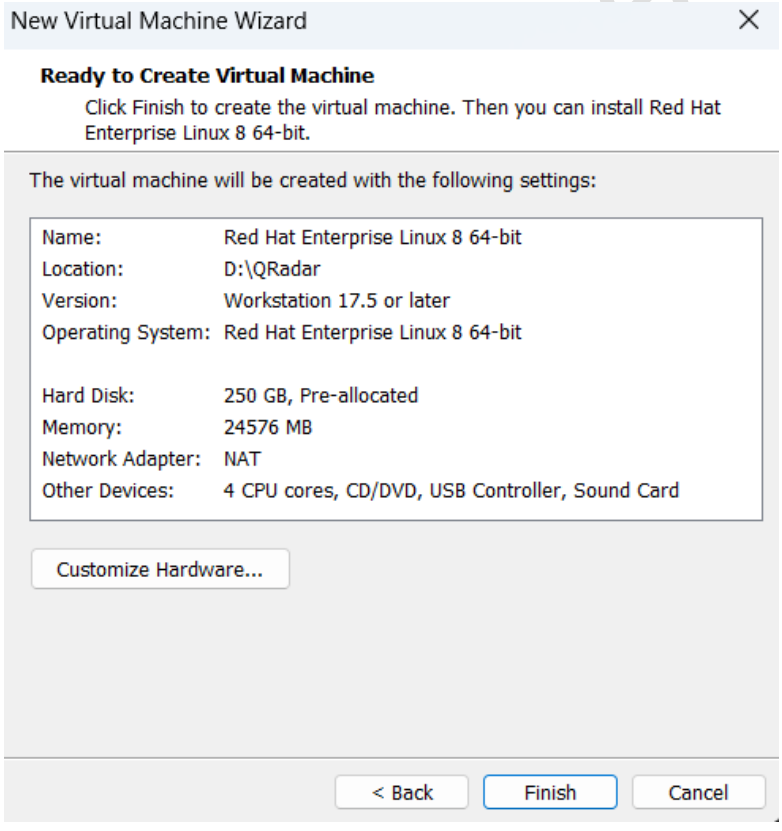


After choosing the disk type I created a new virtual disk.

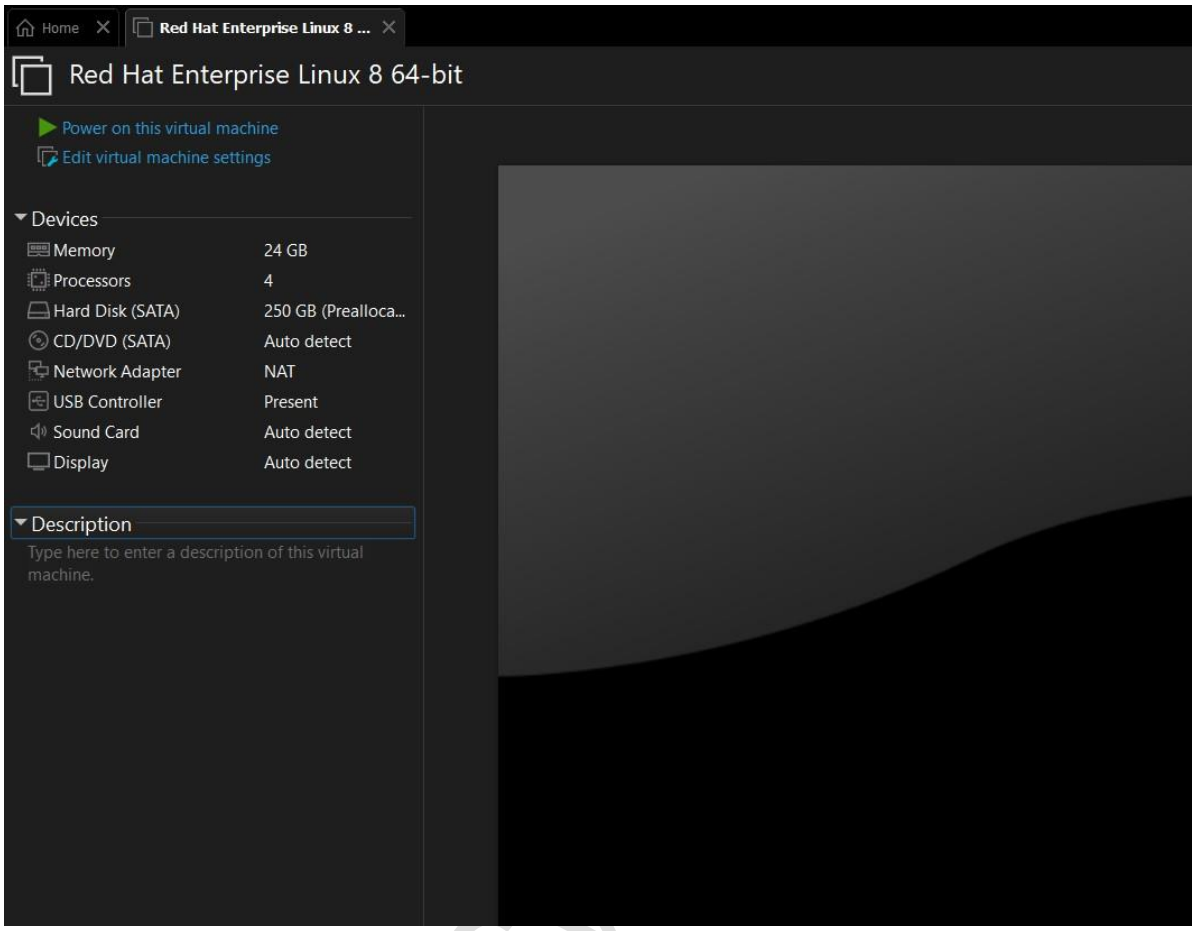


I allocated 250 GB disk size so it can run smoothly and checked the option allocate all disk space now and stored the virtual disk as a single file


New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
Maximum disk size (GB): 250
Recommended size for Red Hat Enterprise Linux 8 64-bit: 20 GB
Allocate all disk space now.
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel

