Continued Vulnerability Management Activities at the Institute for Defense Analyses

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

Navjot Singh is a student at George Mason University graduated with a bachelor's degree in Cybersecurity. He is currently pursuing a Master's in Digital Forensics through Mason's accelerated BAM (Bachelor's to Accelerated Masters) program. His academic background and recent internship experience have provided him with valuable knowledge in cybersecurity principles and vulnerability management.

Salome Kotei is a student at George Mason University pursuing a master's degree in Cybersecurity Engineering. She holds a bachelor's degree in Computer Science with a concentration in Cybersecurity and Project Management. She is committed to building a career in cybersecurity.

----- ***Industry Participant / Mentor*** -----

Christopher Murphy
Enterprise IT Operations Manager
Institute for Defense Analyses

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
Instructional Faculty, Dean's Teaching Fellow, & FWI Corporate Partner Faculty Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

Introduction

During our PREP project, we supported IDA's vulnerability management effort on their unclassified side. In the spring, the primary focus was on identifying and addressing system vulnerabilities using Tenable Security Center then remediation of the vulnerabilities. This summer, we took it a step further and planned to automate the process of identifying and addressing vulnerabilities on end user's systems.

Business Challenge

IDA was facing an increasing number of vulnerabilities across their systems and applications. These vulnerabilities ranged in severity, with some being critical or high risk, and posed a threat to the integrity and confidentiality of business operations. A major challenge was the lack of a streamlined process to ensure that findings from vulnerability scans were clearly communicated to the appropriate end users.

Activities Done to Address the Business Challenge

To address IDA's escalating vulnerability issues, we took the initiative to develop an automated process which would pull the vulnerability findings from Tenable for end users and email each user the vulnerabilities found on their systems and the steps they need to remediate these findings.

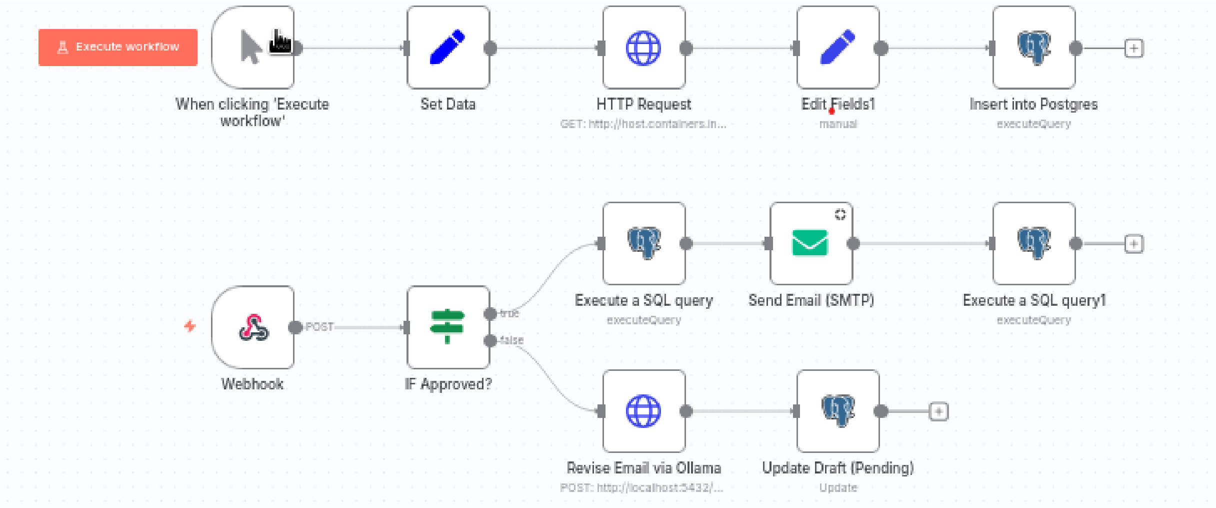
Results & Metrics

Over the span of 12 weeks, we were able to build and harden our own Linux RHEL system which we will host this project on, create SOPs for these Linux server processes, establish a workflow on n8n, and create kb documents for the remediation steps per application/vulnerability, and more.

Team Learning & Professional Development

Throughout the internship, we experienced continuous learning and skill development, both individually and collectively. We continued to use industry standard tools such as Tenable SC for vulnerability scanning and Active Directory for managing user accounts, improving our ability to identify, prioritize, and report vulnerabilities across systems. In addition, we learned how to use new tools such as Podman(Containerization), Remedy, n8n, PostgreSQL etc.

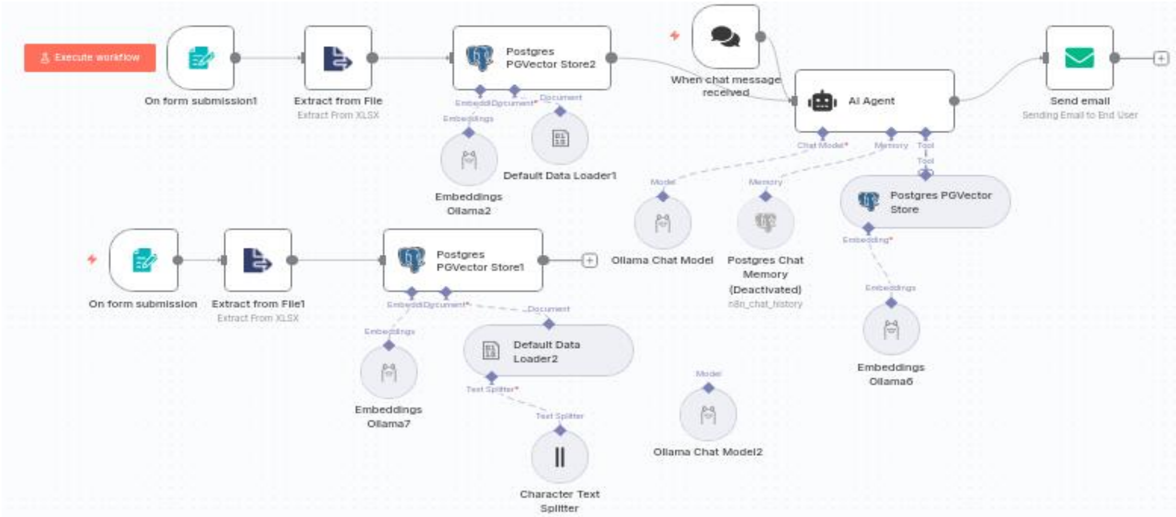
n8n Workflow – Draft 1



This is a draft of our n8n workflow. The first flow on top is for our AI agent, we've given it a prompt in the HTTP request and it generates an email and stores it into our Postgres database. The second flow is our system owner flow. This will receive feedback if the email is good, or if the system owner wants the AI to make changes. After that, it will send an email to the user about their vuln.

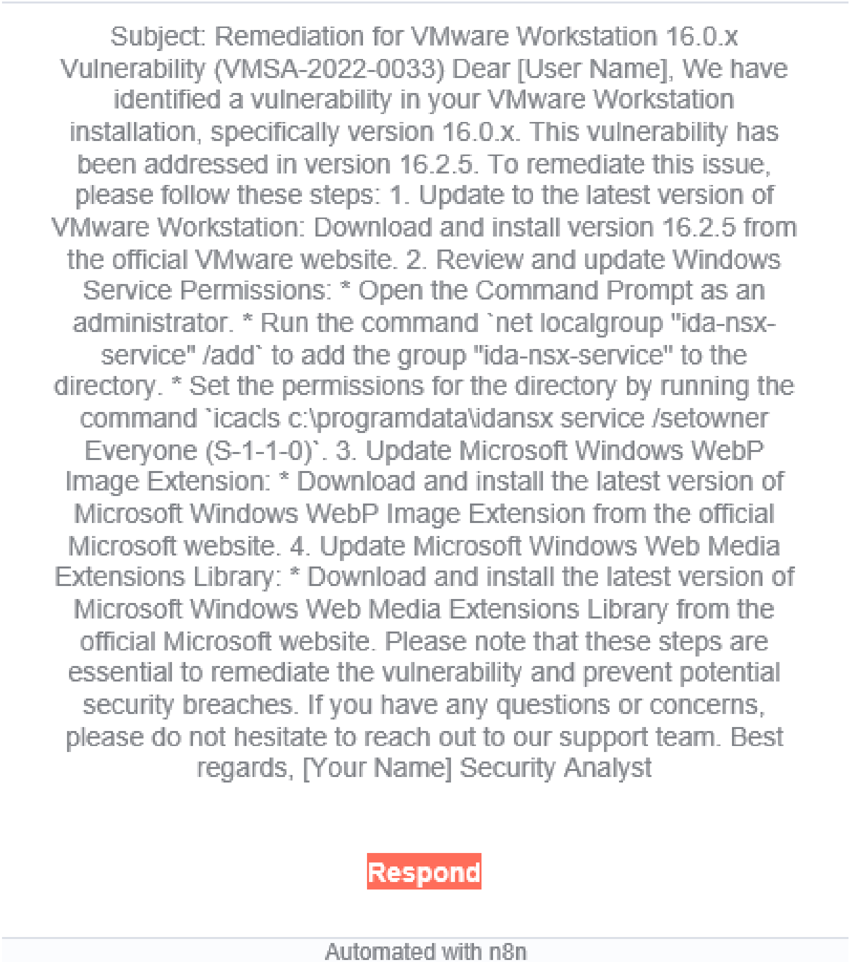
A key milestone was building a server using Nutanix and hardening the server, which deepened our understanding of virtual infrastructure and system deployment. This experience provided valuable insight into the backend setup that supports secure enterprise operations. Below is an example of the steps taken to build a Linux server and the end result.

