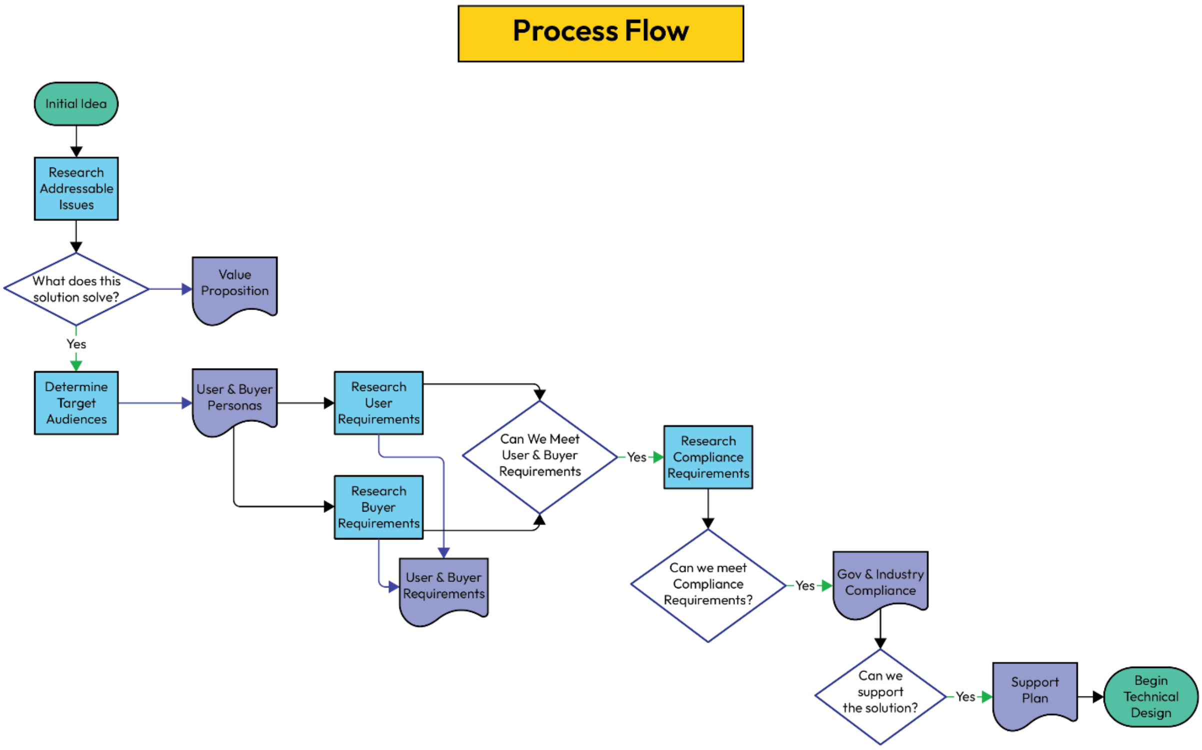
Chapter 1: Welcome to the Cyber Security Landscape