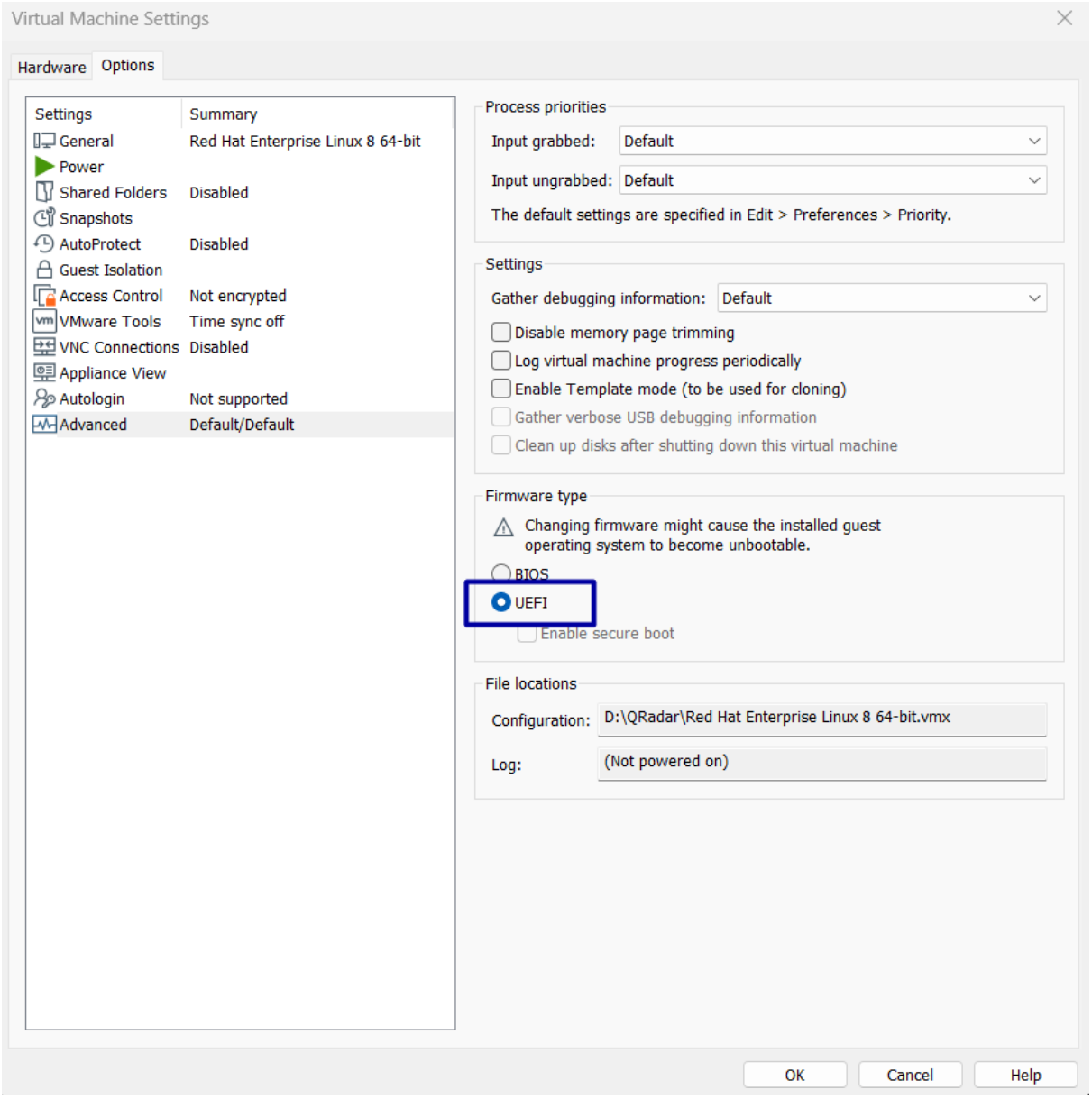

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Red Hat Enterprise Linux 8 64-bit.
The virtual machine will be created with the following settings:
Name: Red Hat Enterprise Linux 8 64-bit
Location: D:\QRadar
Version: Workstation 17.5 or later
Operating System: Red Hat Enterprise Linux 8 64-bit
Hard Disk: 250 GB, Pre-allocated
Memory: 24576 MB
Network Adapter: NAT
Other Devices: 4 CPU cores, CD/DVD, USB Controller, Sound Card
Customize Hardware...
< Back
Finish
Cancel

Now our VM has been created now we have to procced to the next options



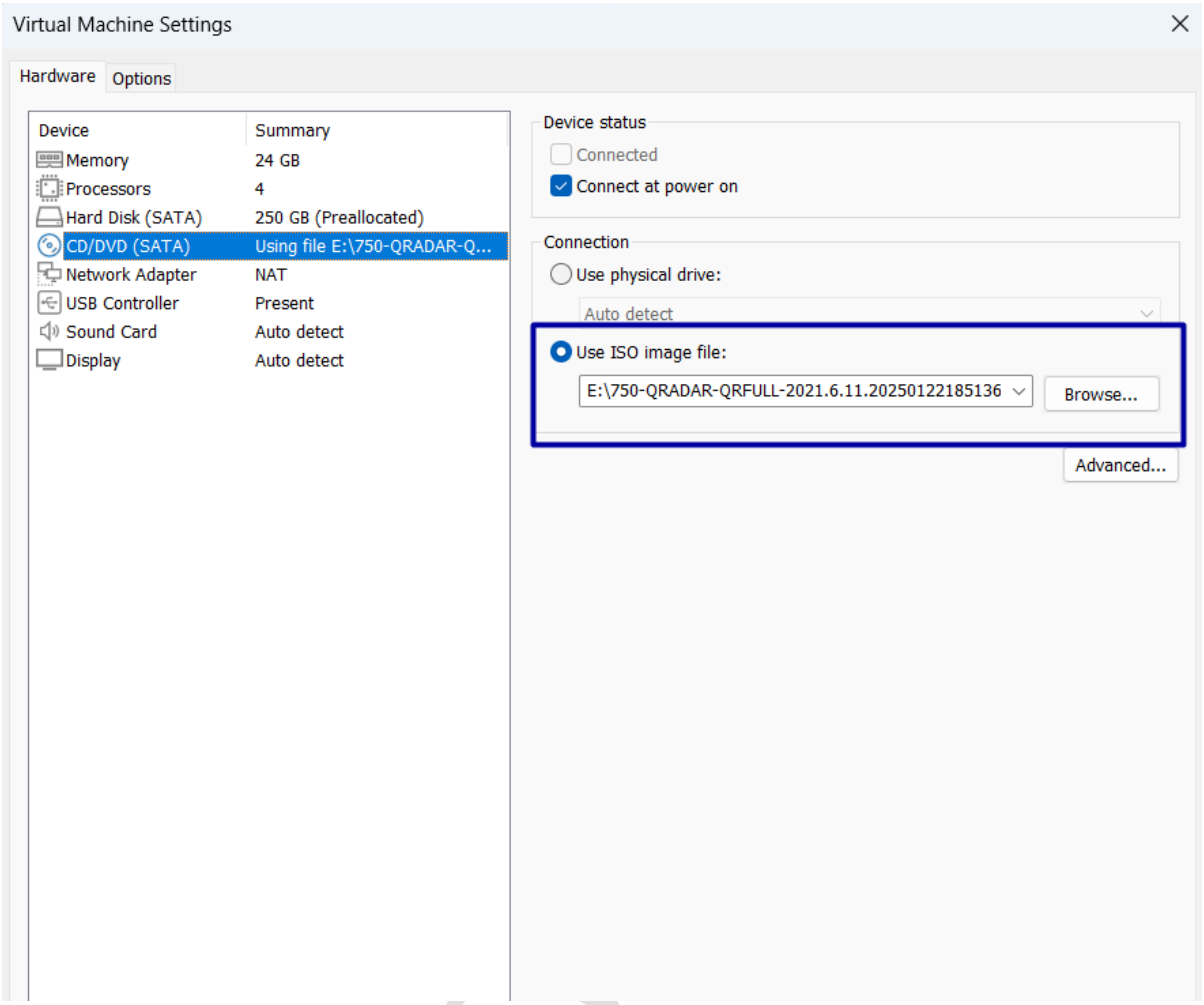
BIOS Settings:

- If you encounter boot issues, enable **UEFI mode**:
    - Go to VM Settings → Options → Advanced → Check **UEFI Firmware**



Boot from ISO:

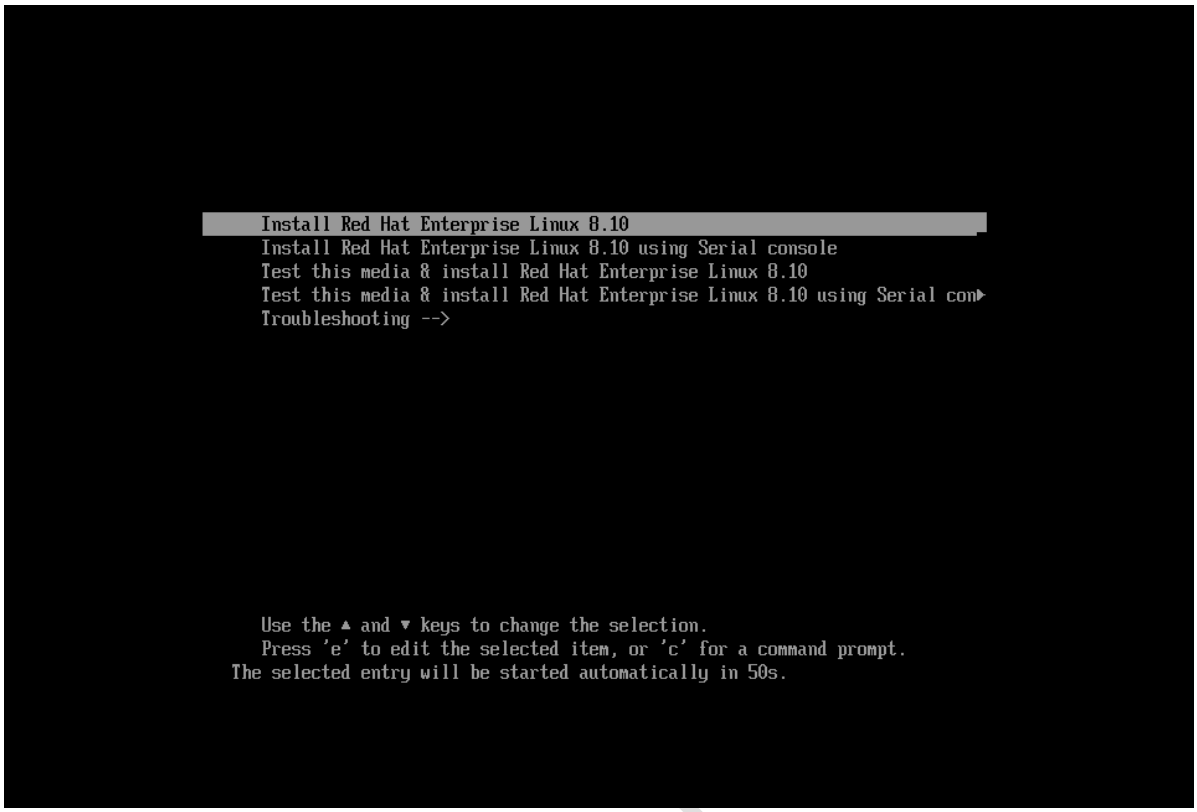
- Mount the downloaded QRadar ISO file and boot the virtual machine from it