N8N Draft 2



This is the second draft for our workflow. We have refined our process of inserting and downloading Vulnerability excel sheet and Knowledge Base excel sheet. We have several vector store that gather and pinpoint contents of files. Those vector store then feed into the AI as a tool for AI to look up references and use the knowledge base. This AI model is called **RAG**(**Retrieval-Augmented Generation**). This allows the AI to look at external data sources such as knowledge base and use that context to provide accurate information. We are using this model because this helps us optimize the email output accurately.

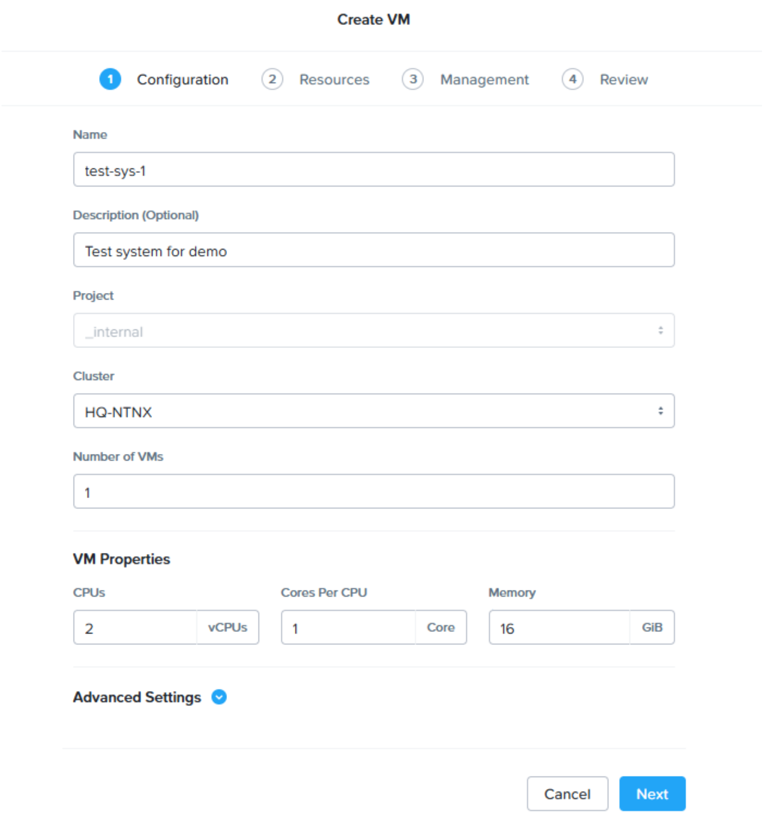
N8N sample email



Subject: Remediation for VMware Workstation 16.0.x Vulnerability (VMSA-2022-0033) Dear [User Name], We have identified a vulnerability in your VMware Workstation installation, specifically version 16.0.x. This vulnerability has been addressed in version 16.2.5. To remediate this issue, please follow these steps: 1. Update to the latest version of VMware Workstation: Download and install version 16.2.5 from the official VMware website. 2. Review and update Windows Service Permissions: * Open the Command Prompt as an administrator. * Run the command `net localgroup "ida-nsx-service" /add` to add the group "ida-nsx-service" to the directory. * Set the permissions for the directory by running the command `icacls c:\programdata\idansx service /setowner Everyone (S-1-1-0)`. 3. Update Microsoft Windows WebP Image Extension: * Download and install the latest version of Microsoft Windows WebP Image Extension from the official Microsoft website. 4. Update Microsoft Windows Web Media Extensions Library: * Download and install the latest version of Microsoft Windows Web Media Extensions Library from the official Microsoft website. Please note that these steps are essential to remediate the vulnerability and prevent potential security breaches. If you have any questions or concerns, please do not hesitate to reach out to our support team. Best regards, [Your Name] Security Analyst

This is a sample email that was sent to security analyst. The security analyst then has a respond option to either send out that email or have respond to the AI to correct its output.

How to Build a Linux Server



Create VM

Name: test-sys-1

Description (Optional): Test system for demo

Project: _internal

Cluster: HQ-NTNX

Number of VMs: 1

VM Properties

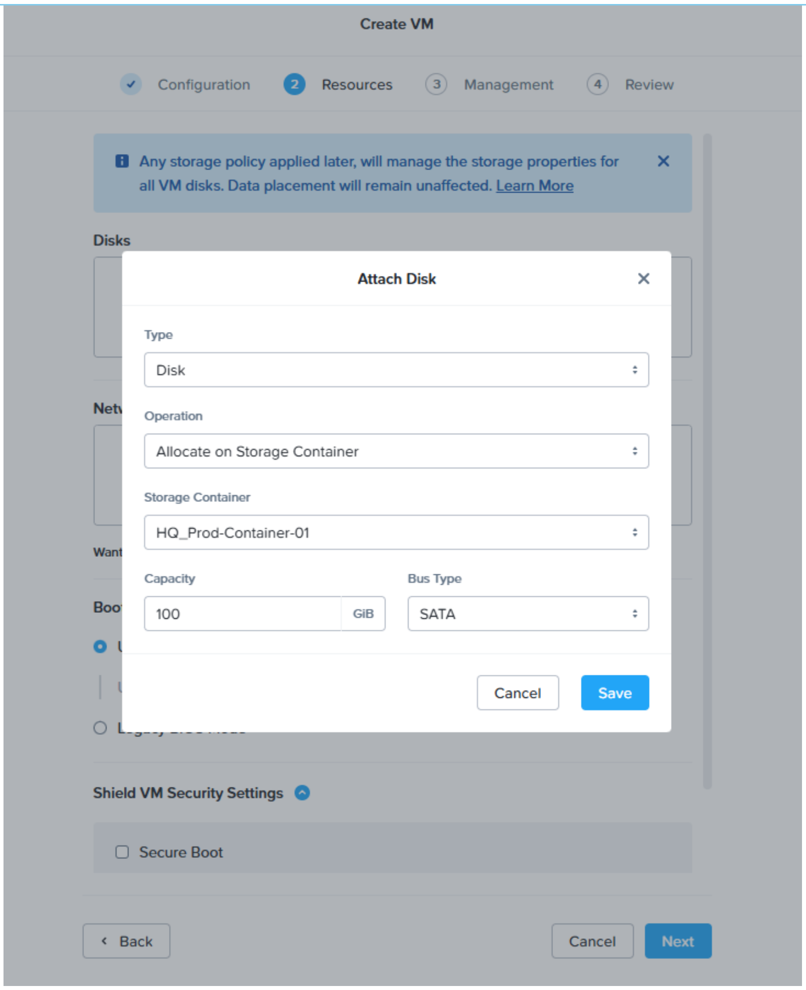
CPUs: 2 vCPUs

Cores Per CPU: 1 Core

Memory: 16 GiB

Advanced Settings

The first step of building a server in Nutanix is the configuration. You need to give the system a name, add a description, then set up the properties.



Any storage policy applied later, will manage the storage properties for all VM disks. Data placement will remain unaffected. Learn More

☐ Secure Boot

Attach Disk

Type: Disk

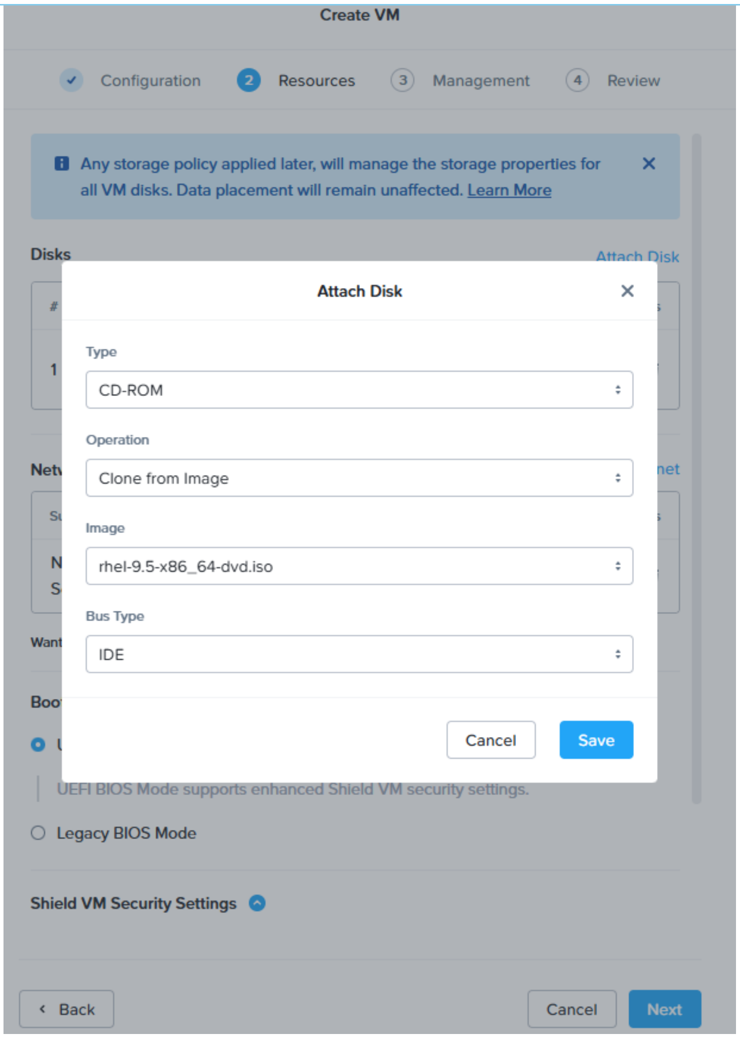
Operation: Allocate on Storage Container

Storage Container: HQ_Prod-Container-01

Capacity: 100 GiB

Bus Type: SATA

Next, you will attach two disks to the system. The first disk type is a disk which we will allocate on storage container and select a container. Then, you will put it at your desired capacity.