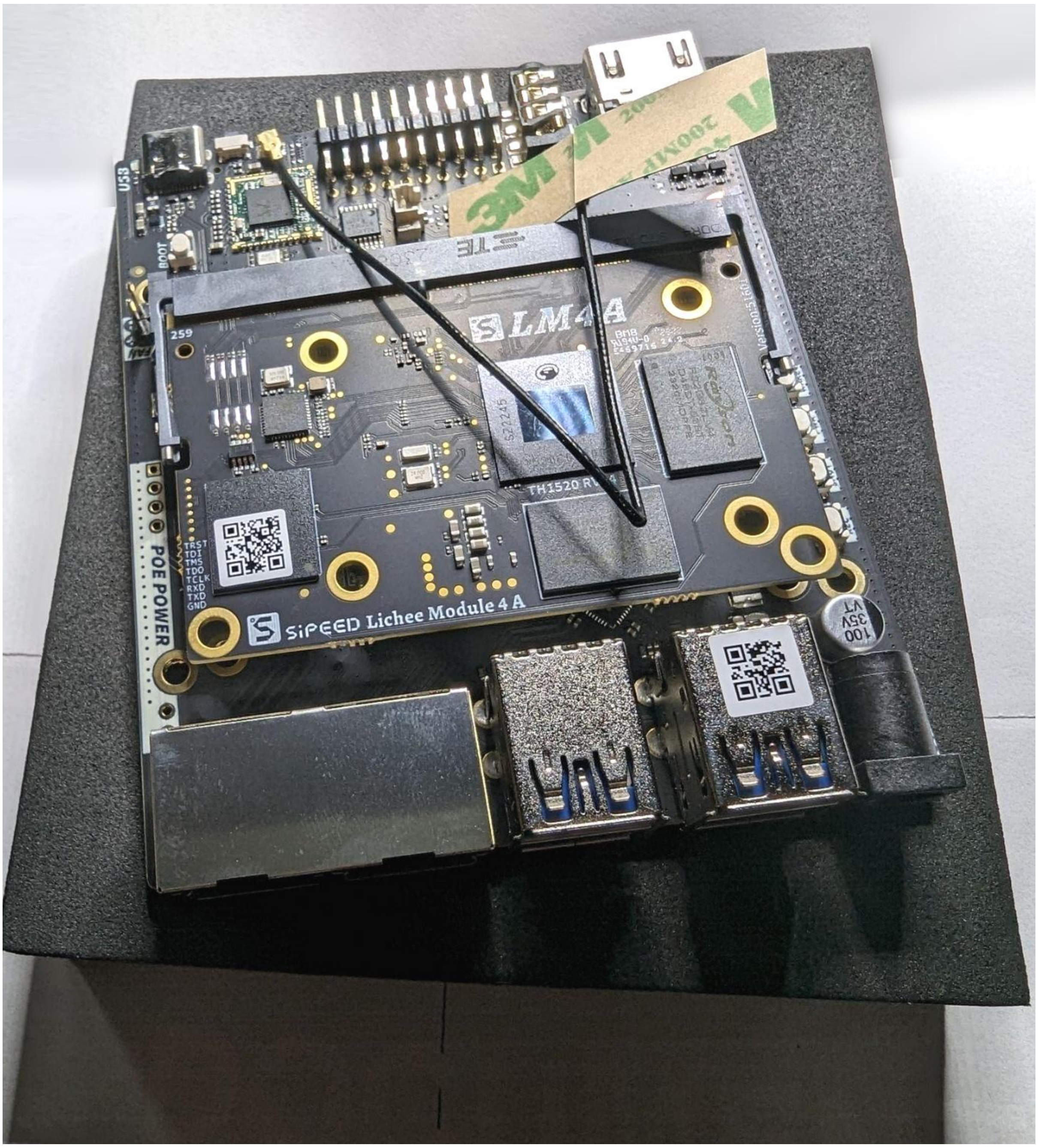
No Images

Chapter 2: Security Starts at the Design Table

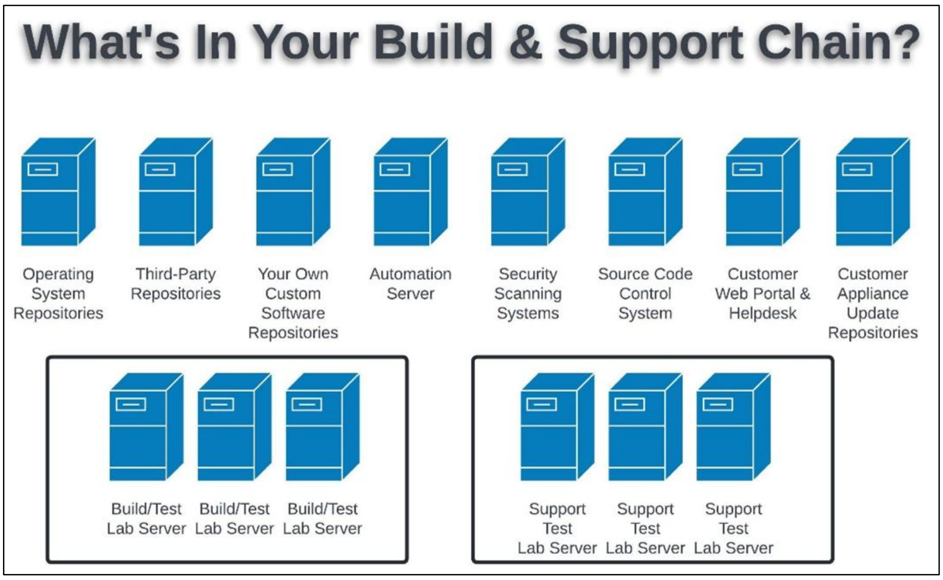

Process Flow
Initial Idea
Research Addressable Issues
What does this solution solve?
Value Proposition
Yes
Determine Target Audiences
User & Buyer Personas
Research User Requirements
Research Buyer Requirements
User & Buyer Requirements
Can We Meet User & Buyer Requirements
Yes
Research Compliance Requirements
Can we meet Compliance Requirements?
Yes
Gov & Industry Compliance
Can we support the solution?
Yes
Support Plan
Begin Technical Design

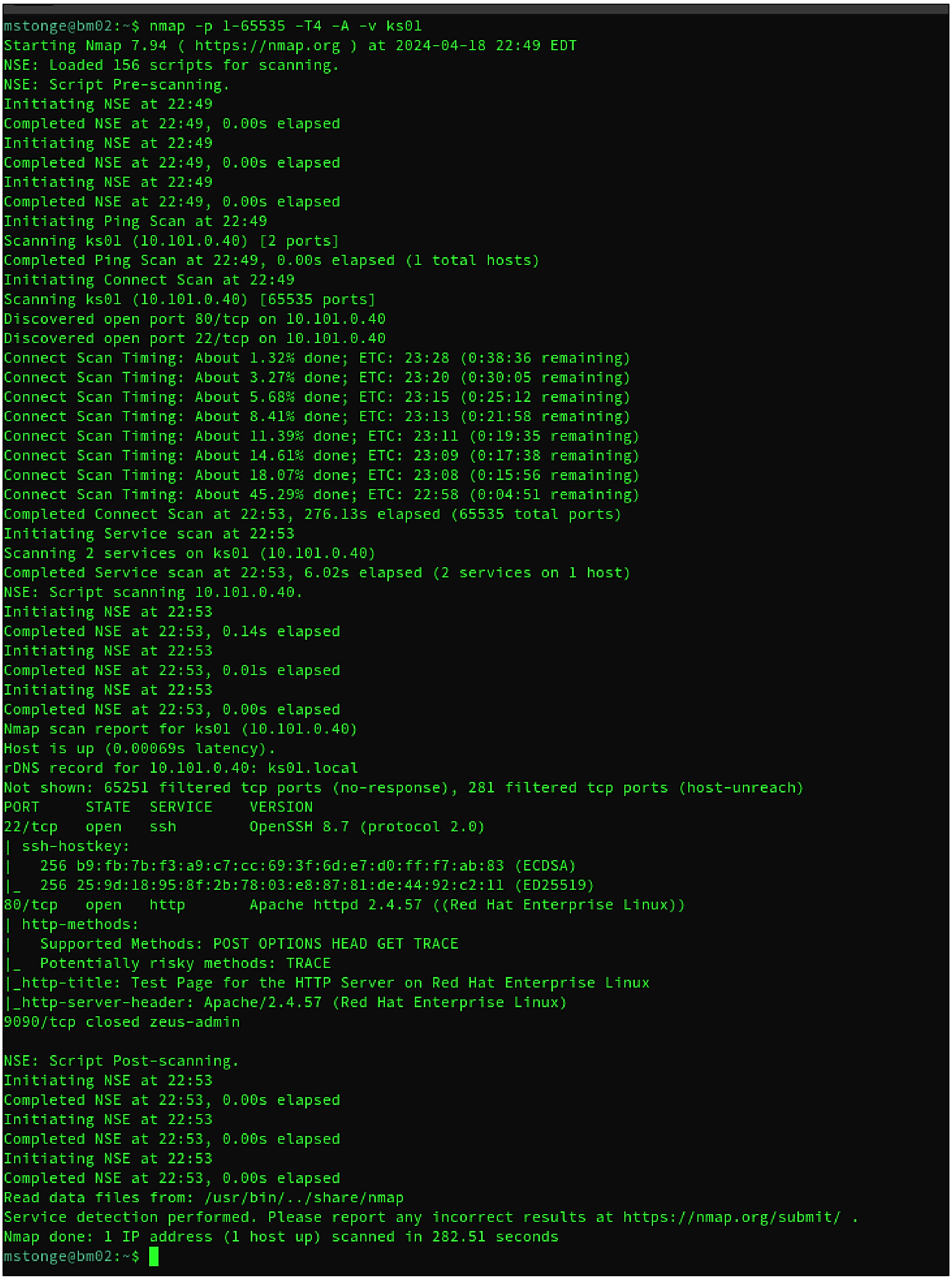
Chapter 3: Applying Design Requirements Criteria – Hardware Selection