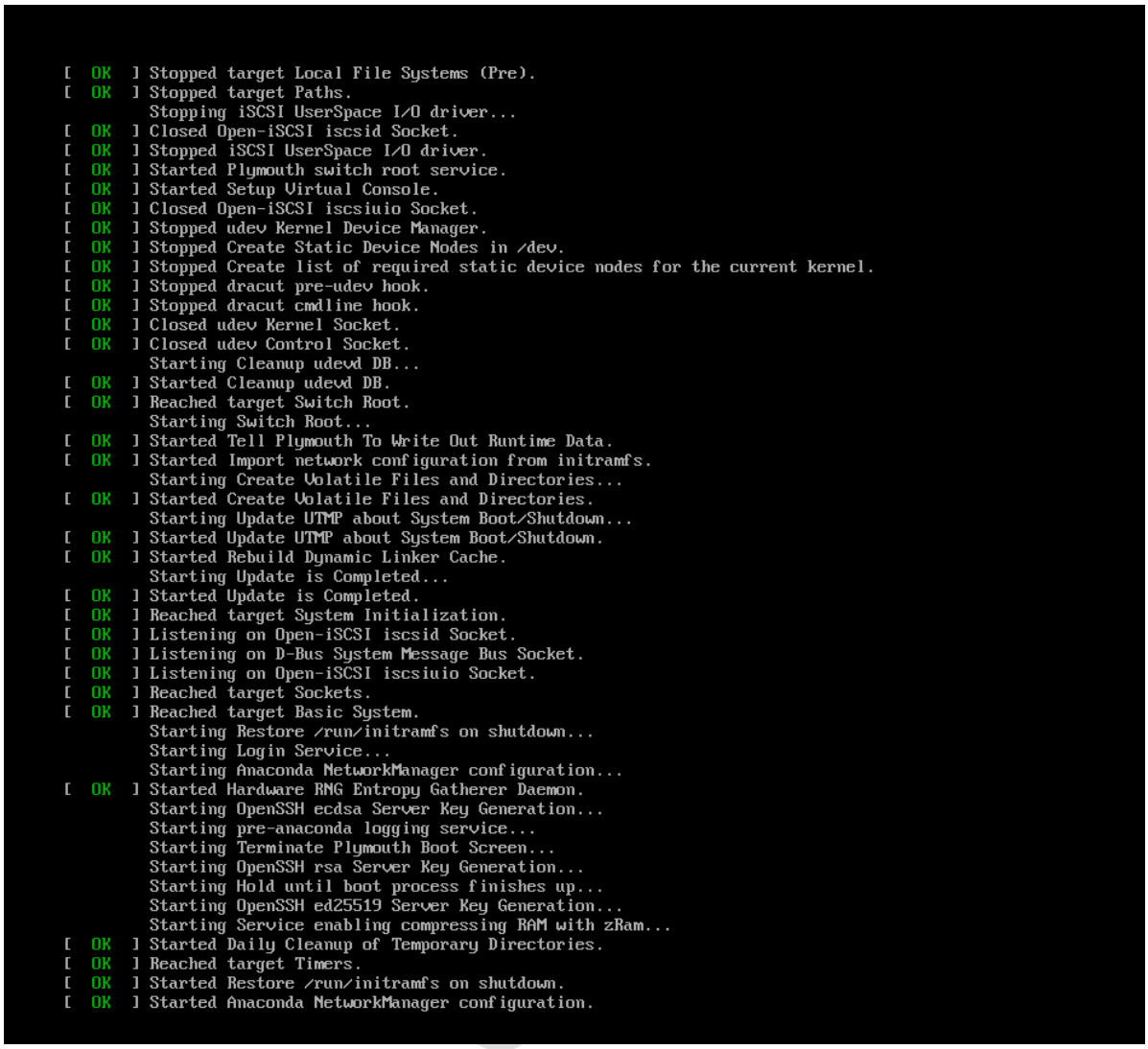


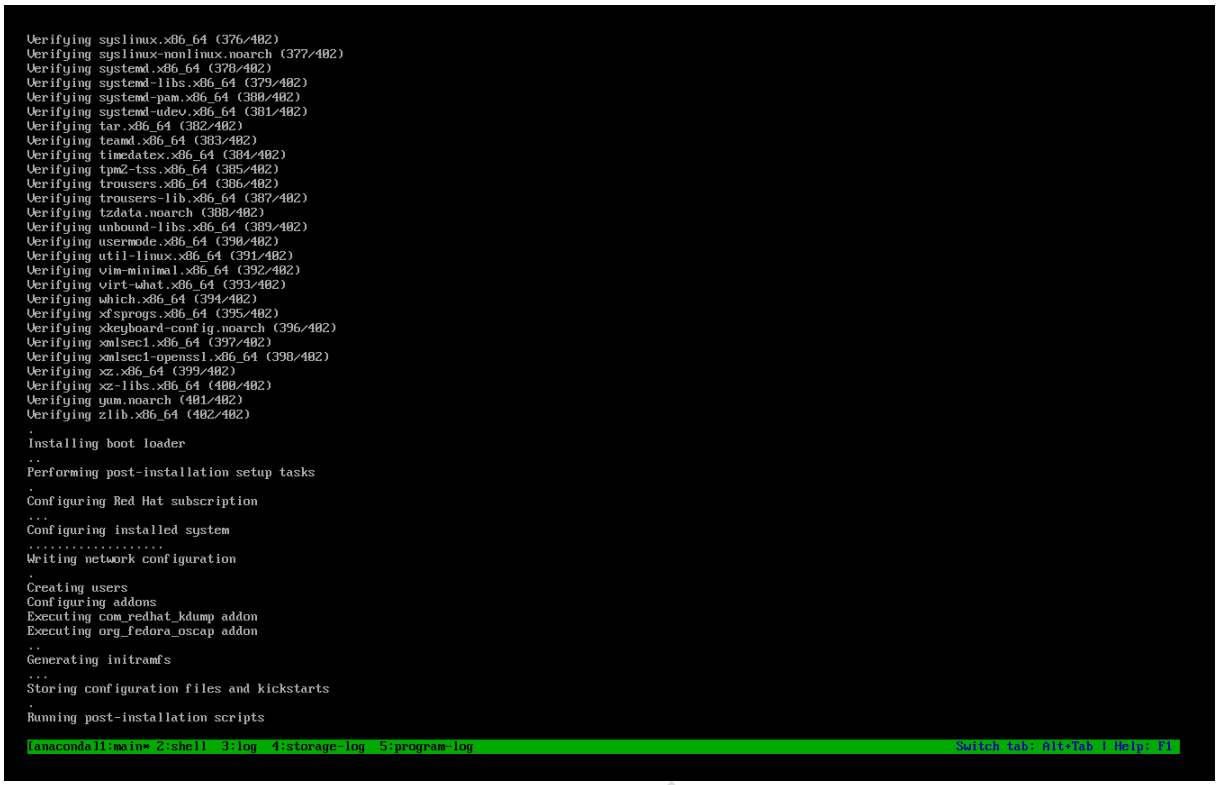
5. Installation:

Begin Installation

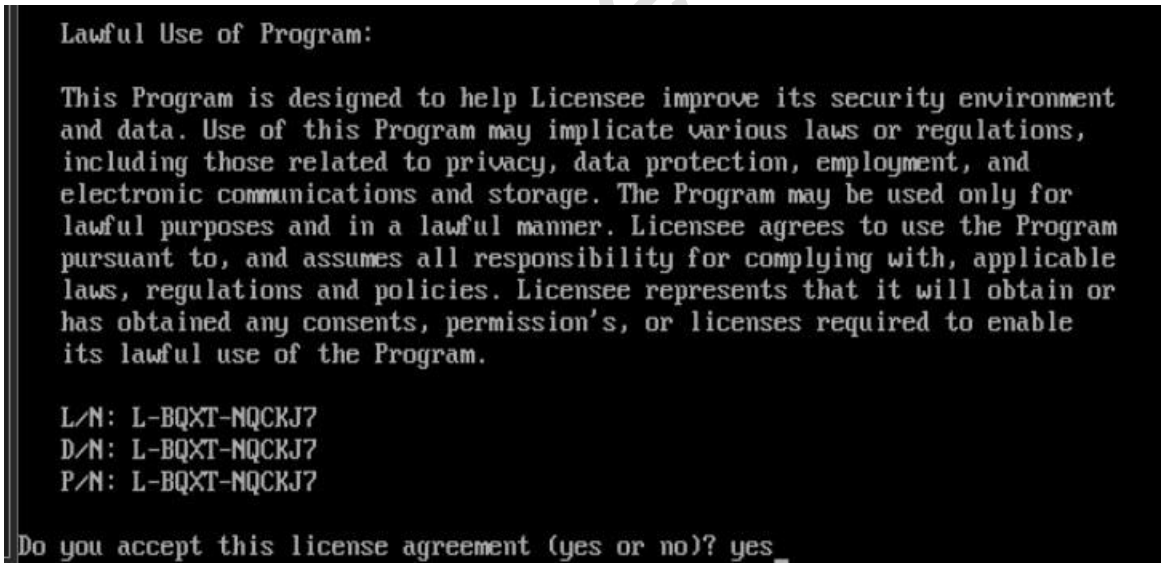
- Start the VM and allow the installation to run.
- Agree to the license agreement when prompted.