Create VM
Configuration
2 Resources
3 Management
4 Review
Any storage policy applied later, will manage the storage properties for all VM disks. Data placement will remain unaffected. Learn More
Disks
Attach Disk
Attach Disk
UEFI BIOS Mode supports enhanced Shield VM security settings.
○ Legacy BIOS Mode
Shield VM Security Settings
Cancel
Save
Back
Cancel
Next

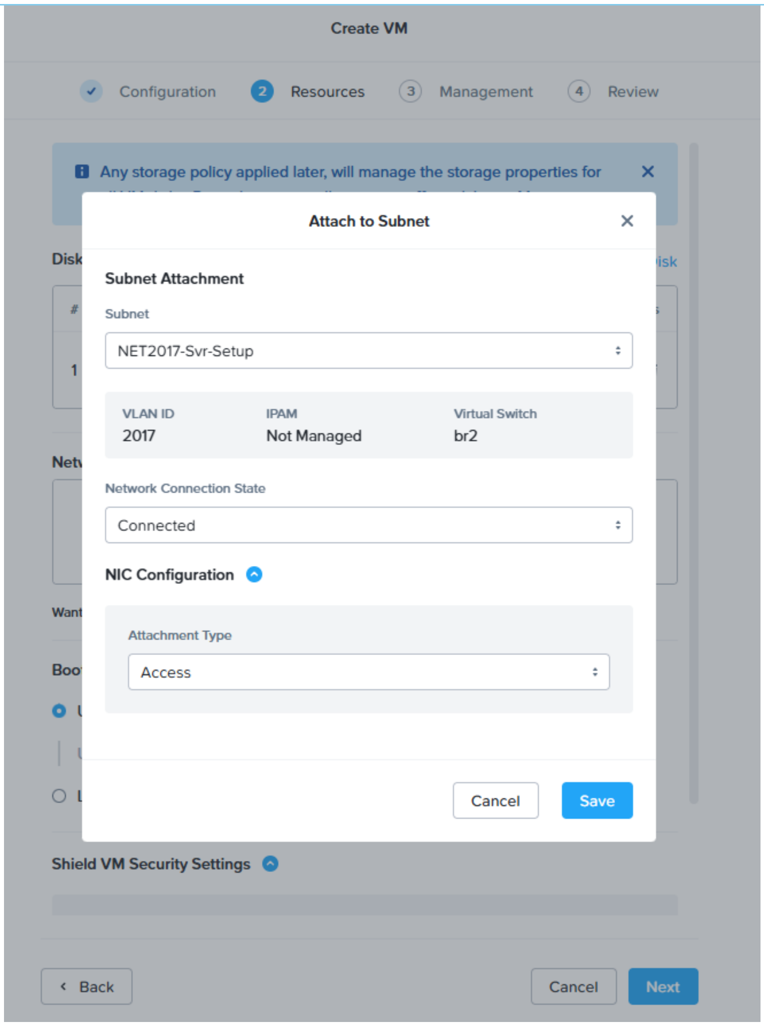
Type: CD-ROM

Operation: Clone from Image

Image: rhel-9.5-x86_64-dvd.iso

Bus Type: IDE

The next disk type is a CD-ROM, we will clone from image and select the RHEL 9.5-x86 image. If you want a different OS for the system, you may choose another option.



Any storage policy applied later, will manage the storage properties for

Attach to Subnet

Subnet Attachment

Subnet: NET2017-Svr-Setup

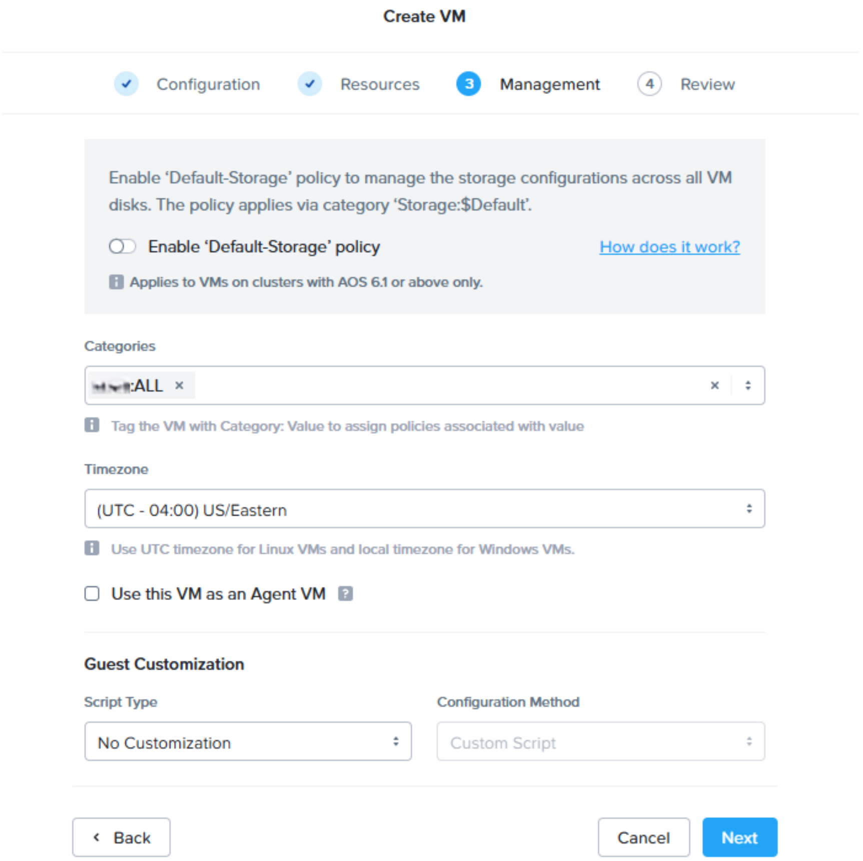
VLAN ID	IPAM	Virtual Switch
2017	Not Managed	br2

Network Connection State: Connected

NIC Configuration

Attachment Type: Access

Here, we attach a subnet and leave the network connection and attachment type as is. For this server we selected NET2017.



Create VM

✓ Configuration ✓ Resources 3 Management 4 Review

Enable 'Default-Storage' policy to manage the storage configurations across all VM disks. The policy applies via category 'Storage:$Default'.

○ Enable 'Default-Storage' policy

How does it work?

Applies to VMs on clusters with AOS 6.1 or above only.

Categories

[redacted]:ALL ×

Tag the VM with Category: Value to assign policies associated with value

Timezone

(UTC - 04:00) US/Eastern

Use UTC timezone for Linux VMs and local timezone for Windows VMs.

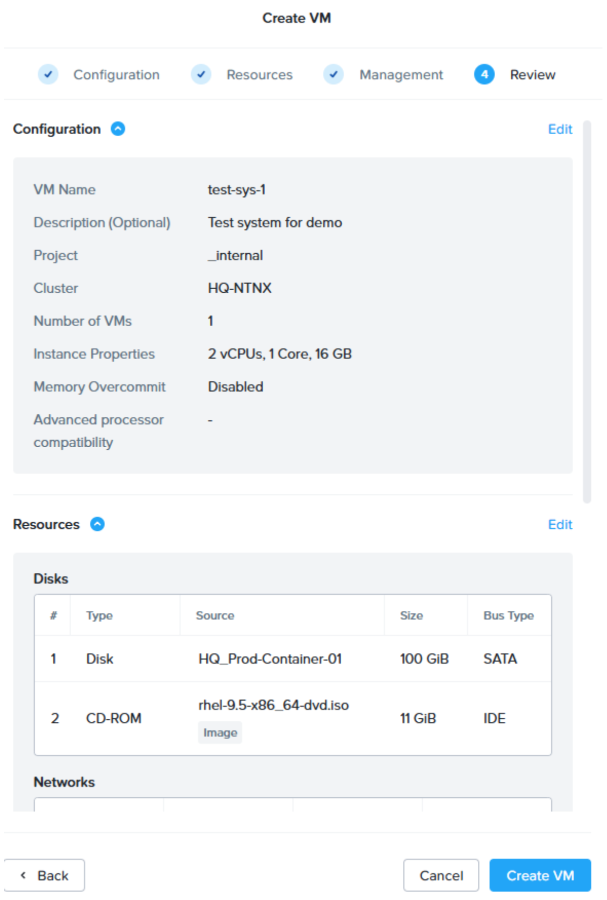
□ Use this VM as an Agent VM

Guest Customization

Script Type: No Customization

Configuration Method: Custom Script

Few final steps, we will select who we want to have access to this server and change the time zone to EST.