Chapter 4: Applying Design Requirements Criteria – the Operating System

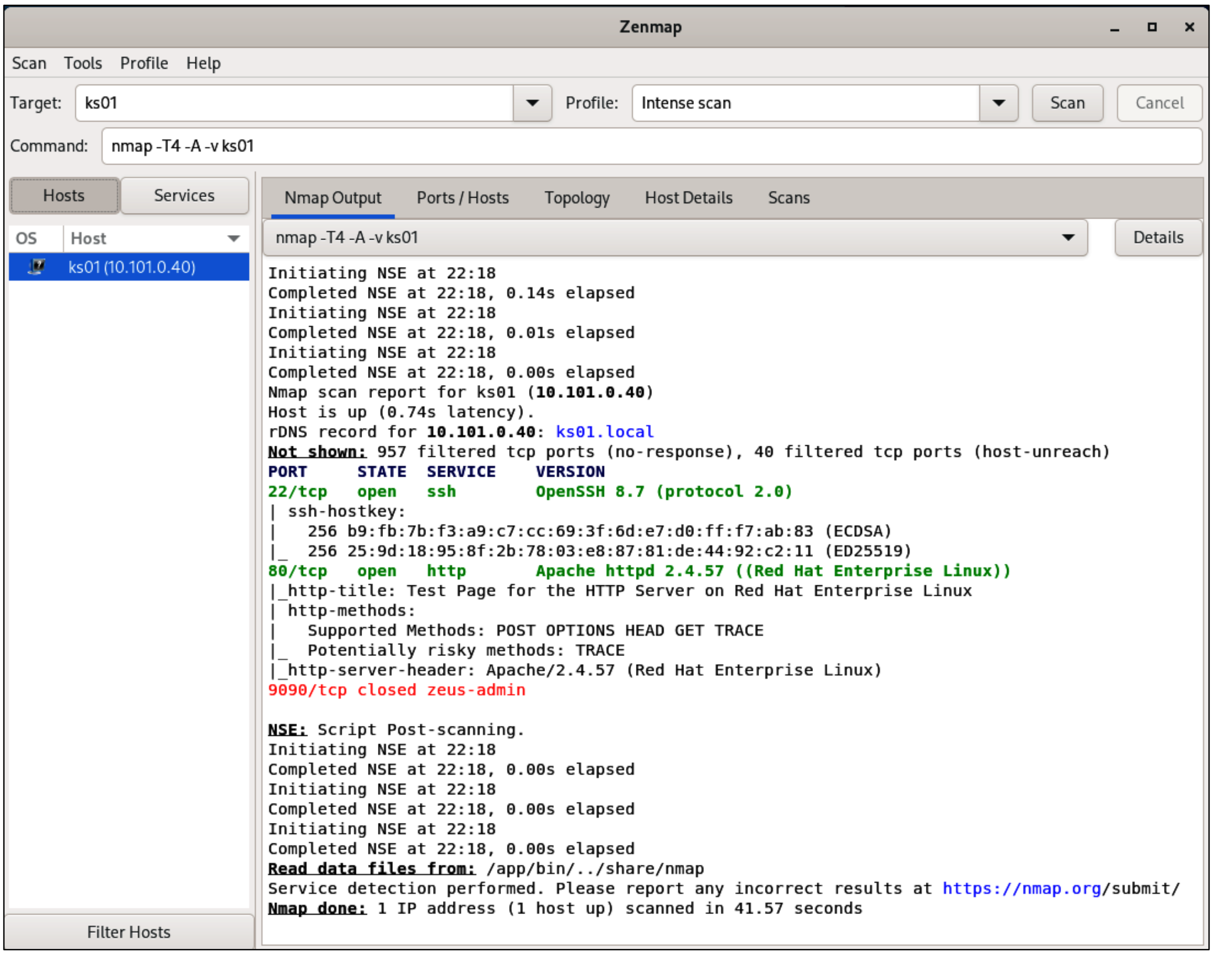


Chapter 5: Basic Needs in My Build Chain


What's In Your Build & Support Chain?
Operating System Repositories
Third-Party Repositories
Your Own Custom Software Repositories
Automation Server
Security Scanning Systems
Source Code Control System
Customer Web Portal & Helpdesk
Customer Appliance Update Repositories
Build/Test Lab Server
Build/Test Lab Server
Build/Test Lab Server
Support Test Lab Server
Support Test Lab Server
Support Test Lab Server



```
mstonge@bm02:~$ nmap -p 1-65535 -T4 -A -v ks01
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-18 22:49 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:49
Completed NSE at 22:49, 0.00s elapsed
Initiating NSE at 22:49
Completed NSE at 22:49, 0.00s elapsed
Initiating NSE at 22:49
Completed NSE at 22:49, 0.00s elapsed
Initiating Ping Scan at 22:49
Scanning ks01 (10.101.0.40) [2 ports]
Completed Ping Scan at 22:49, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 22:49
Scanning ks01 (10.101.0.40) [65535 ports]
Discovered open port 80/tcp on 10.101.0.40
Discovered open port 22/tcp on 10.101.0.40
Connect Scan Timing: About 1.32% done; ETC: 23:28 (0:38:36 remaining)
Connect Scan Timing: About 3.27% done; ETC: 23:20 (0:30:05 remaining)
Connect Scan Timing: About 5.68% done; ETC: 23:15 (0:25:12 remaining)
Connect Scan Timing: About 8.41% done; ETC: 23:13 (0:21:58 remaining)
Connect Scan Timing: About 11.39% done; ETC: 23:11 (0:19:35 remaining)
Connect Scan Timing: About 14.61% done; ETC: 23:09 (0:17:38 remaining)
Connect Scan Timing: About 18.07% done; ETC: 23:08 (0:15:56 remaining)
Connect Scan Timing: About 45.29% done; ETC: 22:58 (0:04:51 remaining)
Completed Connect Scan at 22:53, 276.13s elapsed (65535 total ports)
Initiating Service scan at 22:53
Scanning 2 services on ks01 (10.101.0.40)
Completed Service scan at 22:53, 6.02s elapsed (2 services on 1 host)
NSE: Script scanning 10.101.0.40.
Initiating NSE at 22:53
Completed NSE at 22:53, 0.14s elapsed
Initiating NSE at 22:53
Completed NSE at 22:53, 0.01s elapsed
Initiating NSE at 22:53
Completed NSE at 22:53, 0.00s elapsed
Nmap scan report for ks01 (10.101.0.40)
Host is up (0.00069s latency).
rDNS record for 10.101.0.40: ks01.local
Not shown: 65251 filtered tcp ports (no-response), 281 filtered tcp ports (host-unreach)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 8.7 (protocol 2.0)
| ssh-hostkey:
|   256 b9:fb:7b:f3:a9:c7:cc:69:3f:6d:e7:d0:ff:f7:ab:83 (ECDSA)
|_  256 25:9d:18:95:8f:2b:78:03:e8:87:81:de:44:92:c2:11 (ED25519)
80/tcp   open   http       Apache httpd 2.4.57 ((Red Hat Enterprise Linux))
| http-methods:
|   Supported Methods: POST OPTIONS HEAD GET TRACE
|_  Potentially risky methods: TRACE
|_http-title: Test Page for the HTTP Server on Red Hat Enterprise Linux
|_http-server-header: Apache/2.4.57 (Red Hat Enterprise Linux)
9090/tcp closed zeus-admin

NSE: Script Post-scanning.
Initiating NSE at 22:53
Completed NSE at 22:53, 0.00s elapsed
Initiating NSE at 22:53
Completed NSE at 22:53, 0.00s elapsed
Initiating NSE at 22:53
Completed NSE at 22:53, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 282.51 seconds
mstonge@bm02:~$
```