Install Red Hat Enterprise Linux 8.10
Install Red Hat Enterprise Linux 8.10 using Serial console
Test this media & install Red Hat Enterprise Linux 8.10
Test this media & install Red Hat Enterprise Linux 8.10 using Serial con
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 50s.


[OK] Stopped target Local File Systems (Pre).
[OK] Stopped target Paths.
Stopping iSCSI UserSpace I/O driver...
[OK] Closed Open-iSCSI iscsid Socket.
[OK] Stopped iSCSI UserSpace I/O driver.
[OK] Started Plymouth switch root service.
[OK] Started Setup Virtual Console.
[OK] Closed Open-iSCSI iscsiuio Socket.
[OK] Stopped udev Kernel Device Manager.
[OK] Stopped Create Static Device Nodes in /dev.
[OK] Stopped Create list of required static device nodes for the current kernel.
[OK] Stopped dracut pre-udev hook.
[OK] Stopped dracut cmdline hook.
[OK] Closed udev Kernel Socket.
[OK] Closed udev Control Socket.
Starting Cleanup udevd DB...
[OK] Started Cleanup udevd DB.
[OK] Reached target Switch Root.
Starting Switch Root...
[OK] Started Tell Plymouth To Write Out Runtime Data.
[OK] Started Import network configuration from initramfs.
Starting Create Volatile Files and Directories...
[OK] Started Create Volatile Files and Directories.
Starting Update UTMP about System Boot/Shutdown...
[OK] Started Update UTMP about System Boot/Shutdown.
[OK] Started Rebuild Dynamic Linker Cache.
Starting Update is Completed...
[OK] Started Update is Completed.
[OK] Reached target System Initialization.
[OK] Listening on Open-iSCSI iscsid Socket.
[OK] Listening on D-Bus System Message Bus Socket.
[OK] Listening on Open-iSCSI iscsiuio Socket.
[OK] Reached target Sockets.
[OK] Reached target Basic System.
Starting Restore /run/initramfs on shutdown...
Starting Login Service...
Starting Anaconda NetworkManager configuration...
[OK] Started Hardware RNG Entropy Gatherer Daemon.
Starting OpenSSH ecdsa Server Key Generation...
Starting pre-anaconda logging service...
Starting Terminate Plymouth Boot Screen...
Starting OpenSSH rsa Server Key Generation...
Starting Hold until boot process finishes up...
Starting OpenSSH ed25519 Server Key Generation...
Starting Service enabling compressing RAM with zRam...
[OK] Started Daily Cleanup of Temporary Directories.
[OK] Reached target Timers.
[OK] Started Restore /run/initramfs on shutdown.
[OK] Started Anaconda NetworkManager configuration.