Configuration

VM Name	test-sys-1
Description (Optional)	Test system for demo
Project	_internal
Cluster	HQ-NTNX
Number of VMs	1
Instance Properties	2 vCPUs, 1 Core, 16 GB
Memory Overcommit	Disabled
Advanced processor compatibility	-

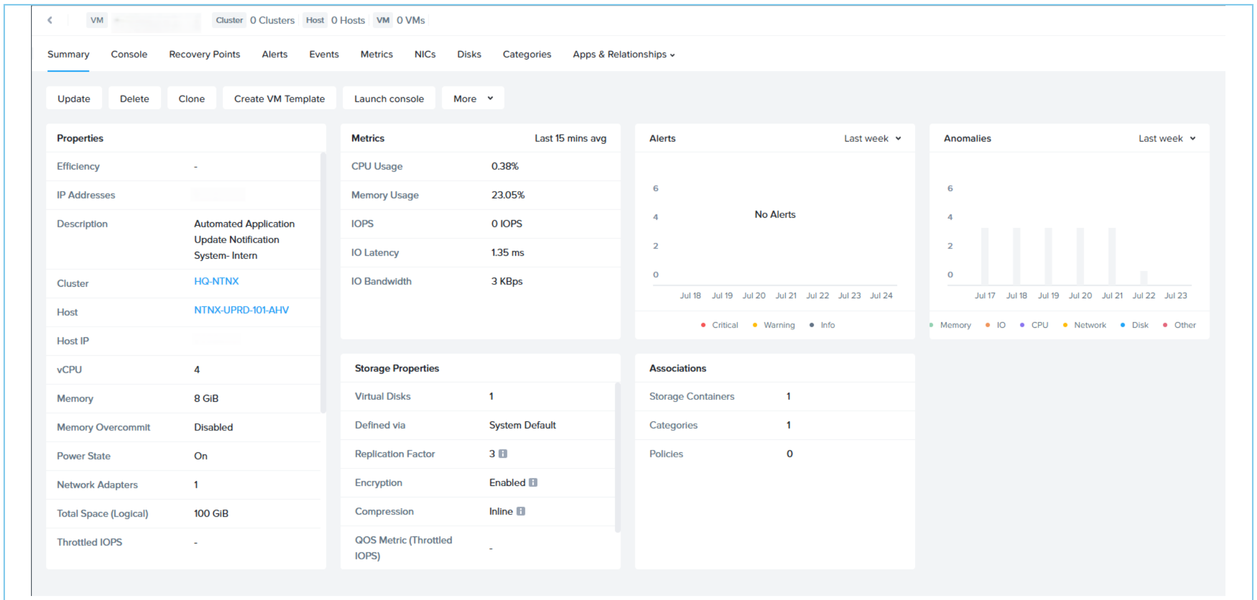
Resources

Disks

#	Type	Source	Size	Bus Type
1	Disk	HQ_Prod-Container-01	100 GiB	SATA
2	CD-ROM	rhel-9.5-x86_64-dvd.iso Image	11 GiB	IDE

Networks

Lastly, just review your selections and hit create VM. That’s it!



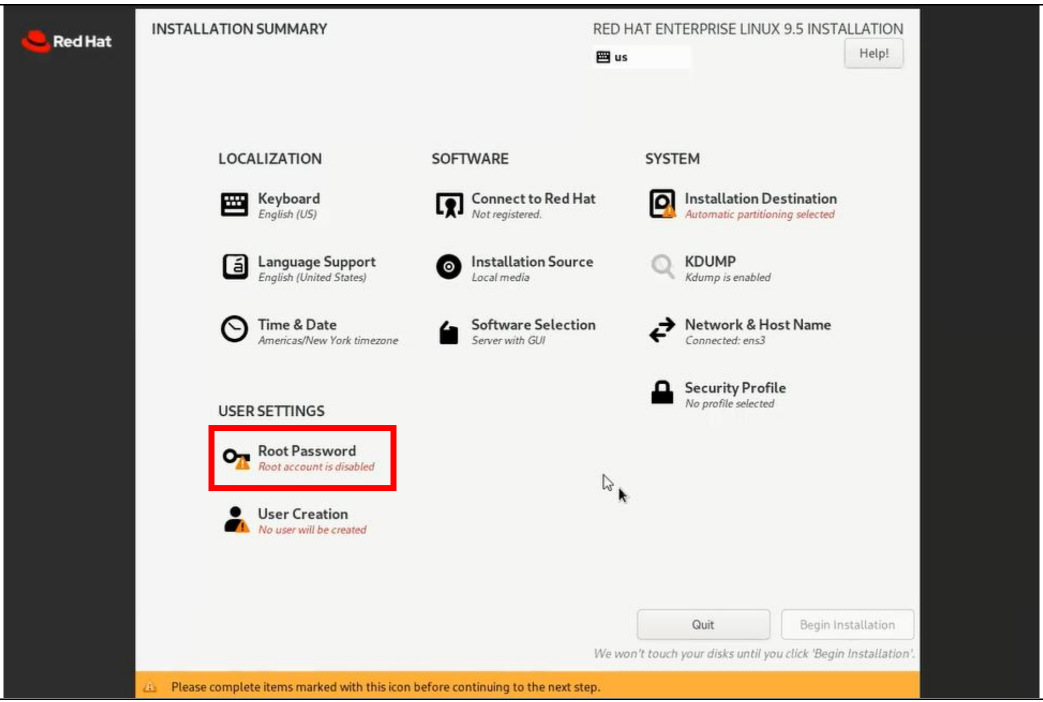
Properties	
Efficiency	-
IP Addresses	[redacted]
Description	Automated Application Update Notification System- Intern
Cluster	HQ-NTNX
Host	NTNX-UPRD-101-AHV
Host IP	[redacted]
vCPU	4
Memory	8 GiB
Memory Overcommit	Disabled
Power State	On
Network Adapters	1
Total Space (Logical)	100 GiB
Throttled IOPS	-

Metrics	Last 15 mins avg
CPU Usage	0.38%
Memory Usage	23.05%
IOPS	0 IOPS
IO Latency	1.35 ms
IO Bandwidth	3 KBps

Storage Properties	
Virtual Disks	1
Defined via	System Default
Replication Factor	3
Encryption	Enabled
Compression	Inline
QOS Metric (Throttled IOPS)	-

Associations	
Storage Containers	1
Categories	1
Policies	0

Here is a summary of what your new server will look like. After this, you can power on the device and launch the console, so we can finish the build.



INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 9.5 INSTALLATION

LOCALIZATION

- Keyboard — *English (US)*
- Language Support — *English (United States)*
- Time & Date — *Americas/New York timezone*

SOFTWARE

- Connect to Red Hat — *Not registered.*
- Installation Source — *Local media*
- Software Selection — *Server with GUI*

SYSTEM

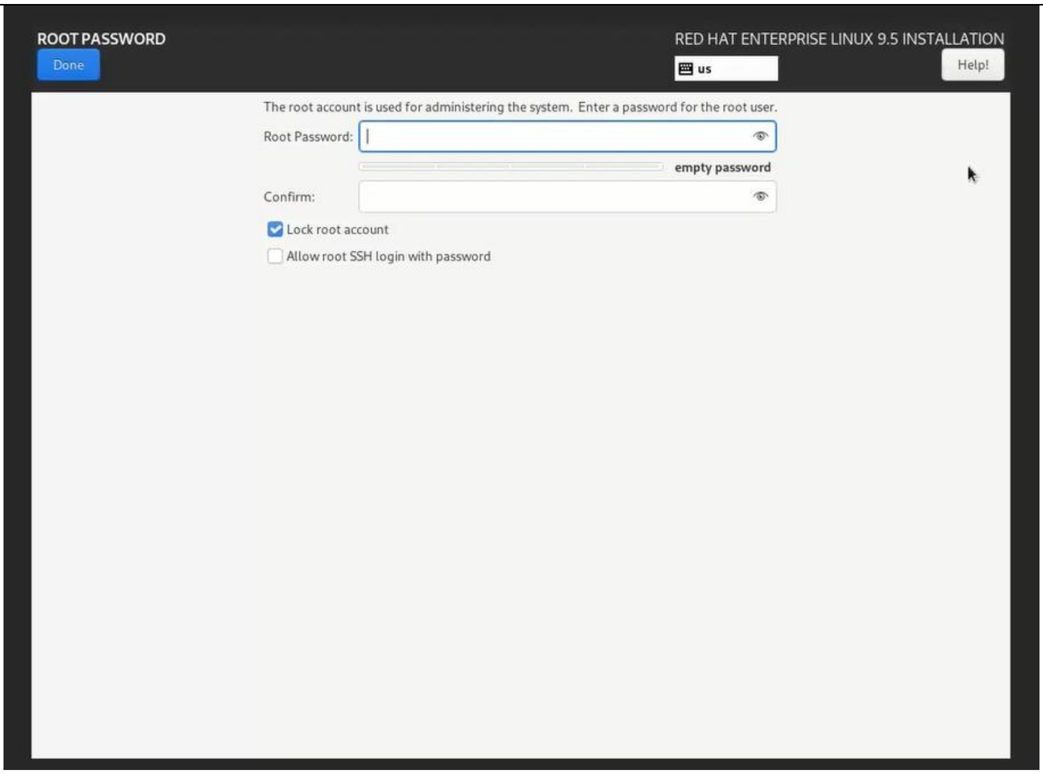
- Installation Destination — *Automatic partitioning selected*
- KDUMP — *Kdump is enabled*
- Network & Host Name — *Connected: ens3*
- Security Profile — *No profile selected*

USER SETTINGS

- Root Password — *Root account is disabled*
- User Creation — *No user will be created*

We won't touch your disks until you click 'Begin Installation'.

⚠ Please complete items marked with this icon before continuing to the next step.