Target: ks01

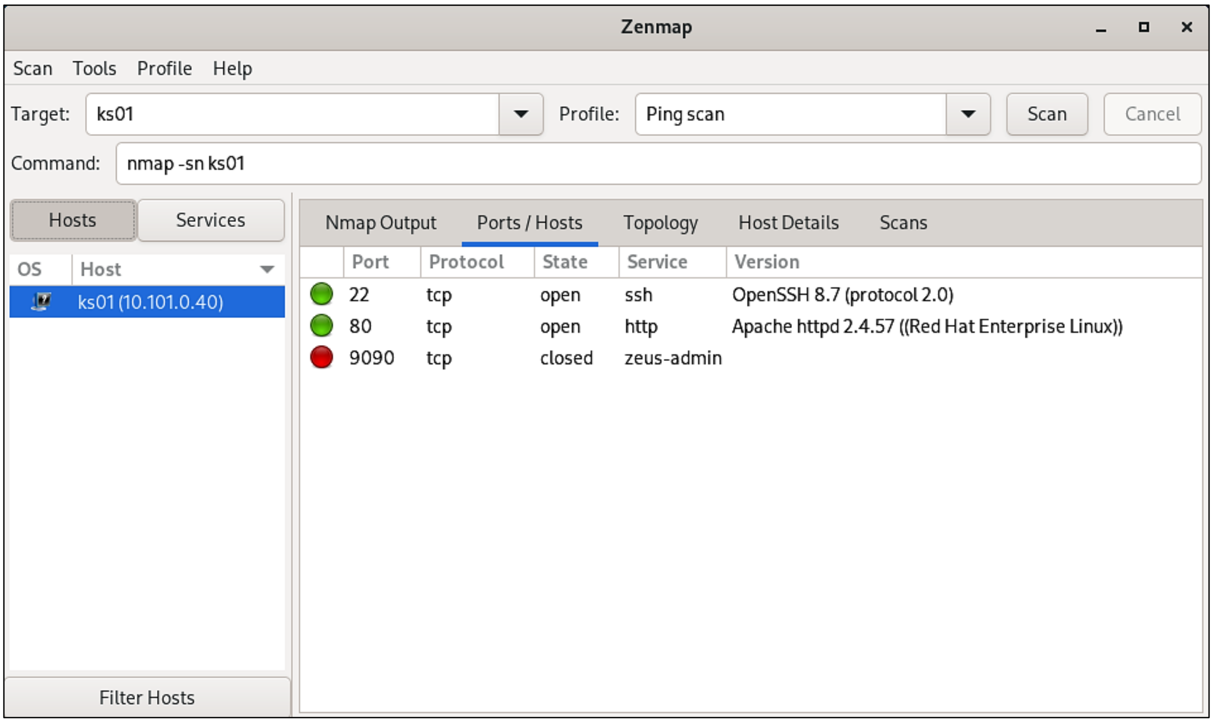
Profile: Intense scan

Command: nmap -T4 -A -v ks01

ks01 (10.101.0.40)

nmap -T4 -A -v ks01

```
Initiating NSE at 22:18
Completed NSE at 22:18, 0.14s elapsed
Initiating NSE at 22:18
Completed NSE at 22:18, 0.01s elapsed
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Nmap scan report for ks01 (10.101.0.40)
Host is up (0.74s latency).
rDNS record for 10.101.0.40: ks01.local
Not shown: 957 filtered tcp ports (no-response), 40 filtered tcp ports (host-unreach)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 8.7 (protocol 2.0)
| ssh-hostkey:
|   256 b9:fb:7b:f3:a9:c7:cc:69:3f:6d:e7:d0:ff:f7:ab:83 (ECDSA)
|_  256 25:9d:18:95:8f:2b:78:03:e8:87:81:de:44:92:c2:11 (ED25519)
80/tcp   open   http       Apache httpd 2.4.57 ((Red Hat Enterprise Linux))
|_http-title: Test Page for the HTTP Server on Red Hat Enterprise Linux
| http-methods:
|   Supported Methods: POST OPTIONS HEAD GET TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.57 (Red Hat Enterprise Linux)
9090/tcp closed zeus-admin

NSE: Script Post-scanning.
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Read data files from: /app/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 41.57 seconds
```