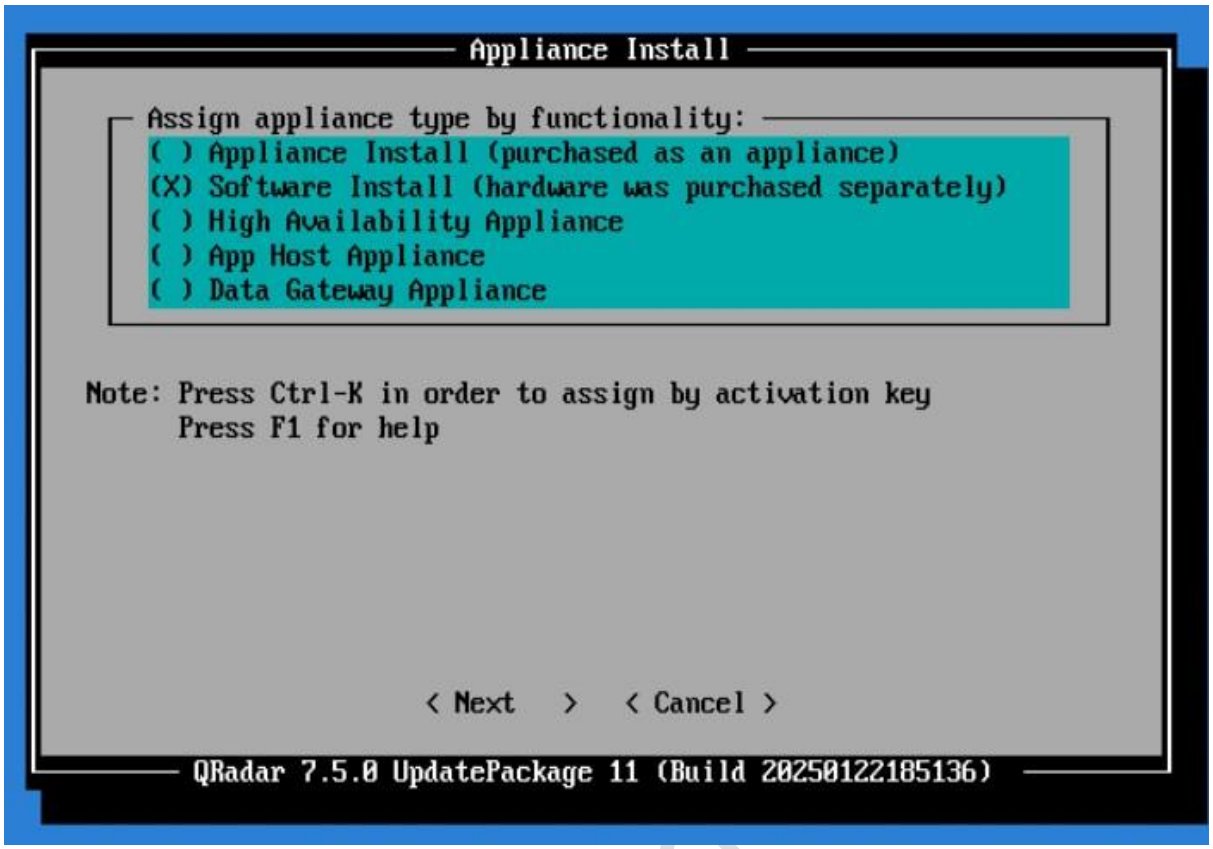


Then comes the license agreement we have to agree with it

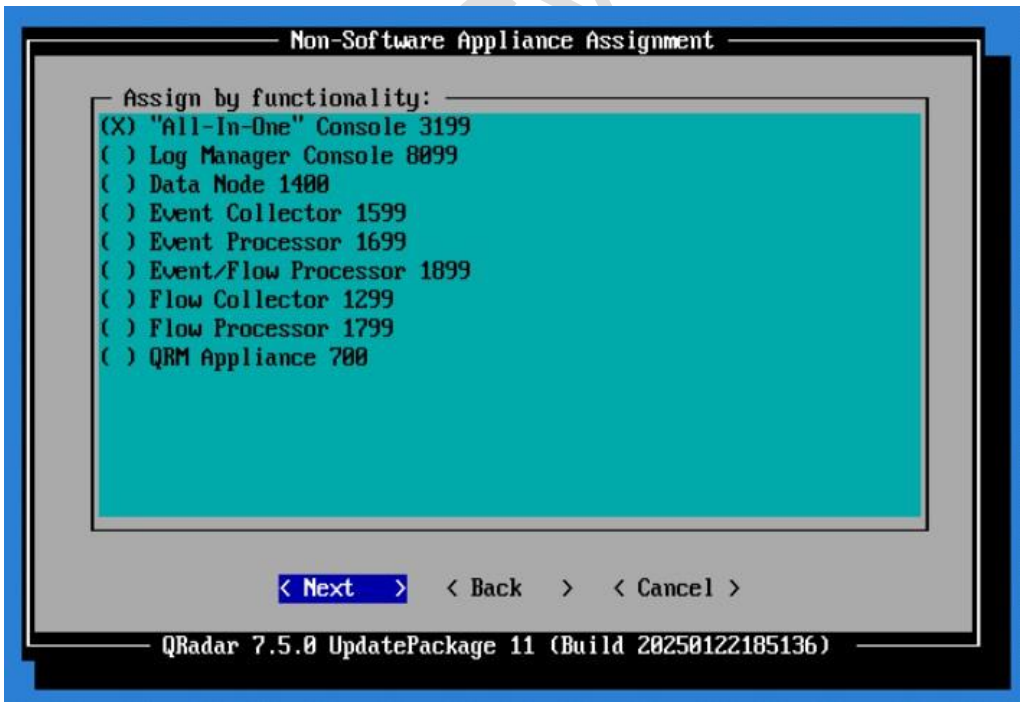


Software Install Selection

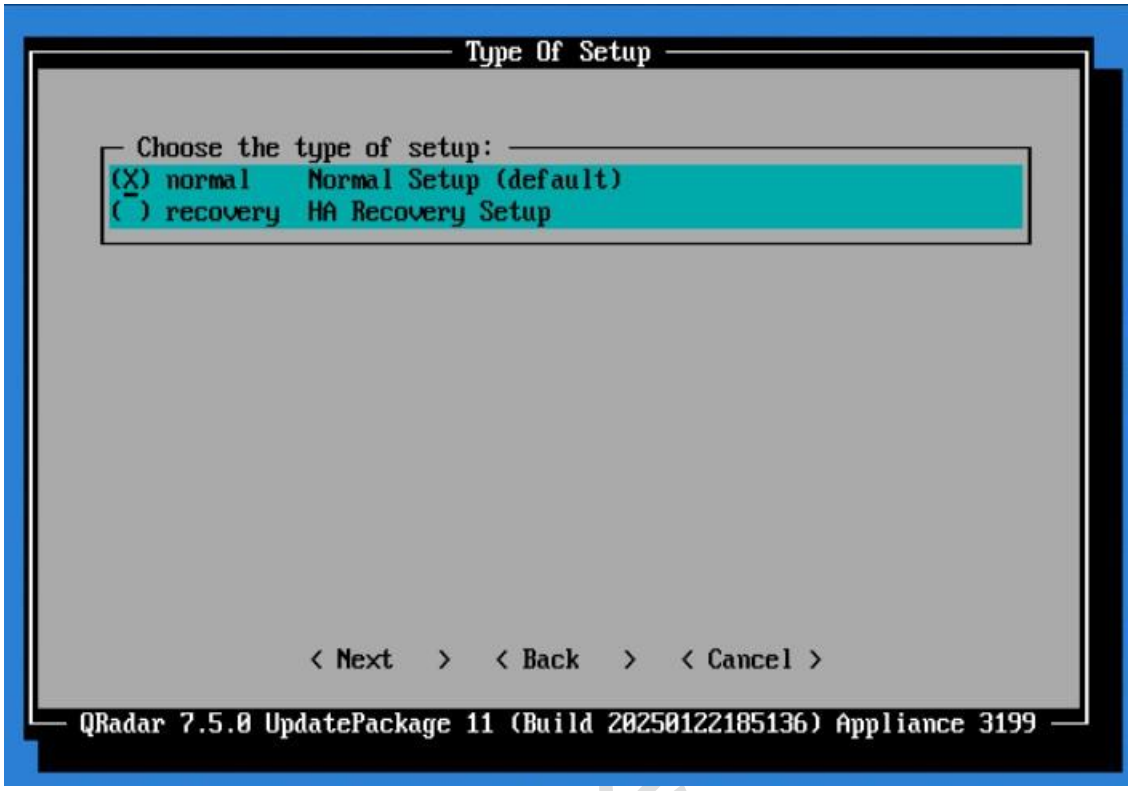
Now the most important steps comes we have to choose the Software Install option we can arrow keys and space bar for choosing options.