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

Root Password:

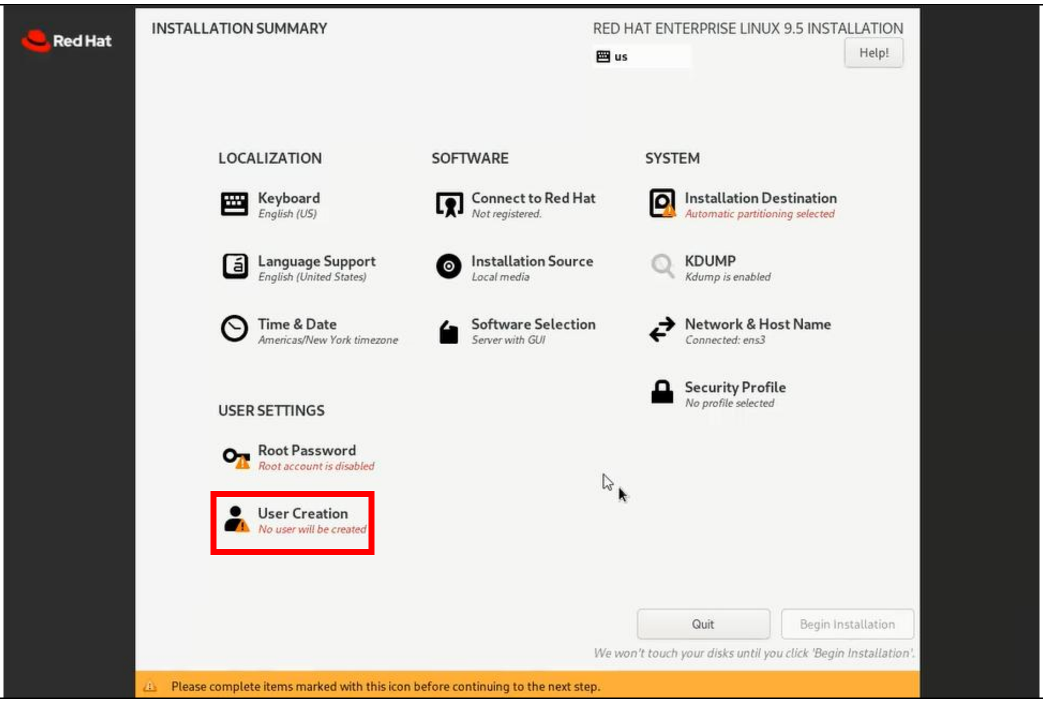
empty password

Confirm:

☑ Lock root account

☐ Allow root SSH login with password

Once your system is powered on and you land on this screen, you need to enable the root account by creating a password. Once you decide on a password and type it in, make sure you select "**lock root account**" and hit "**Done**."



LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Connect to Red Hat
Not registered.

Installation Source
Local media

Software Selection
Server with GUI

SYSTEM

Installation Destination
Automatic partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Connected: ens3

Security Profile
No profile selected

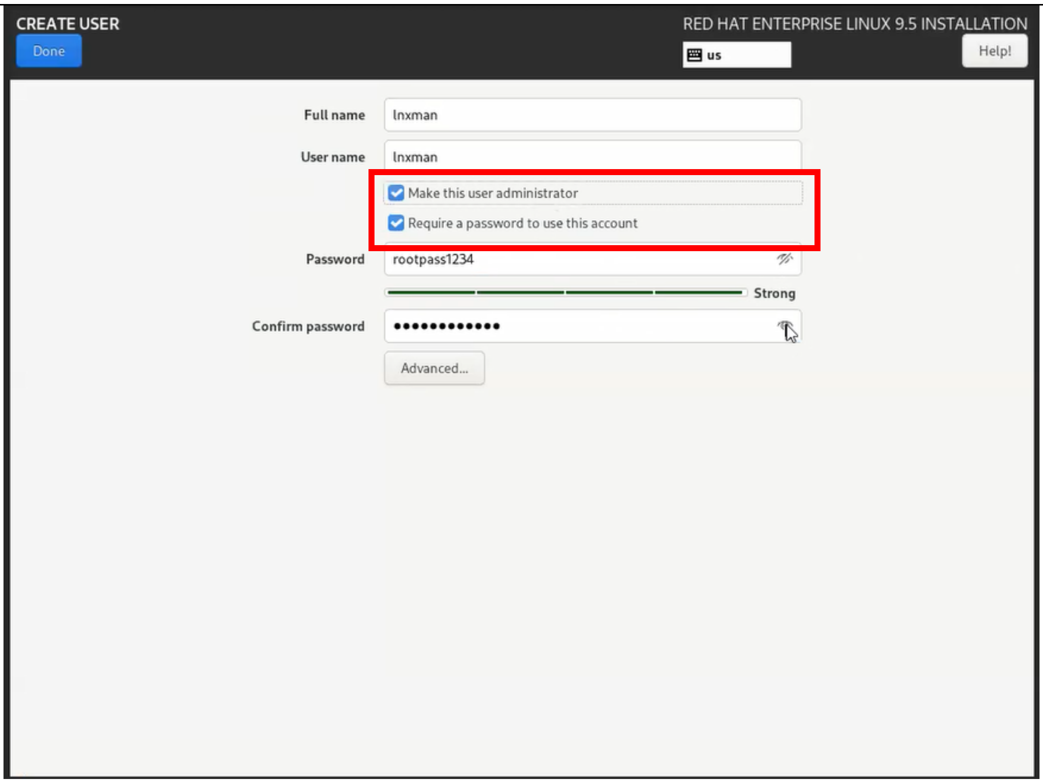
USER SETTINGS

Root Password
Root account is disabled

User Creation
No user will be created

We won't touch your disks until you click 'Begin Installation'.

⚠ Please complete items marked with this icon before continuing to the next step.



Full name: lnxman

User name: lnxman

☑ Make this user administrator

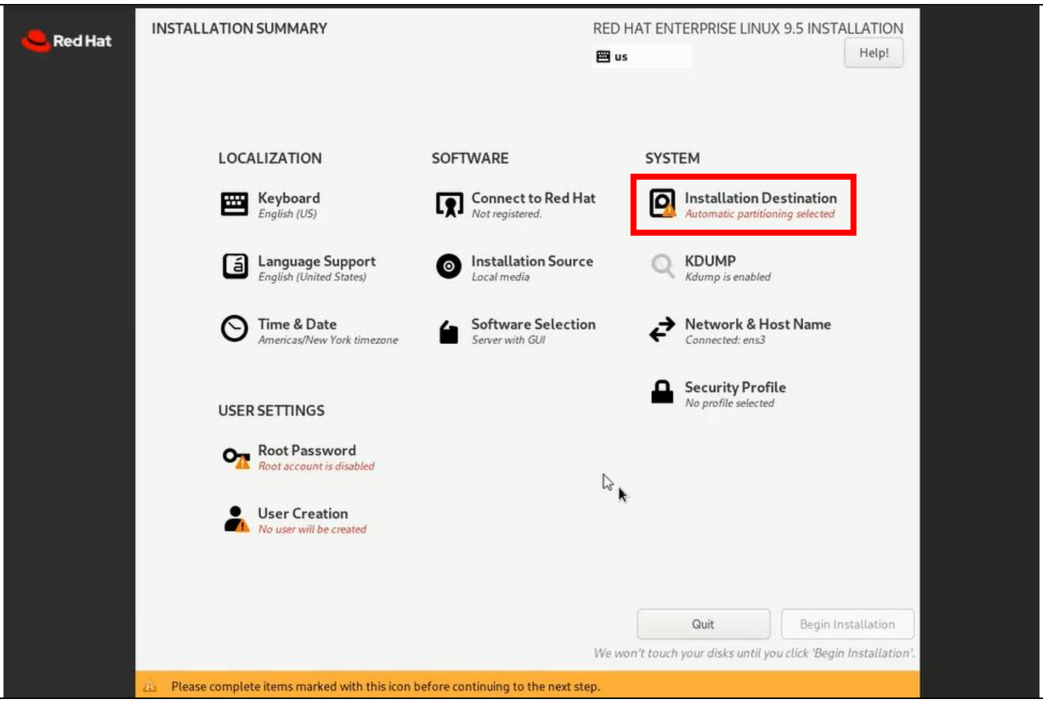
☑ Require a password to use this account

Password: rootpass1234

Strong

Confirm password: ••••••••••••

You'll get back to the installation screen and select User Creation. Here you will create a username and set a password for this account. Make sure the two boxes are checked and hit "**Done**."