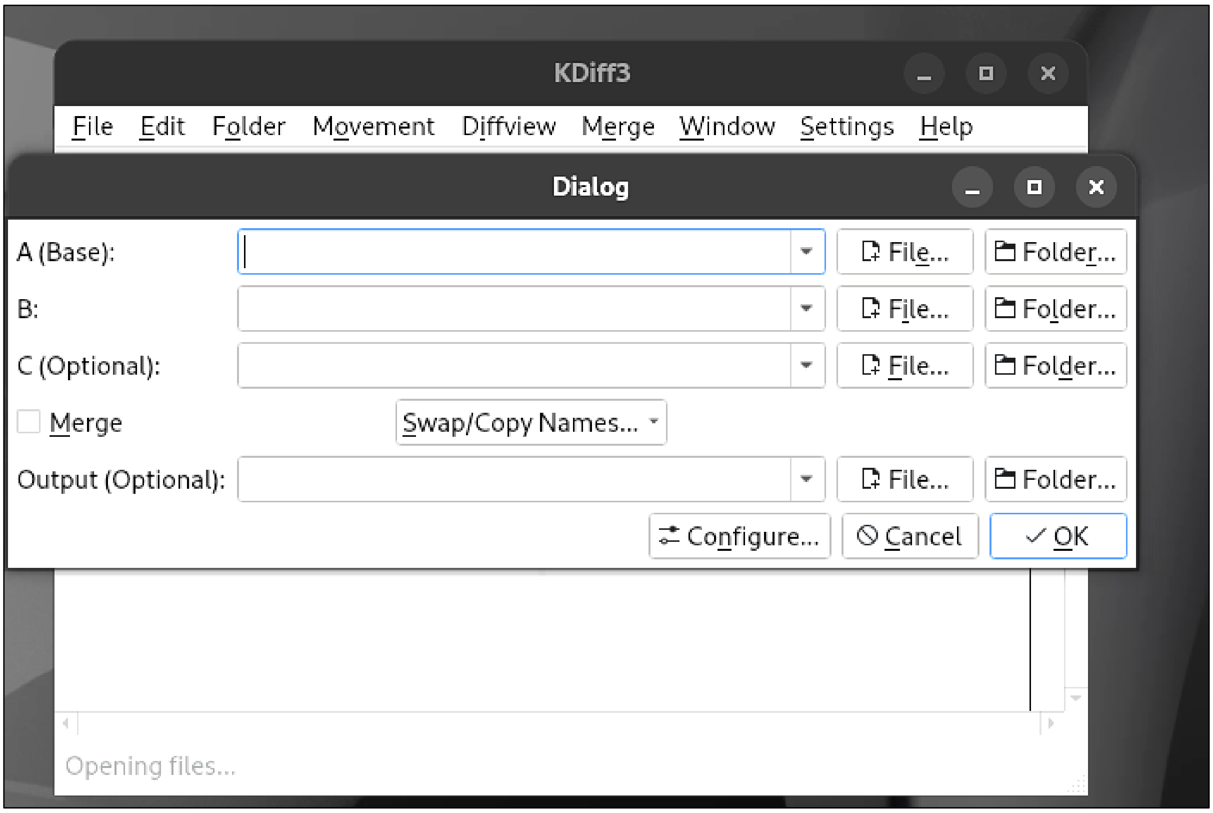
Target: ks01

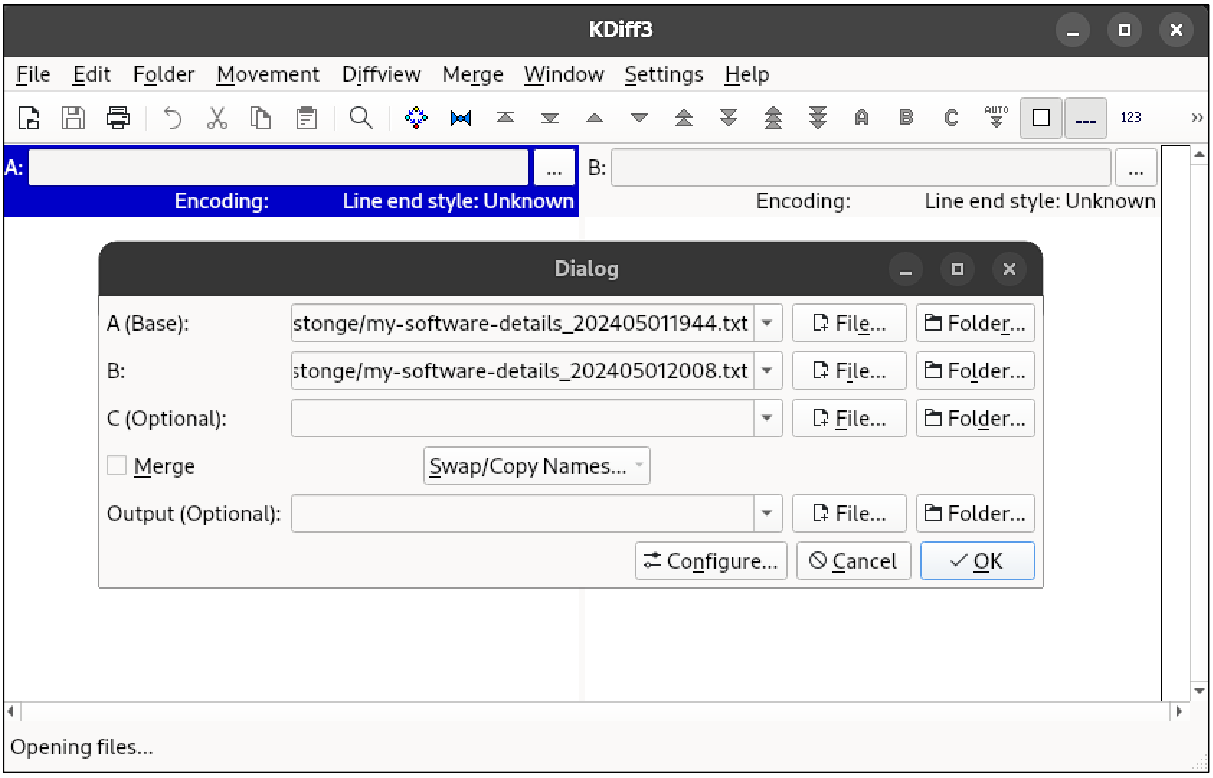
Profile: Ping scan

Command: nmap -sn ks01

ks01 (10.101.0.40)

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 8.7 (protocol 2.0)
●	80	tcp	open	http	Apache httpd 2.4.57 ((Red Hat Enterprise Linux))
●	9090	tcp	closed	zeus-admin	





A: Encoding: Line end style: Unknown

B: Encoding: Line end style: Unknown

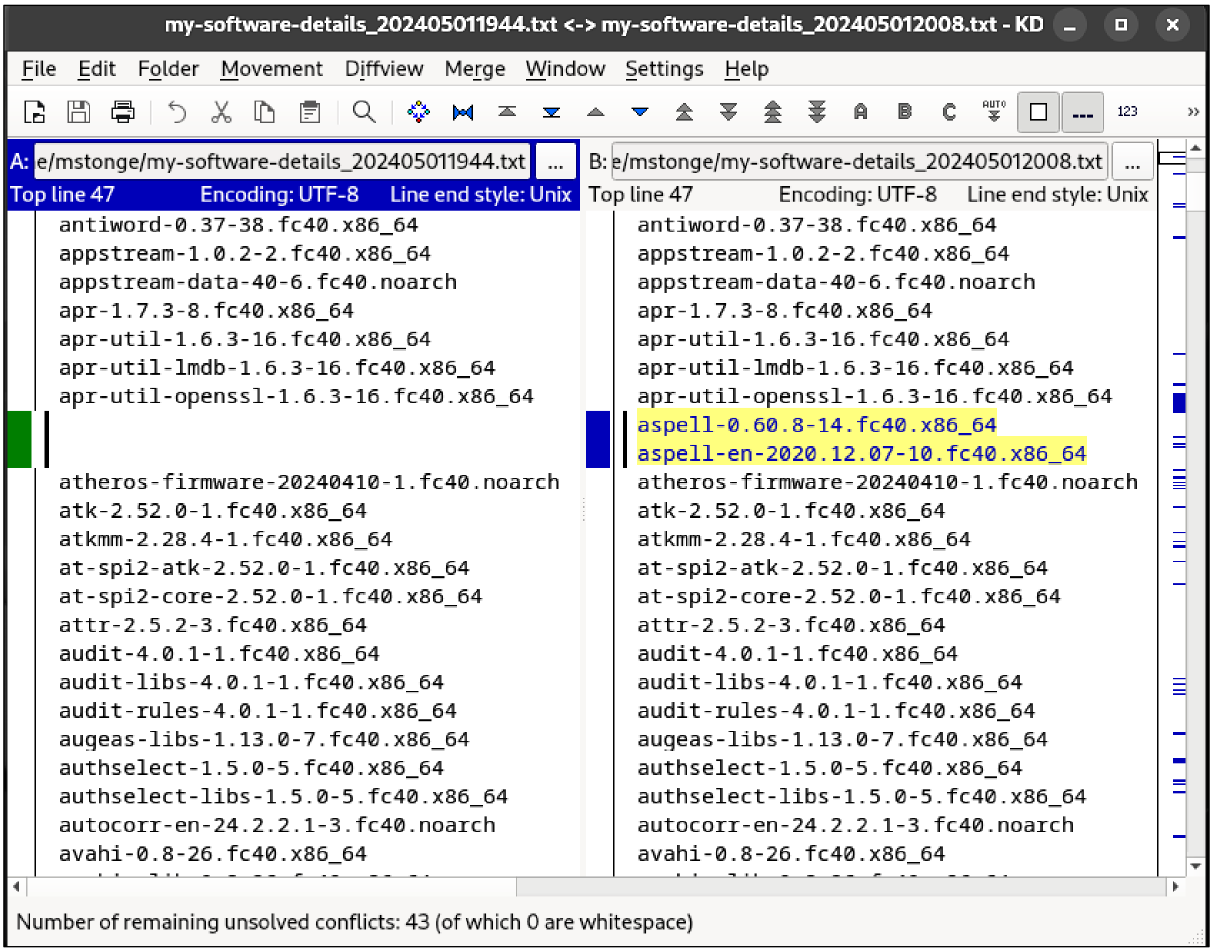
A (Base): stonge/my-software-details_202405011944.txt

B: stonge/my-software-details_202405012008.txt

C (Optional):

Output (Optional):

Opening files...

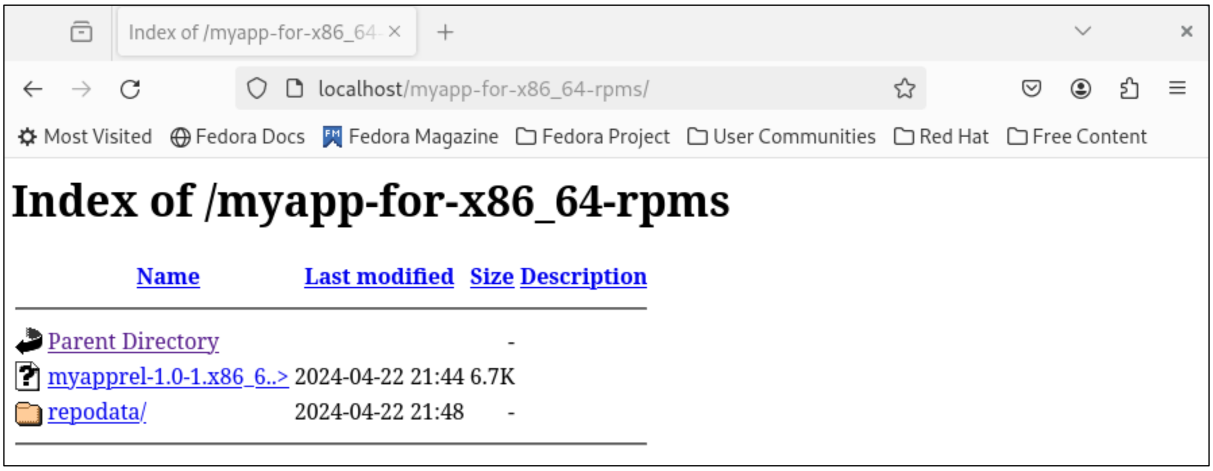

my-software-details_202405011944.txt <-> my-software-details_202405012008.txt - KD
File Edit Folder Movement Diffview Merge Window Settings Help
123