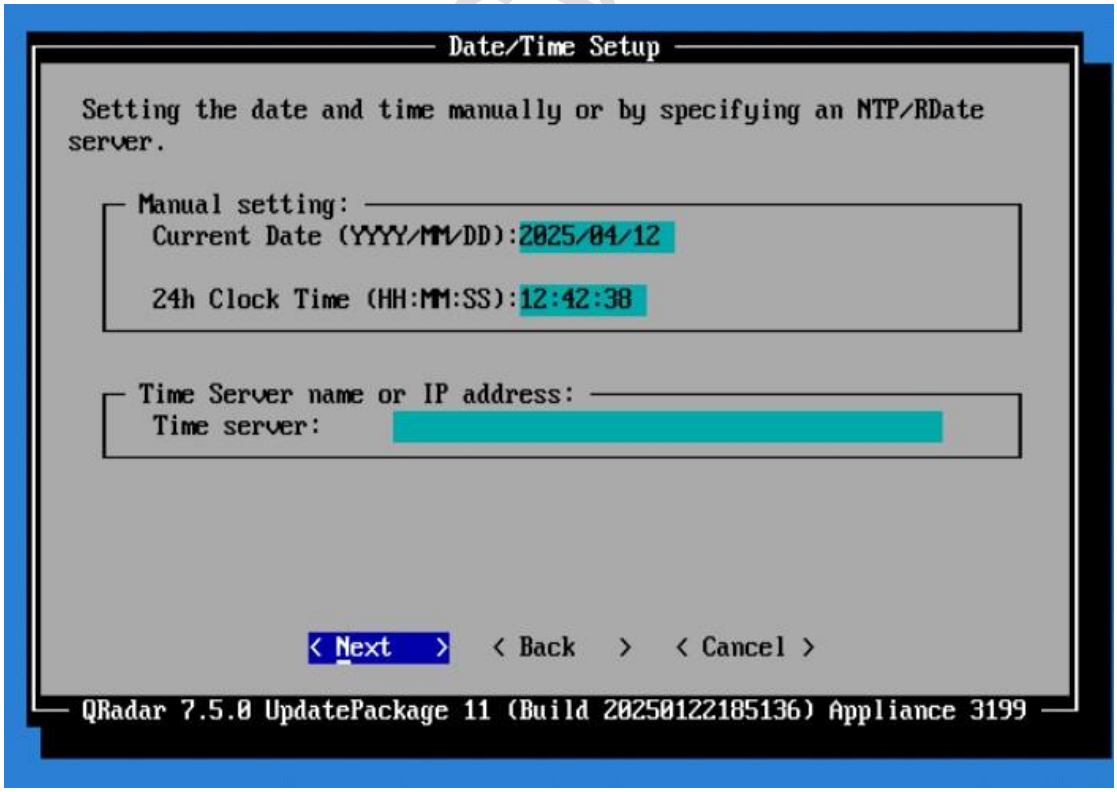


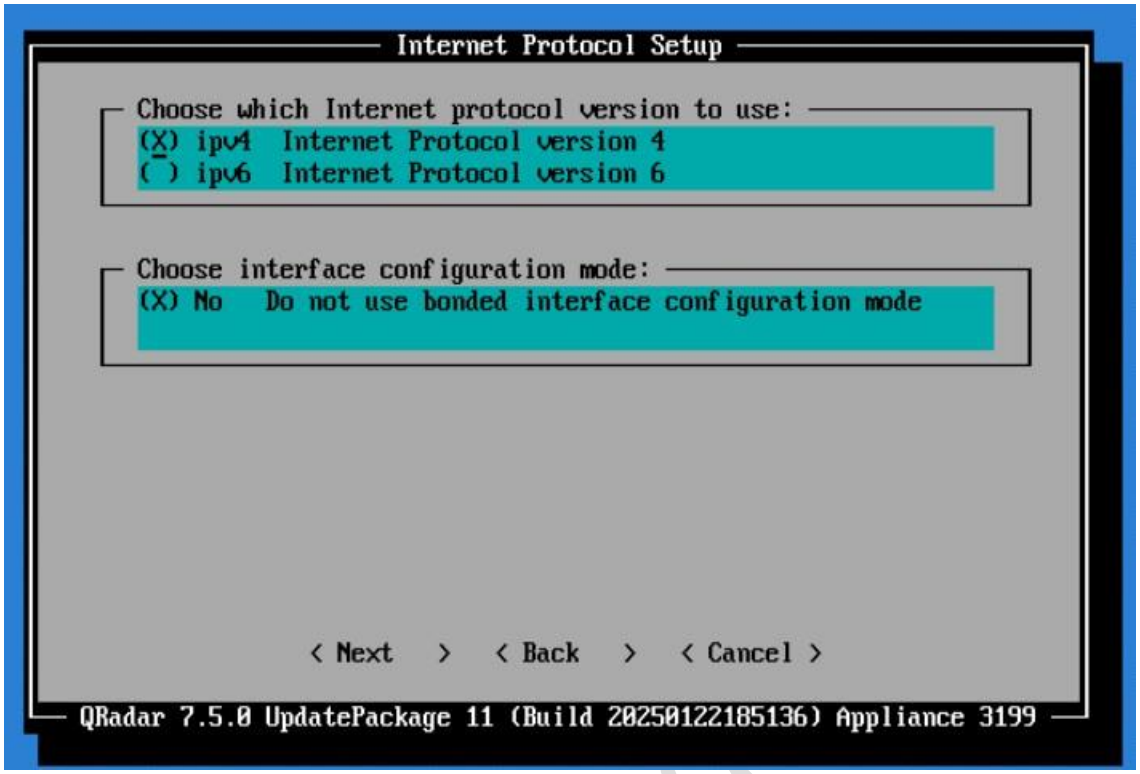
We have to choose all in one deployment

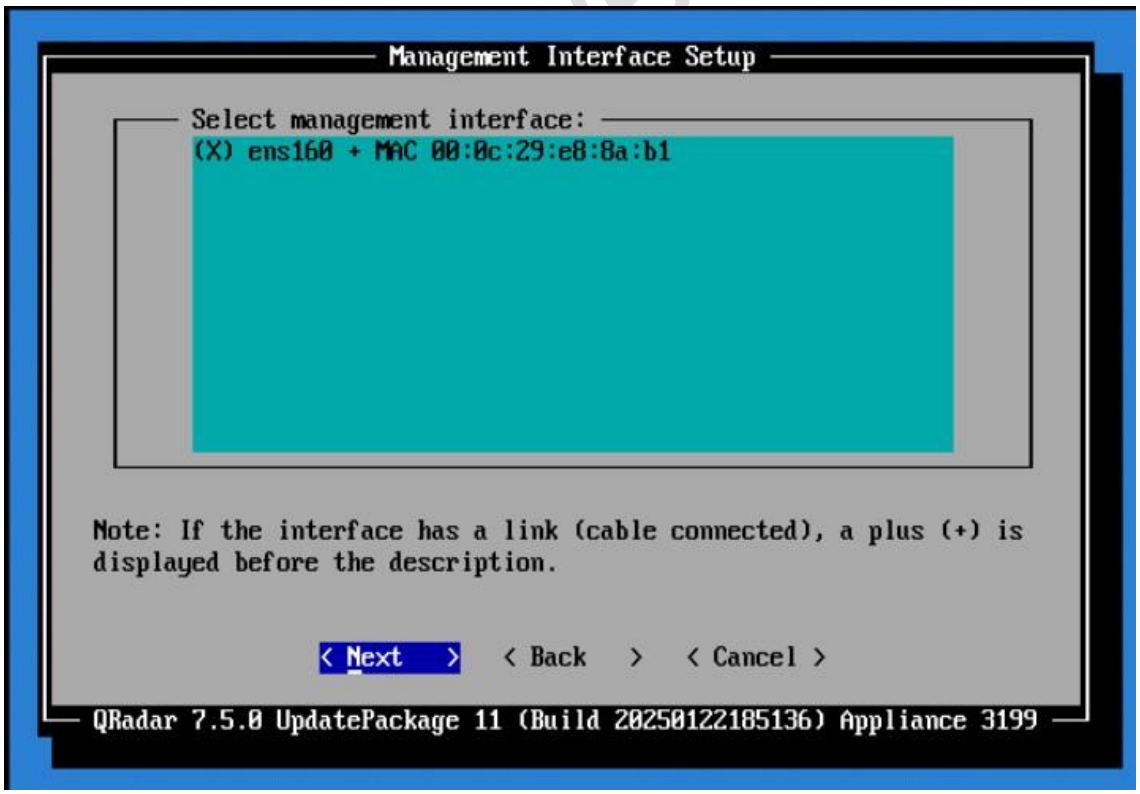


The setup type will be normal we will not be setting up HA





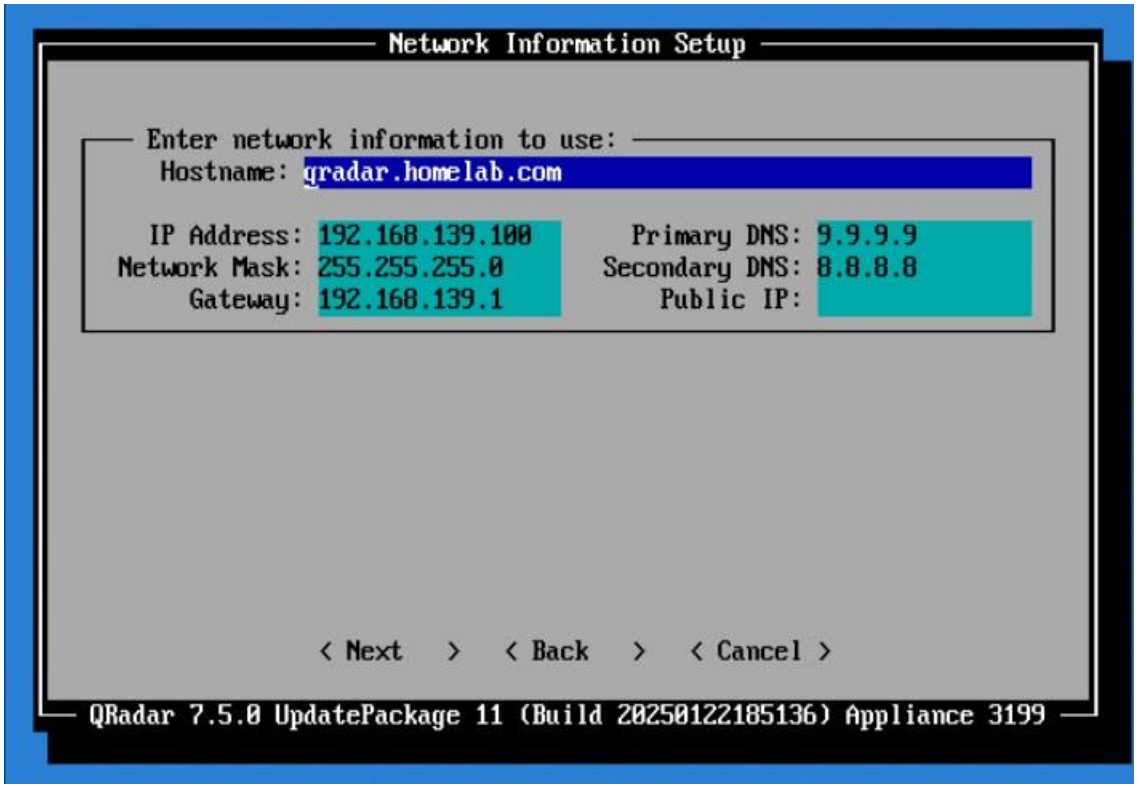

Internet Protocol Setup
Choose which Internet protocol version to use:
(X) ipv4 Internet Protocol version 4
( ) ipv6 Internet Protocol version 6
Choose interface configuration mode:
(X) No Do not use bonded interface configuration mode
< Next > < Back > < Cancel >
QRadar 7.5.0 UpdatePackage 11 (Build 20250122185136) Appliance 3199


Management Interface Setup
Select management interface:
(X) ens160 + MAC 00:0c:29:e8:8a:b1
Note: If the interface has a link (cable connected), a plus (+) is displayed before the description.
< Next > < Back > < Cancel >
QRadar 7.5.0 UpdatePackage 11 (Build 20250122185136) Appliance 3199