LOCALIZATION

- Keyboard: English (US)
- Language Support: English (United States)
- Time & Date: Americas/New York timezone

SOFTWARE

- Connect to Red Hat: Not registered.
- Installation Source: Local media
- Software Selection: Server with GUI

SYSTEM

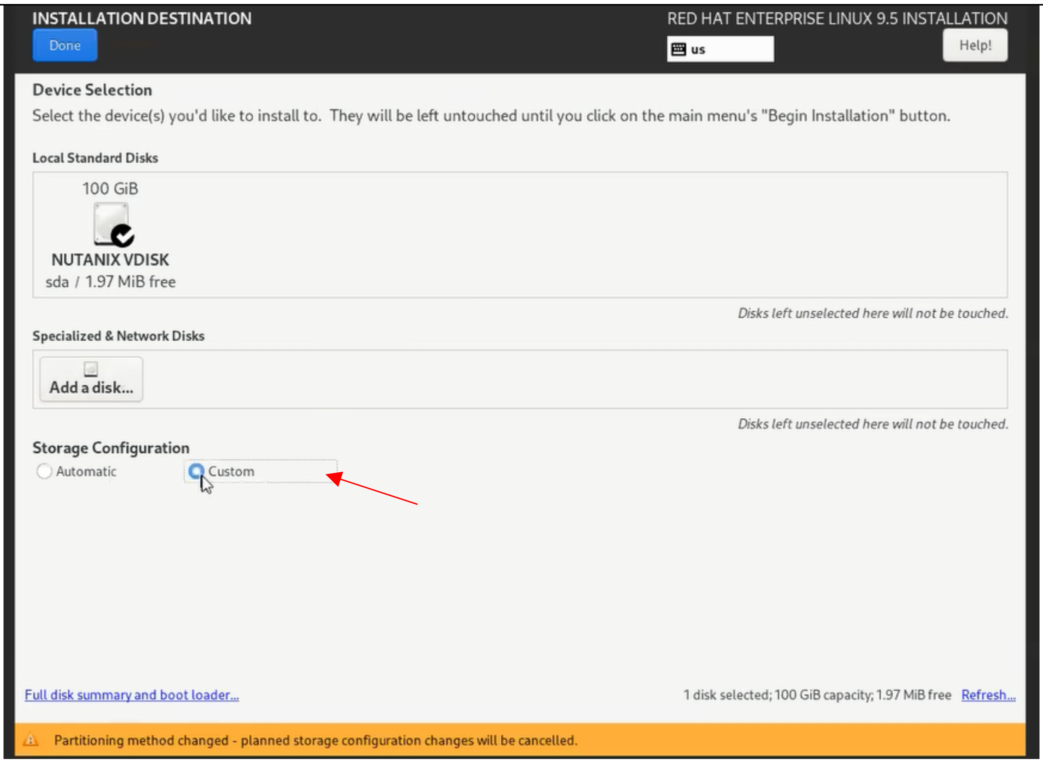
- Installation Destination: Automatic partitioning selected
- KDUMP: Kdump is enabled
- Network & Host Name: Connected: ens3
- Security Profile: No profile selected

USER SETTINGS

- Root Password: Root account is disabled
- User Creation: No user will be created

We won't touch your disks until you click 'Begin Installation'.

Please complete items marked with this icon before continuing to the next step.



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

sda / 1.97 MiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Disks left unselected here will not be touched.

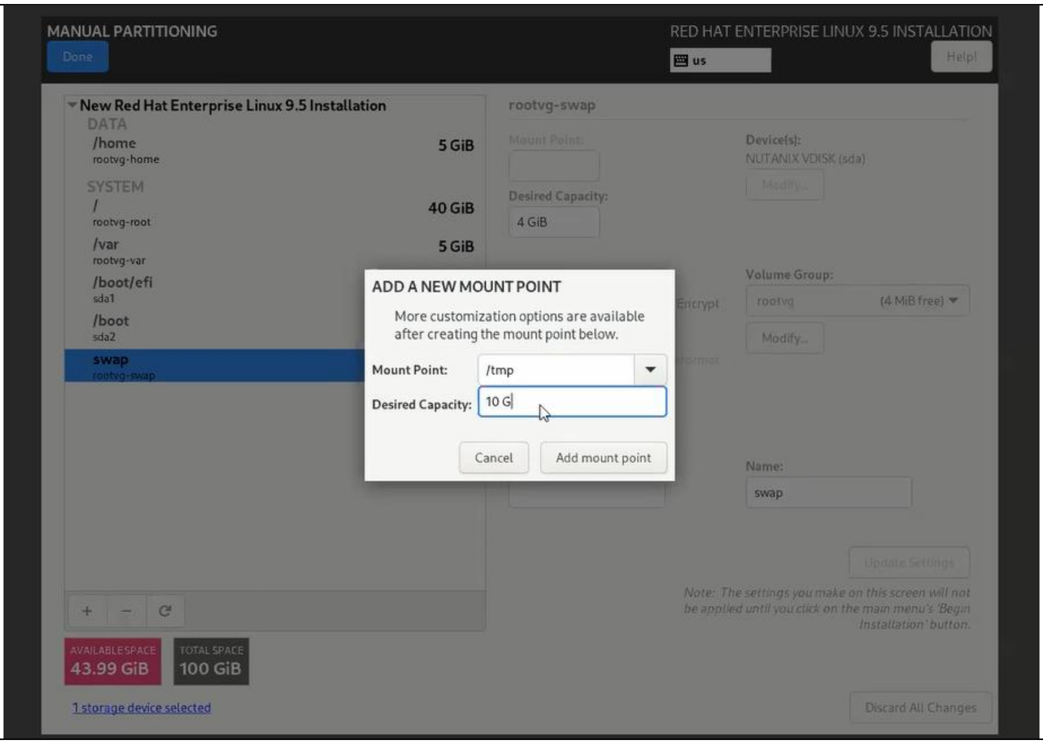
Storage Configuration

○ Automatic ● Custom

1 disk selected; 100 GiB capacity; 1.97 MiB free

Partitioning method changed - planned storage configuration changes will be cancelled.

Back on the installation screen, you will go to Installation Destination. On this screen, you will select “**Custom**” for the Storage Configuration which will bring you to the following step.



New Red Hat Enterprise Linux 9.5 Installation

DATA	
/home rootvg-home	5 GiB
SYSTEM	
/ rootvg-root	40 GiB
/var rootvg-var	5 GiB
/boot/efi sda1	
/boot sda2	
swap rootvg-swap	

rootvg-swap

Mount Point:

Desired Capacity: 4 GiB

Device(s): NUTANIX VDISK (sda)

Volume Group: rootvg (4 MiB free)

Name: swap

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

AVAILABLE SPACE 43.99 GiB

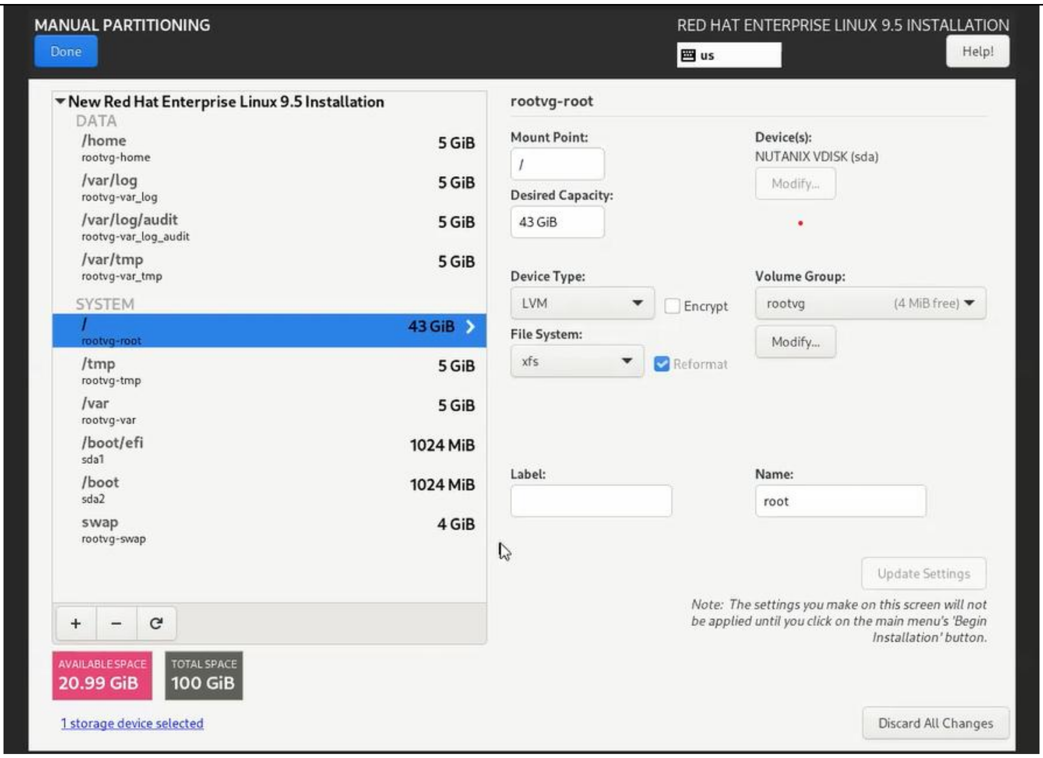
TOTAL SPACE 100 GiB

ADD A NEW MOUNT POINT

More customization options are available after creating the mount point below.

Mount Point: /tmp

Desired Capacity: 10 G



New Red Hat Enterprise Linux 9.5 Installation

DATA

/home rootvg-home	5 GiB
/var/log rootvg-var_log	5 GiB
/var/log/audit rootvg-var_log_audit	5 GiB
/var/tmp rootvg-var_tmp	5 GiB
SYSTEM	
/ rootvg-root	43 GiB
/tmp rootvg-tmp	5 GiB
/var rootvg-var	5 GiB
/boot/efi sda1	1024 MiB
/boot sda2	1024 MiB
swap rootvg-swap	4 GiB

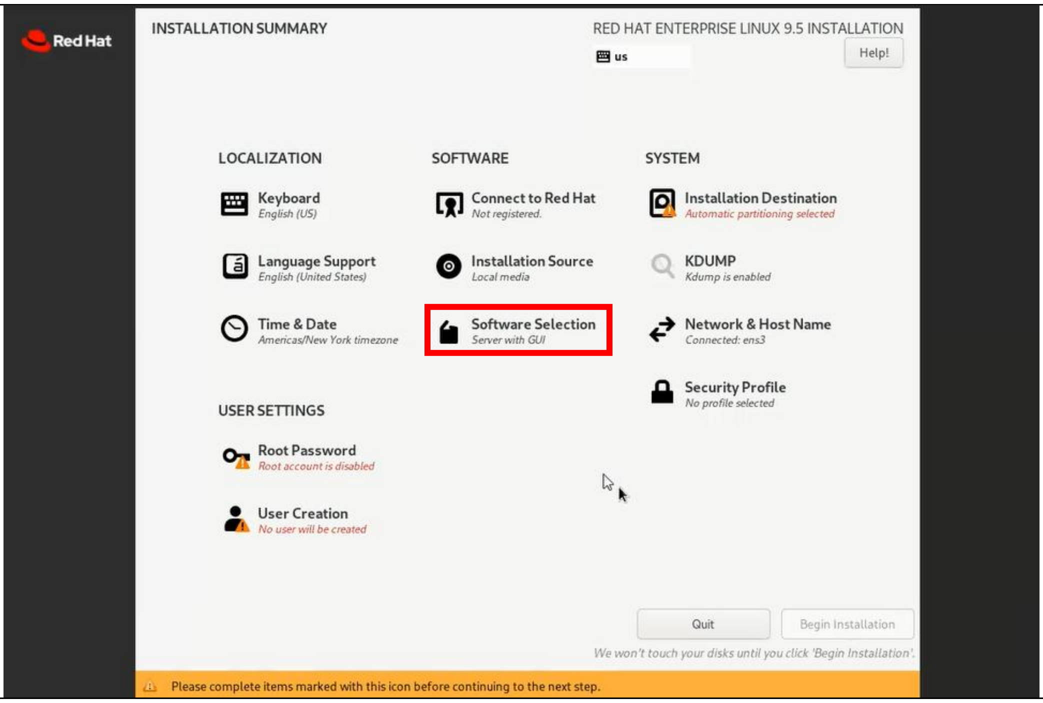
AVAILABLE SPACE 20.99 GiB
TOTAL SPACE 100 GiB

rootvg-root

Mount Point: /
Desired Capacity: 43 GiB
Device(s): NUTANIX VDISK (sda)
Device Type: LVM □ Encrypt
Volume Group: rootvg (4 MiB free)
File System: xfs ☑ Reformat
Label:
Name: root

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

To begin partitioning, select the **+** button. Next, select your mounting point and input your desired capacity. Based on 100 GB, the following allocation is recommended. Once you have finished mounting, select "**Done**."



LOCALIZATION
Keyboard — *English (US)*
Language Support — *English (United States)*
Time & Date — *Americas/New York timezone*

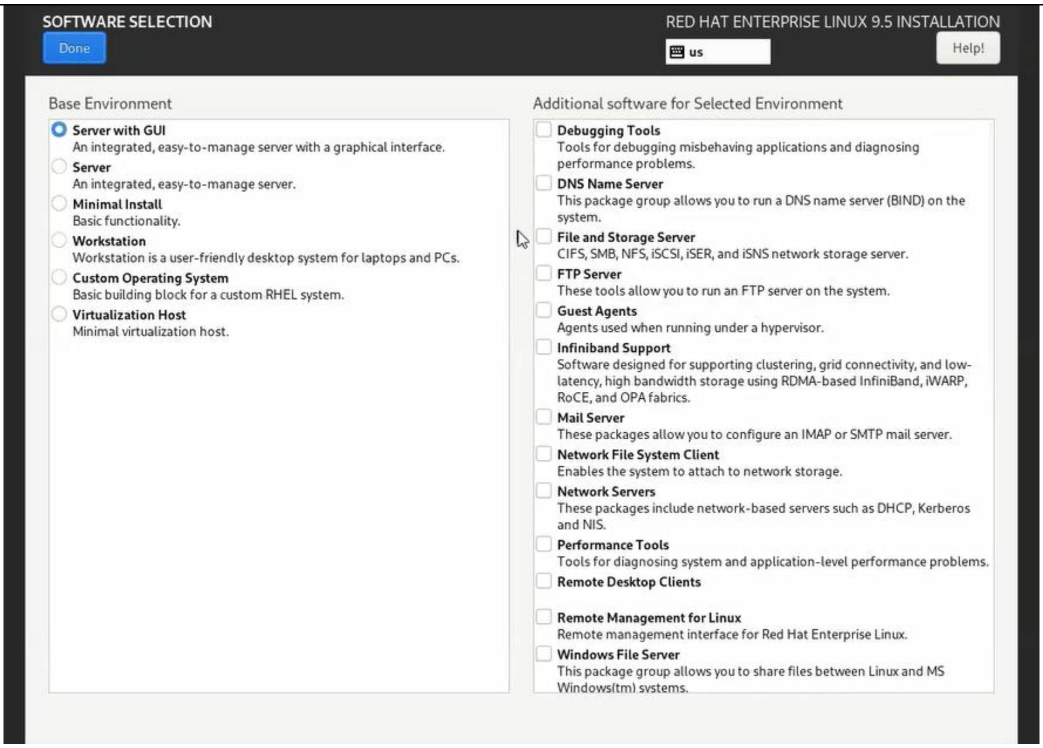
SOFTWARE
Connect to Red Hat — *Not registered.*
Installation Source — *Local media*
Software Selection — *Server with GUI*

SYSTEM
Installation Destination — *Automatic partitioning selected*
KDUMP — *Kdump is enabled*
Network & Host Name — *Connected: ens3*
Security Profile — *No profile selected*

USER SETTINGS
Root Password — *Root account is disabled*
User Creation — *No user will be created*

We won't touch your disks until you click 'Begin Installation'.

Please complete items marked with this icon before continuing to the next step.



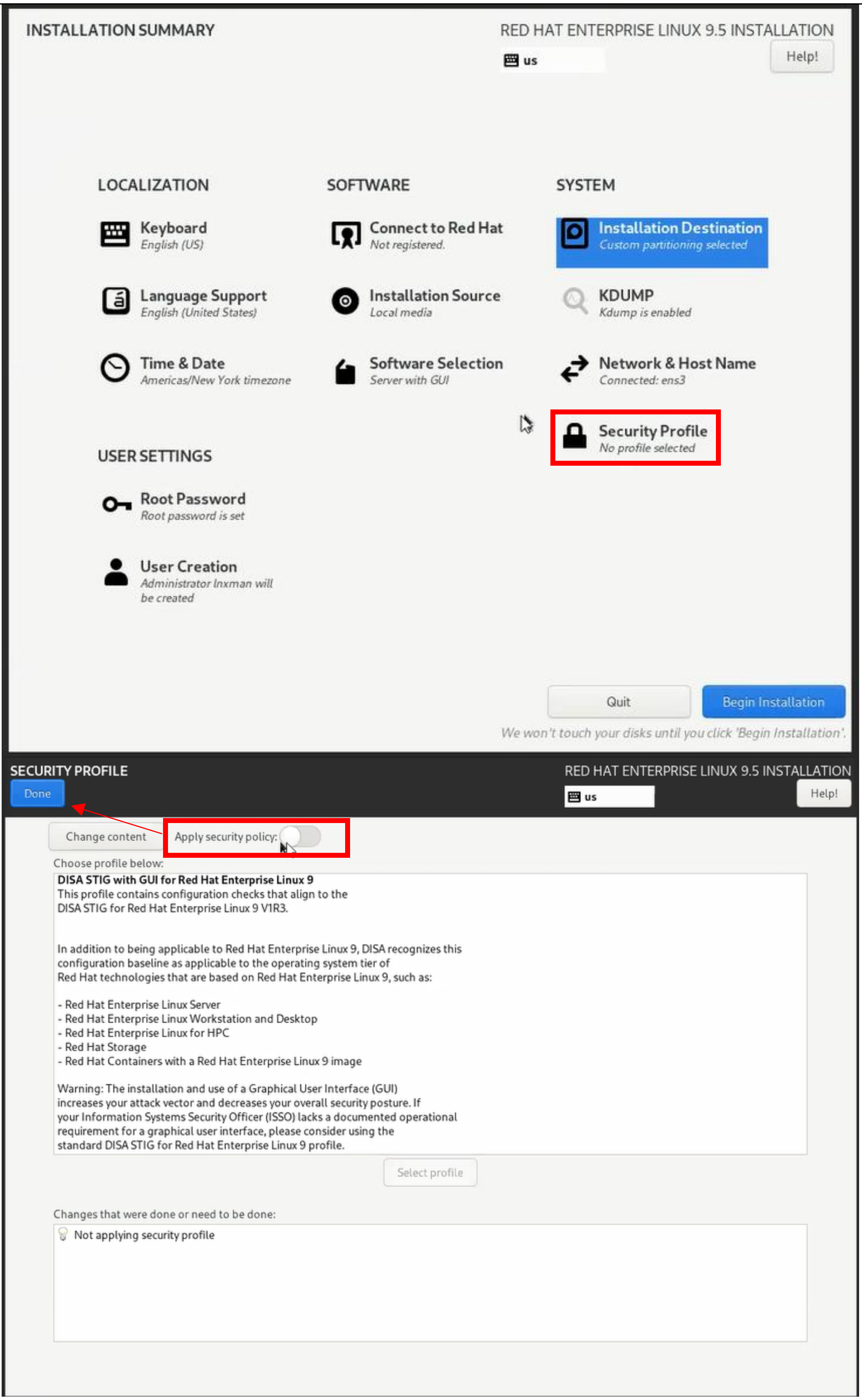
Base Environment

- ● **Server with GUI**
  An integrated, easy-to-manage server with a graphical interface.
- ○ **Server**
  An integrated, easy-to-manage server.
- ○ **Minimal Install**
  Basic functionality.
- ○ **Workstation**
  Workstation is a user-friendly desktop system for laptops and PCs.
- ○ **Custom Operating System**
  Basic building block for a custom RHEL system.
- ○ **Virtualization Host**
  Minimal virtualization host.