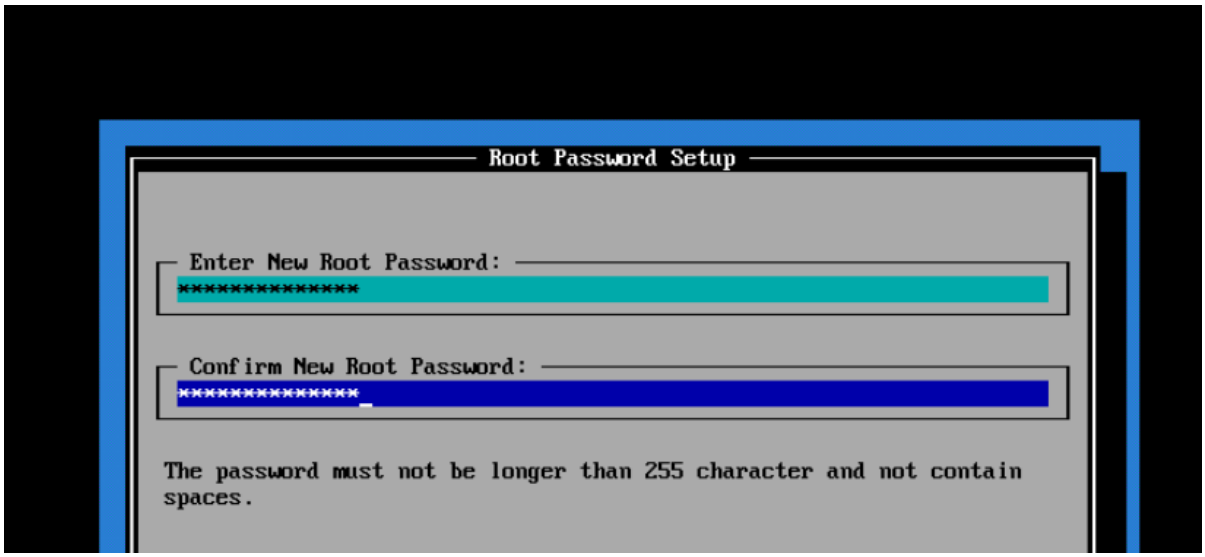
I used my VMware Network Adapter VMnet8's subnet for my QRadar's Network Setup

```
Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b8ae:7909:843:1ab2%11
   IPv4 Address. . . . . . . . . . . : 192.168.139.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter WiFi:
```

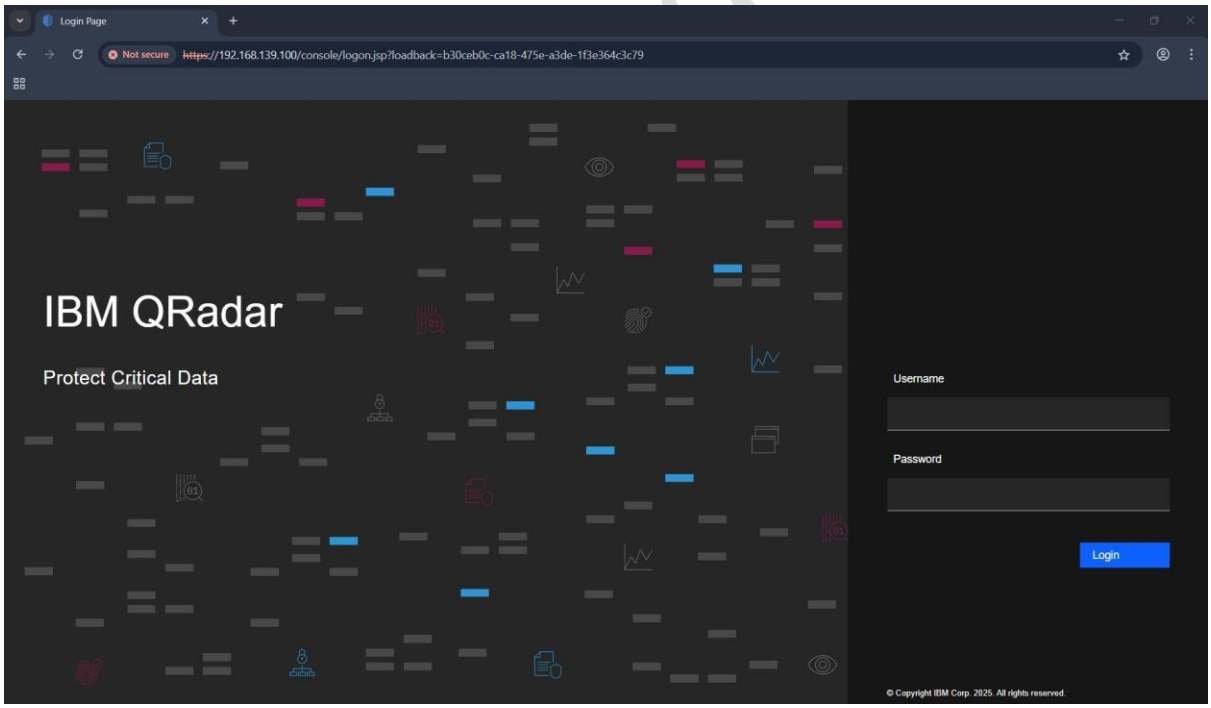
Below is my network setup



Then we have to setup root and GUI password



- The system will install DSM components and finalize setup.
- Once completed, you can access QRadar from a browser using your assigned IP, for example:
  - https://192.168.139.100
- Use the credentials that you entered in password setup

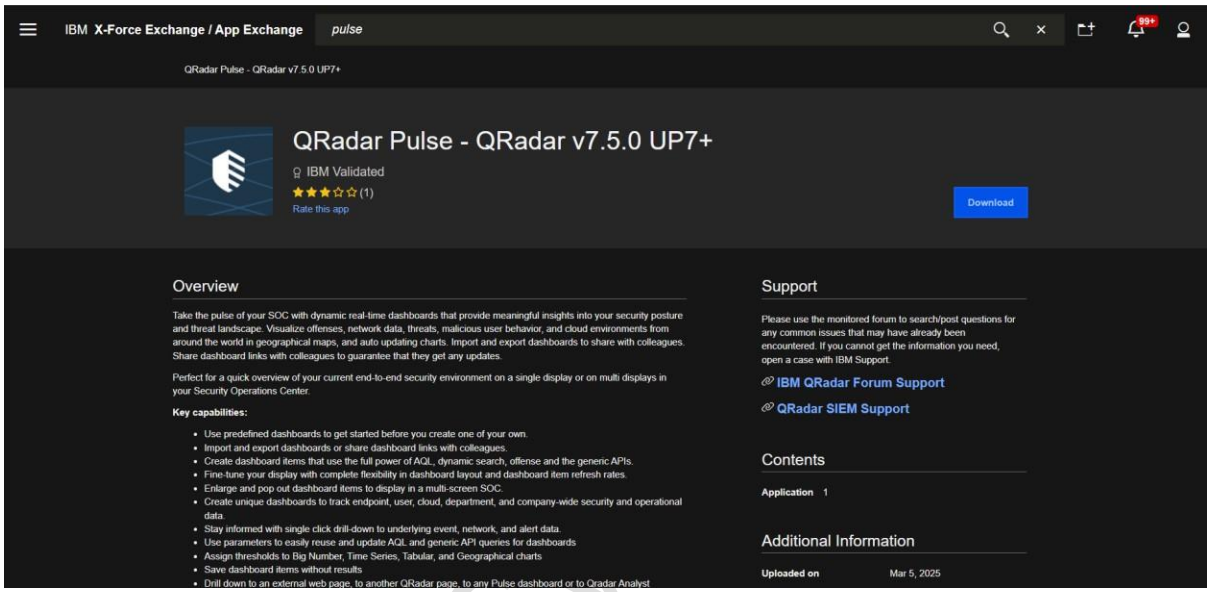


6. Pulse App Setup for Dashboards:

To enhance visualization and build custom dashboards in QRadar Community Edition, the **Pulse App** can be installed from IBM's X-Force App Exchange. Follow these steps to install it:

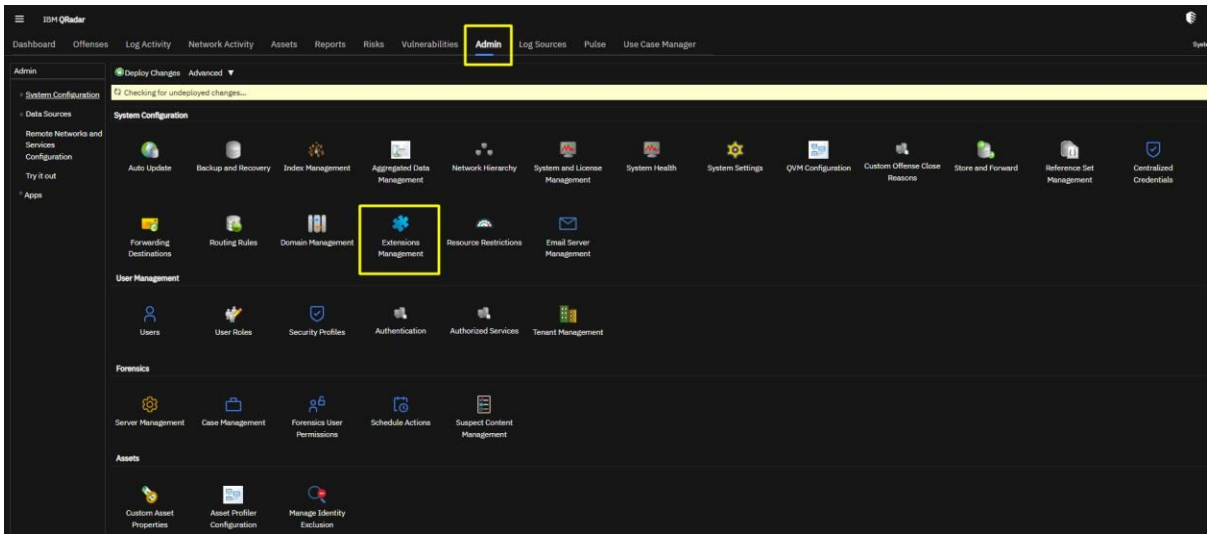
i. Download the App:

- Visit the following link and download the ZIP file for the Pulse App:
  ÷ [Pulse App on IBM X-Force Exchange]



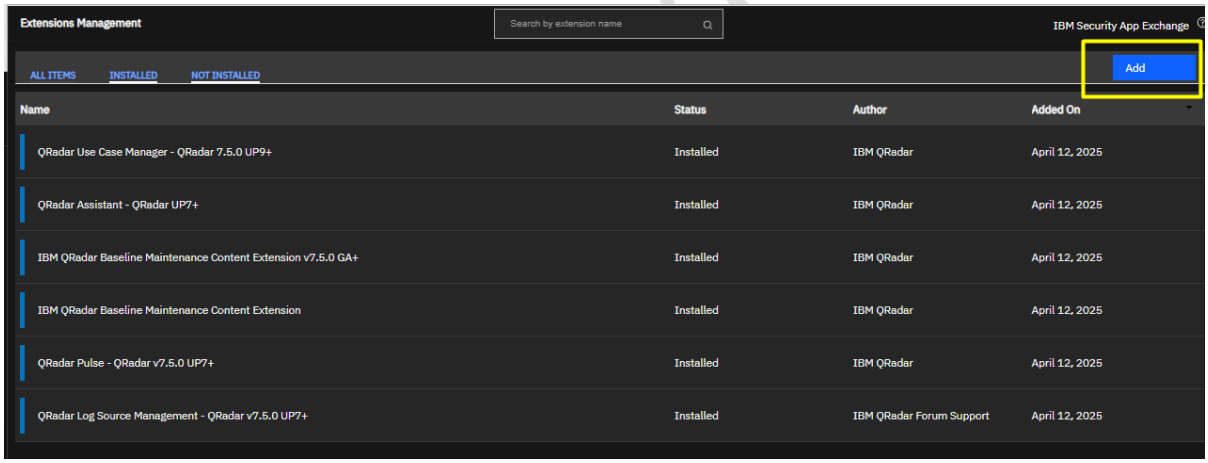
ii. Access Extension Management:

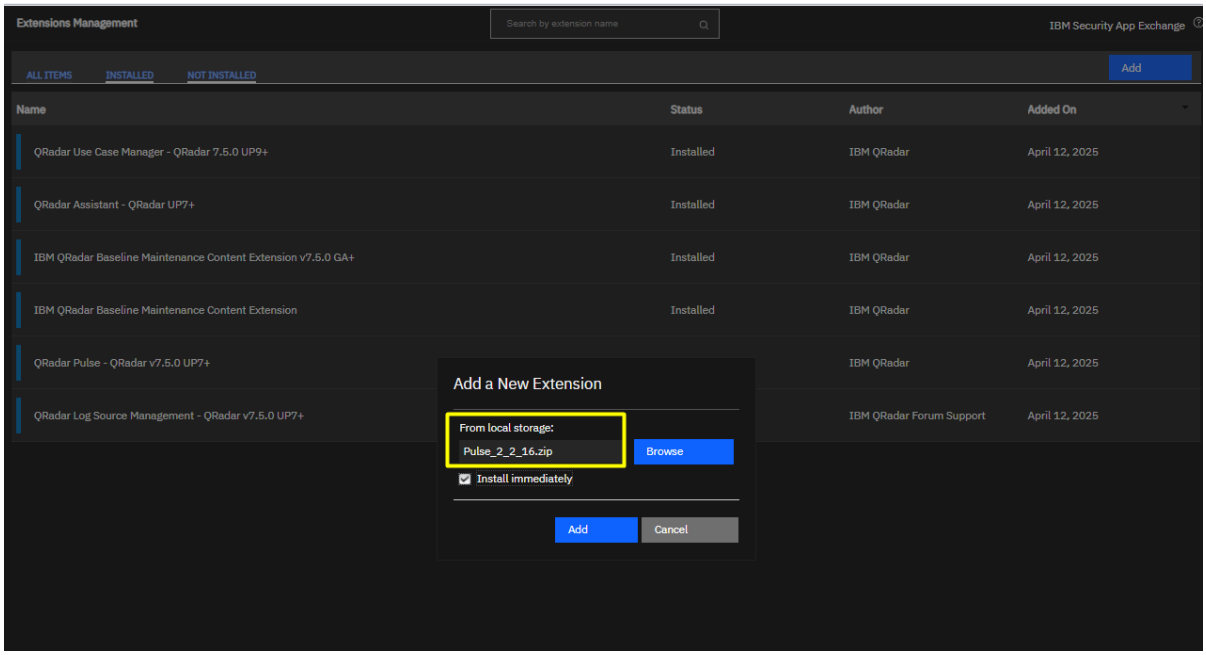
- Log in to the QRadar web interface.
- Navigate to the **Admin** tab.
- Under **System Configuration**, click on **Extension Management**.



iii. Install the App:

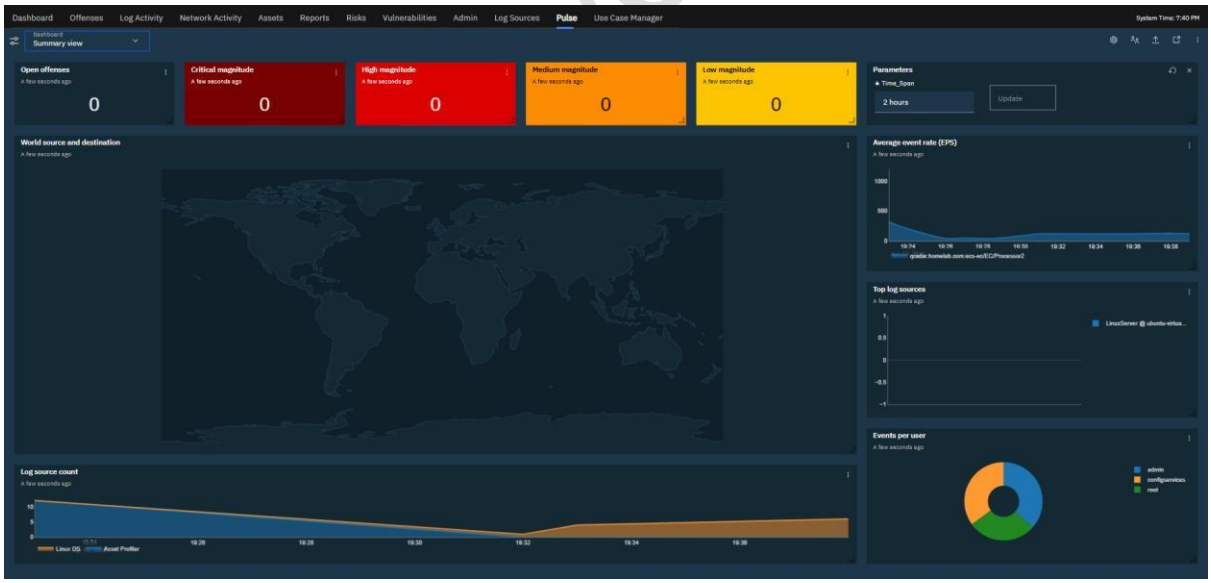
- In the Extension Management window, click **Add**.
- Upload the downloaded Pulse App ZIP file.
- QRadar will begin the installation automatically.





iv. Post-Installation:

- After successful installation, the Pulse App will appear under the **Dashboard** section.
- You can now view built-in statistics and visualizations, and also create your own custom dashboards tailored to your needs.



Tip: In addition to the Pulse App, QRadar supports a variety of other apps available via the IBM X-Force Exchange to further extend functionality for orchestration, monitoring, and threat intelligence.

7. Conclusion:

With the steps outlined above, I have successfully deployed IBM QRadar Community Edition in a virtualized home lab environment. This setup provides a hands-on opportunity to explore QRadar's powerful SIEM capabilities, monitor data flows, analyze security events, and build custom dashboards using the Pulse app.

Whether you're preparing for certification, running personal security research, or testing integrations, this home lab setup will serve as a solid foundation for your cybersecurity journey.