Additional software for Selected Environment

- □ **Debugging Tools**
  Tools for debugging misbehaving applications and diagnosing performance problems.
- □ **DNS Name Server**
  This package group allows you to run a DNS name server (BIND) on the system.
- □ **File and Storage Server**
  CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.
- □ **FTP Server**
  These tools allow you to run an FTP server on the system.
- □ **Guest Agents**
  Agents used when running under a hypervisor.
- □ **Infiniband Support**
  Software designed for supporting clustering, grid connectivity, and low-latency, high bandwidth storage using RDMA-based InfiniBand, iWARP, RoCE, and OPA fabrics.
- □ **Mail Server**
  These packages allow you to configure an IMAP or SMTP mail server.
- □ **Network File System Client**
  Enables the system to attach to network storage.
- □ **Network Servers**
  These packages include network-based servers such as DHCP, Kerberos and NIS.
- □ **Performance Tools**
  Tools for diagnosing system and application-level performance problems.
- □ **Remote Desktop Clients**
- □ **Remote Management for Linux**
  Remote management interface for Red Hat Enterprise Linux.
- □ **Windows File Server**
  This package group allows you to share files between Linux and MS Windows(tm) systems.

Next, select Software Selection and select "**Server with GUI"** for the base environment. For the additional software, select software you will need for the use of the server. Ex. Debugging Tools, File and Storage Server, Remote Management, etc. After you have selected your software, hit **"Done**."



INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 9.5 INSTALLATION

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Connect to Red Hat
Not registered.

Installation Source
Local media

Software Selection
Server with GUI

SYSTEM

Installation Destination
Custom partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Connected: ens3

Security Profile
No profile selected

USER SETTINGS

Root Password
Root password is set

User Creation
Administrator lnxman will be created

We won't touch your disks until you click 'Begin Installation'.

SECURITY PROFILE

RED HAT ENTERPRISE LINUX 9.5 INSTALLATION

Apply security policy: ○

Choose profile below:

DISA STIG with GUI for Red Hat Enterprise Linux 9
This profile contains configuration checks that align to the
DISA STIG for Red Hat Enterprise Linux 9 V1R3.

In addition to being applicable to Red Hat Enterprise Linux 9, DISA recognizes this
configuration baseline as applicable to the operating system tier of
Red Hat technologies that are based on Red Hat Enterprise Linux 9, such as:

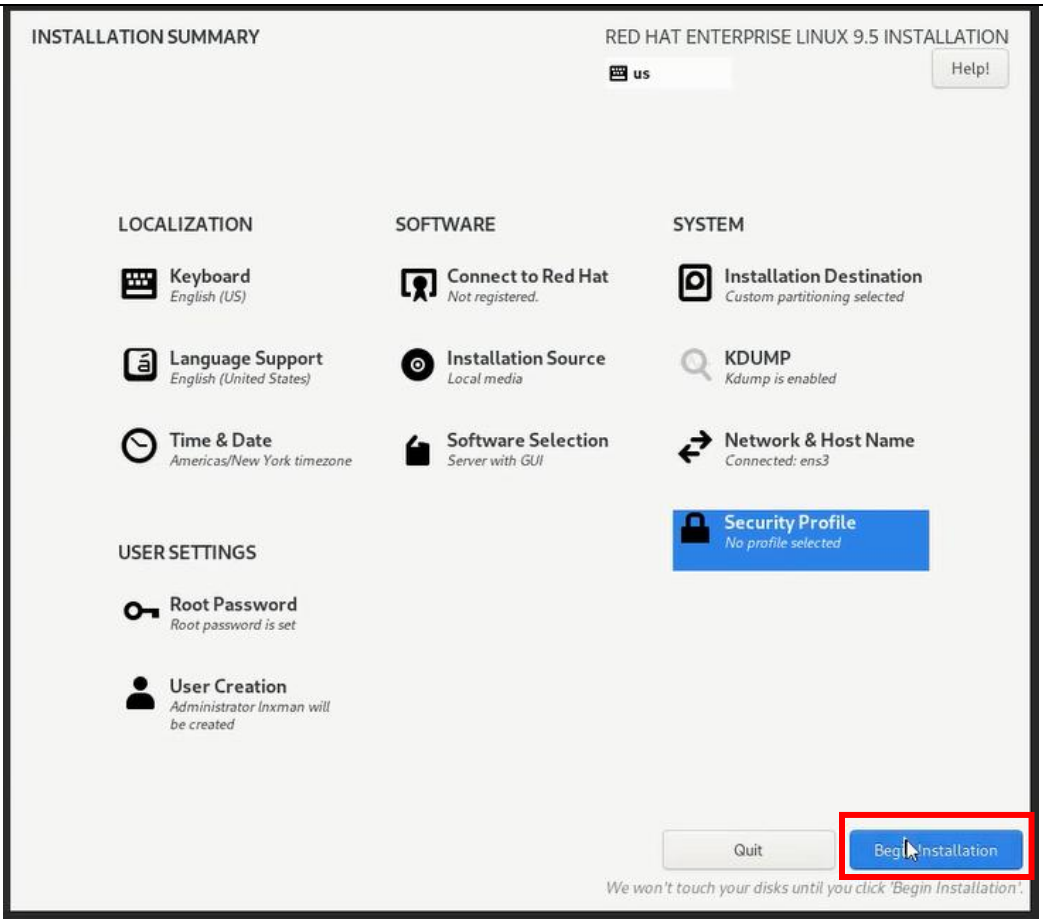
- Red Hat Enterprise Linux Server
- Red Hat Enterprise Linux Workstation and Desktop
- Red Hat Enterprise Linux for HPC
- Red Hat Storage
- Red Hat Containers with a Red Hat Enterprise Linux 9 image

Warning: The installation and use of a Graphical User Interface (GUI)
increases your attack vector and decreases your overall security posture. If
your Information Systems Security Officer (ISSO) lacks a documented operational
requirement for a graphical user interface, please consider using the
standard DISA STIG for Red Hat Enterprise Linux 9 profile.

Changes that were done or need to be done:

Not applying security profile

Finally, go to "**Security Profile**," turn off "**Apply security policy**," then select "**Done**."



INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 9.5 INSTALLATION

us

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Connect to Red Hat
Not registered.

Installation Source
Local media

Software Selection
Server with GUI

SYSTEM

Installation Destination
Custom partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Connected: ens3

Security Profile
No profile selected

USER SETTINGS

Root Password
Root password is set

User Creation
Administrator lnxman will be created

We won't touch your disks until you click 'Begin Installation'.

Once you have done every step, select "**Begin Installation**," and wait for it to finish. After it is done, installation is complete.

Overcoming Challenges

As we developed the automated vulnerability notification system, our team faced several technical and strategic challenges that required careful problem-solving. One major hurdle was setting up and securing our RHEL server from scratch. While we successfully built and hardened the server using STIG principles, the process demanded extensive troubleshooting, especially when aligning security benchmarks with system functionality.

Another challenge was integrating multiple tools – Podman, n8n, PostgreSQL, and Ollama – into a cohesive workflow. Each tool introduced its own complexities, from container management to database structuring to natural language generation for remediation tips. Ensuring compatibility and scalability required ongoing testing, adjustments, and redesign of certain steps.

Results & The Positive Impact

Our team has achieved several important milestones that demonstrate tangible results and long-term value. We successfully built and hardened a RHEL server rom scratch, providing a secure foundation for our automation environment. We also established the core workflow for the notification system, integrating Podman containers, n8n workflows, and PostgreSQL to enable data processing, storage, and automated email generation. Our experimentation with Ollama for AI-assisted email drafting has shown promising potential for creating clear and tailored remediation guidance, reducing the burden on security analysts.

Conclusion

Beyond technical progress, our project has had a positive impact on our professional growth. We deepened our knowledge of vulnerability management, server hardening, and automation tools, while also sharpening our problem-solving and collaboration skills. The work completed this summer has not only advanced the organizations ability to streamline vulnerability remediation but has also prepared us to transition this pilot into a more robust and deployable solution in the future.

PREP Student Reflection

Salome – I enjoyed working hands-on with tools like Tenable, n8n, Nutanix, and more. Our goal this second time around was to create a vulnerability notification system. We were able to incorporate different technologies to create this system. I learned a lot from watching YouTube videos, reading documentation, and using AI. This exposed me to new technologies and taught me how to make a decision on what tools are needed based on requirements. Through this experience, I gained a stronger understanding of real-world cybersecurity operations and now feel more confident in my ability to contribute effectively to a professional team.

Navjot -- This PREP project was an invaluable opportunity to bridge my academic studies with real-world cybersecurity challenges. A major focus was the development of a workflow automation system using n8n to streamline the vulnerability management process. I played a key role in building an automated pipeline that not only pulled vulnerability data but also integrated AI-assisted email generation via Ollama to provide personalized remediation steps to end users. This integration of AI into the workflow enabled us to tailor messages to specific vulnerabilities, reducing manual work and improving communication efficiency. Additionally, automating tasks like retrieving data from Active Directory and managing SUM groups using PowerShell highlighted how automation can significantly optimize security operations. This experience deepened my technical skills in automation, AI, and vulnerability remediation, while reinforcing the importance of proactive cybersecurity measures in preventing incidents from escalating into situations that would require digital forensics.