A: e/mstonge/my-software-details_202405011944.txt
Top line 47 Encoding: UTF-8 Line end style: Unix

B: e/mstonge/my-software-details_202405012008.txt
Top line 47 Encoding: UTF-8 Line end style: Unix

```
A:                                          B:
antiword-0.37-38.fc40.x86_64                antiword-0.37-38.fc40.x86_64
appstream-1.0.2-2.fc40.x86_64               appstream-1.0.2-2.fc40.x86_64
appstream-data-40-6.fc40.noarch             appstream-data-40-6.fc40.noarch
apr-1.7.3-8.fc40.x86_64                     apr-1.7.3-8.fc40.x86_64
apr-util-1.6.3-16.fc40.x86_64               apr-util-1.6.3-16.fc40.x86_64
apr-util-lmdb-1.6.3-16.fc40.x86_64          apr-util-lmdb-1.6.3-16.fc40.x86_64
apr-util-openssl-1.6.3-16.fc40.x86_64       apr-util-openssl-1.6.3-16.fc40.x86_64
                                            aspell-0.60.8-14.fc40.x86_64
                                            aspell-en-2020.12.07-10.fc40.x86_64
atheros-firmware-20240410-1.fc40.noarch     atheros-firmware-20240410-1.fc40.noarch
atk-2.52.0-1.fc40.x86_64                    atk-2.52.0-1.fc40.x86_64
atkmm-2.28.4-1.fc40.x86_64                  atkmm-2.28.4-1.fc40.x86_64
at-spi2-atk-2.52.0-1.fc40.x86_64            at-spi2-atk-2.52.0-1.fc40.x86_64
at-spi2-core-2.52.0-1.fc40.x86_64           at-spi2-core-2.52.0-1.fc40.x86_64
attr-2.5.2-3.fc40.x86_64                    attr-2.5.2-3.fc40.x86_64
audit-4.0.1-1.fc40.x86_64                   audit-4.0.1-1.fc40.x86_64
audit-libs-4.0.1-1.fc40.x86_64              audit-libs-4.0.1-1.fc40.x86_64
audit-rules-4.0.1-1.fc40.x86_64             audit-rules-4.0.1-1.fc40.x86_64
augeas-libs-1.13.0-7.fc40.x86_64            augeas-libs-1.13.0-7.fc40.x86_64
authselect-1.5.0-5.fc40.x86_64              authselect-1.5.0-5.fc40.x86_64
authselect-libs-1.5.0-5.fc40.x86_64         authselect-libs-1.5.0-5.fc40.x86_64
autocorr-en-24.2.2.1-3.fc40.noarch          autocorr-en-24.2.2.1-3.fc40.noarch
avahi-0.8-26.fc40.x86_64                    avahi-0.8-26.fc40.x86_64
```

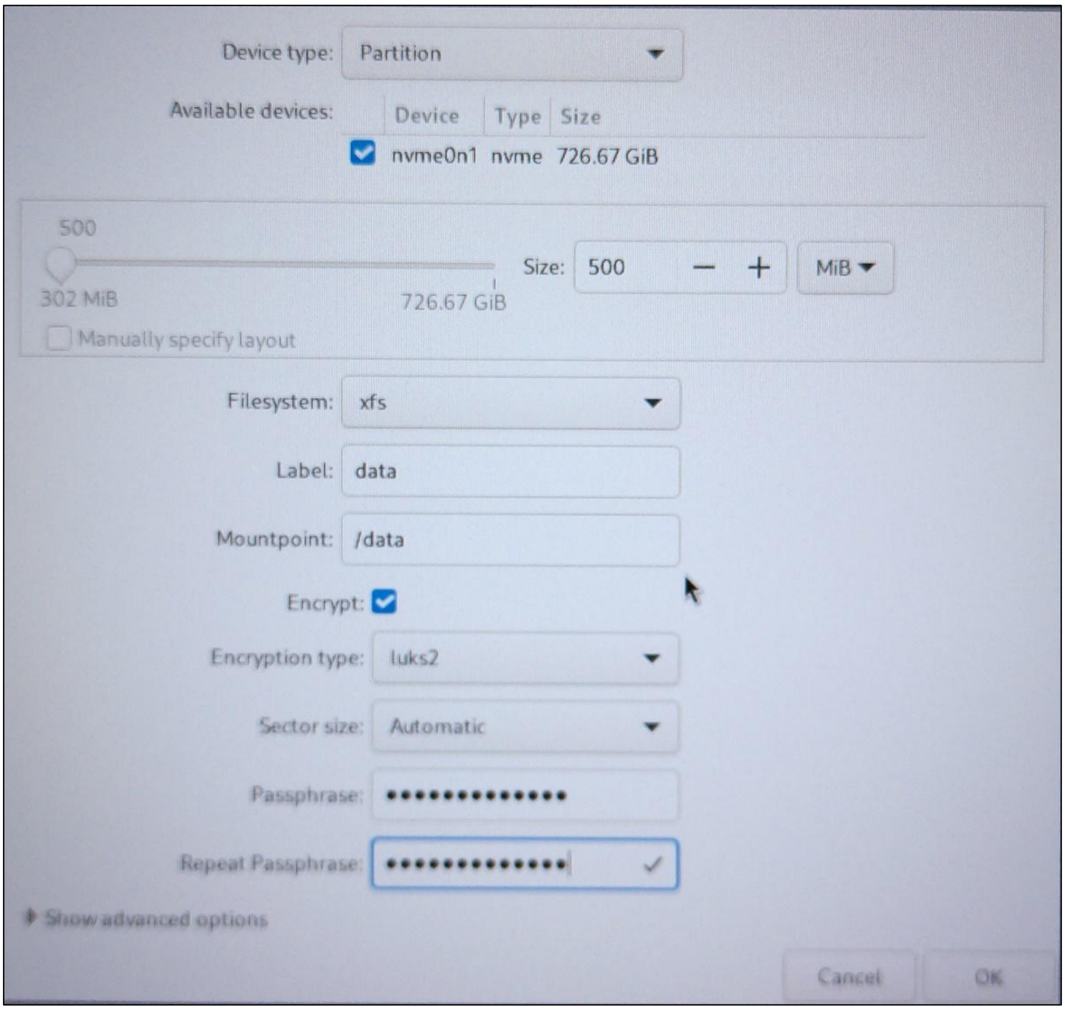
Number of remaining unsolved conflicts: 43 (of which 0 are whitespace)



Index of /myapp-for-x86_64-rpms

Name	Last modified	Size	Description
Parent Directory		-	
myapprel-1.0-1.x86_6..>	2024-04-22 21:44	6.7K	
repodata/	2024-04-22 21:48	-	

Chapter 6: Disk Encryption



Device type: Partition

Available devices:

	Device	Type	Size
☑	nvme0n1	nvme	726.67 GiB

Size: 500 MiB

□ Manually specify layout

Filesystem: xfs

Label: data

Mountpoint: /data

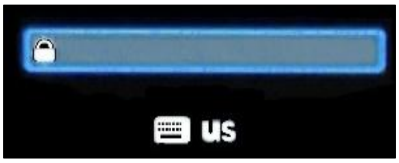
Encrypt: ☑

Encryption type: luks2

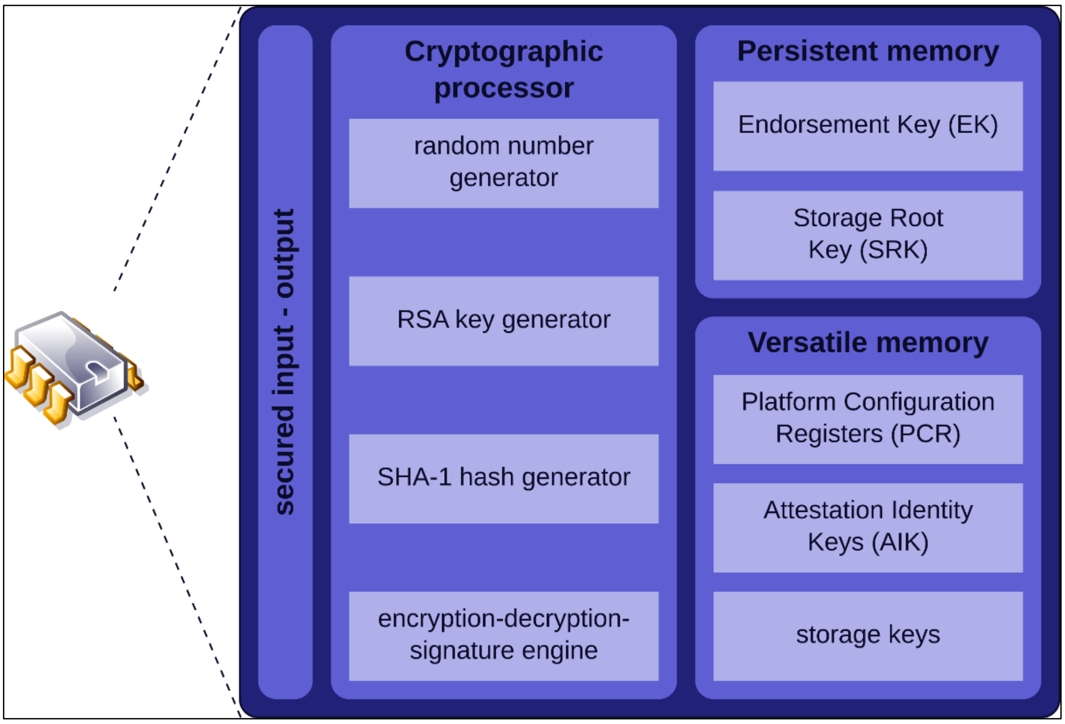
Sector size: Automatic

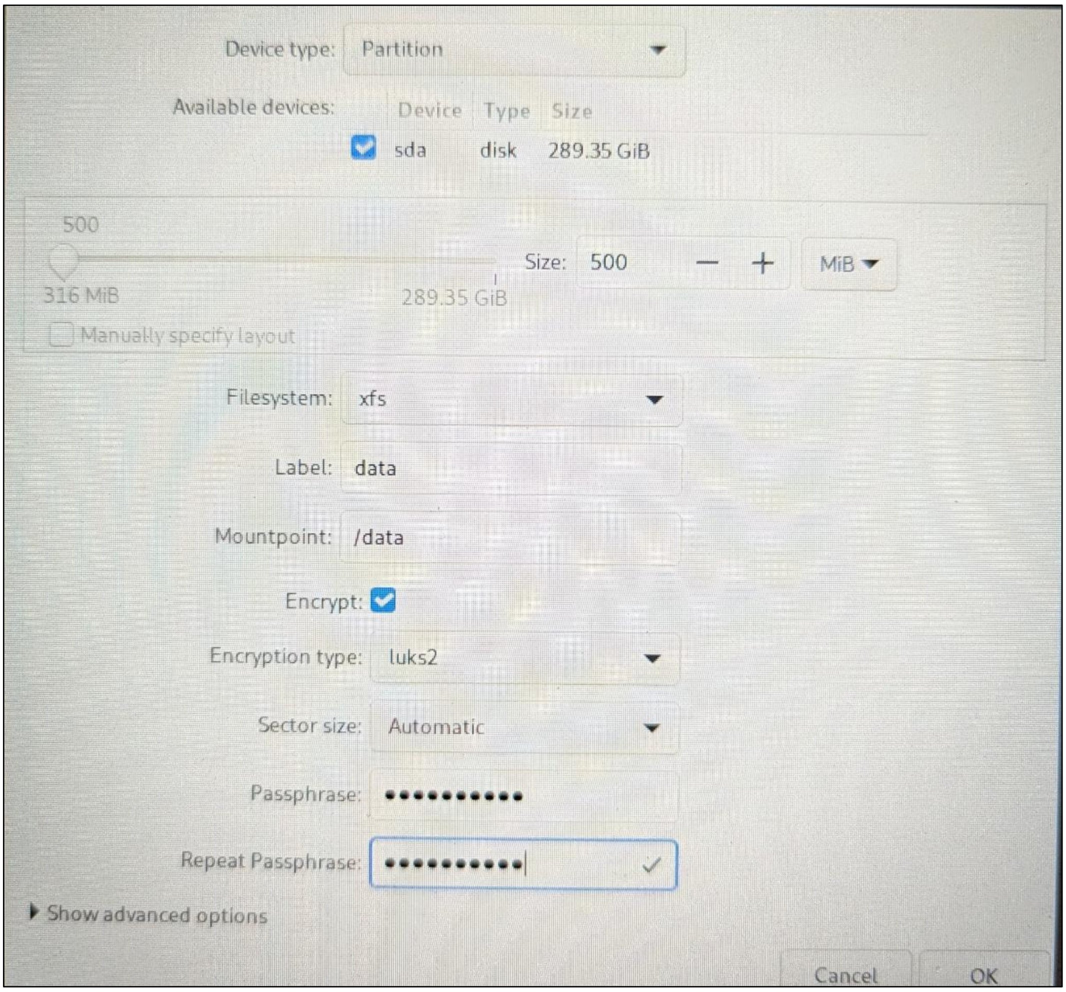
Passphrase: ••••••••••••••

Repeat Passphrase: •••••••••••••• ✓



Chapter 7: The Trusted Platform Module





Device type: Partition

Available devices:

	Device	Type	Size
☑	sda	disk	289.35 GiB

500

316 MiB 289.35 GiB

Size: 500 MiB

□ Manually specify layout

Filesystem: xfs

Label: data

Mountpoint: /data

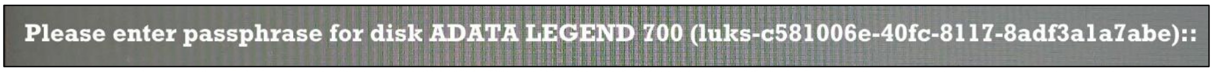
Encrypt: ☑

Encryption type: luks2

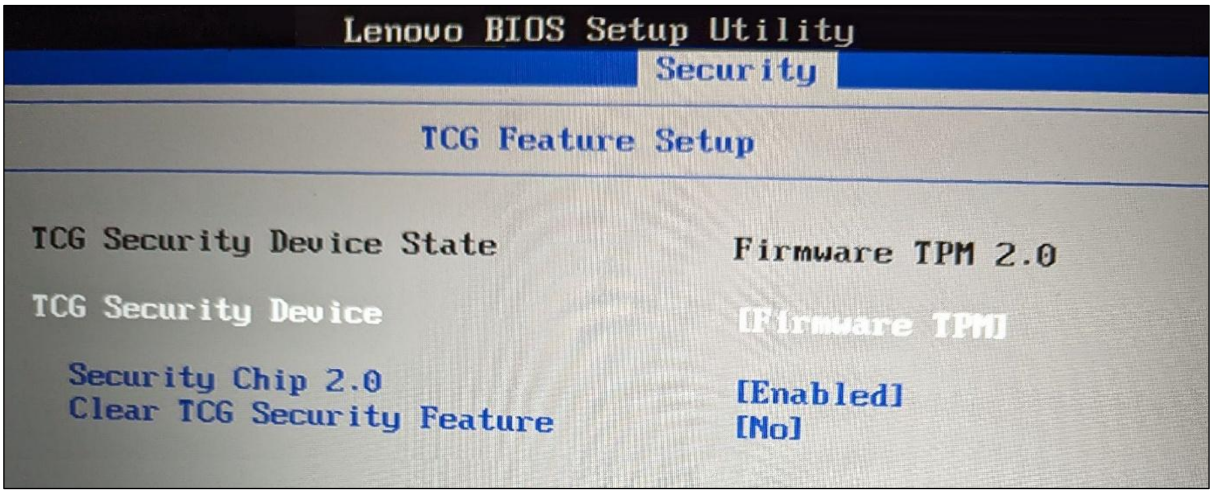
Sector size: Automatic

Passphrase: •••••••••••

Repeat Passphrase: ••••••••••• ✓

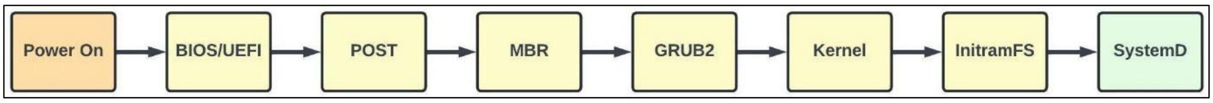


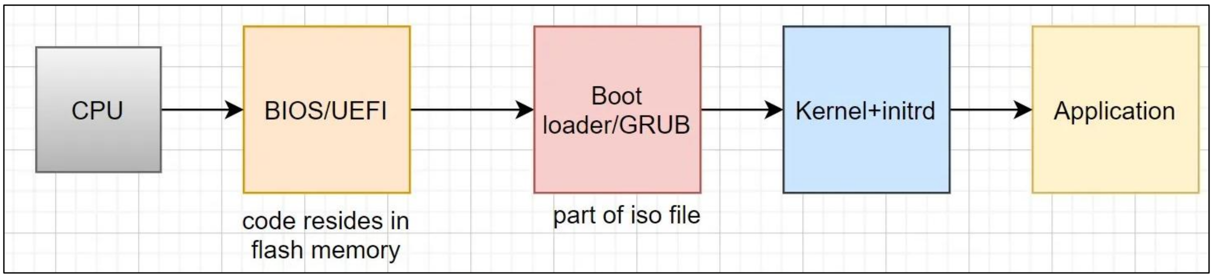
```
Please enter passphrase for disk ADATA LEGEND 700 (luks-c581006e-40fc-8117-8adf3a1a7abe)::
```

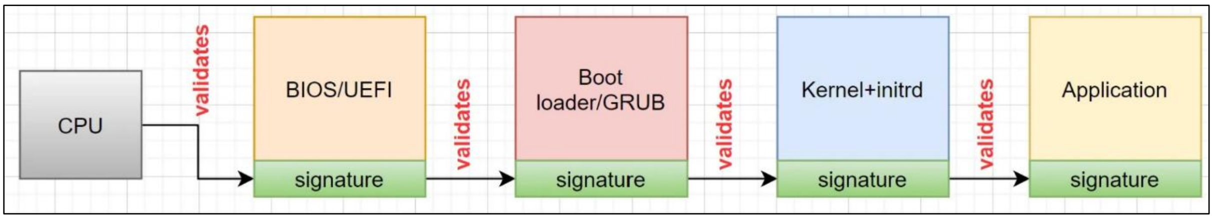


```
                    Lenovo BIOS Setup Utility
                                        Security

                        TCG Feature Setup

TCG Security Device State               Firmware TPM 2.0
TCG Security Device                     [Firmware TPM]
   Security Chip 2.0                    [Enabled]
   Clear TCG Security Feature           [No]
```

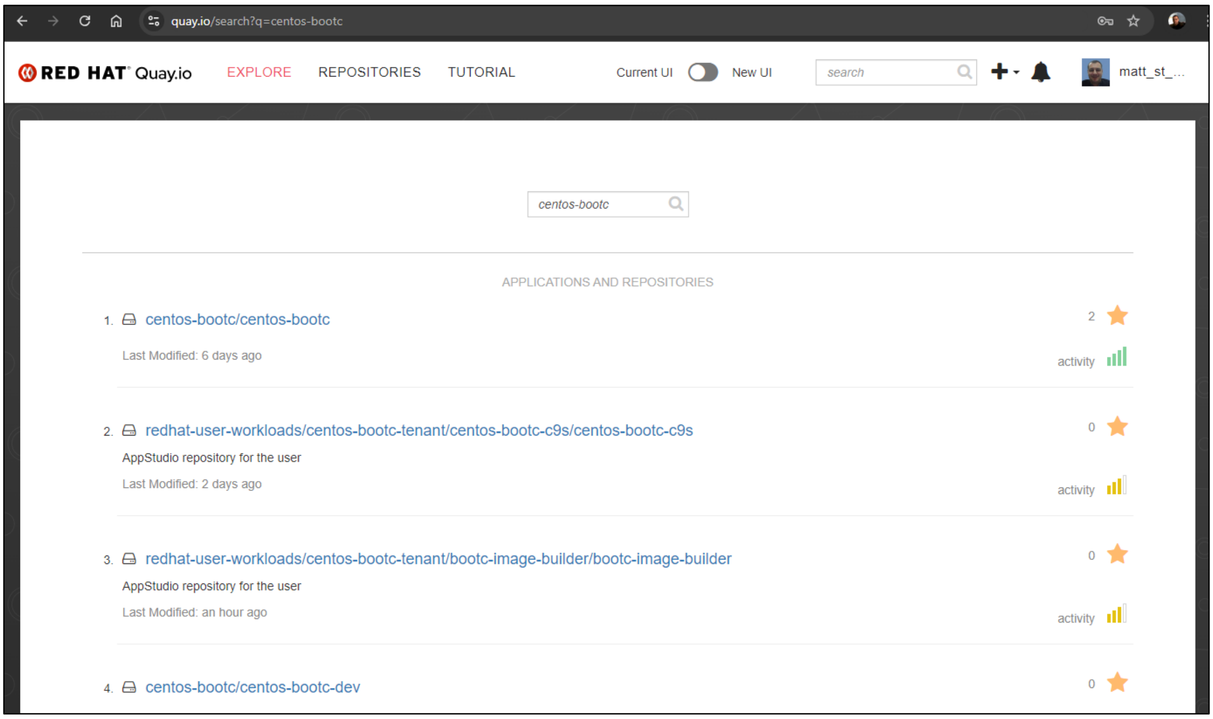
Chapter 8: Boot, BIOS, and Firmware Security







Chapter 9: Image-Based Deployments



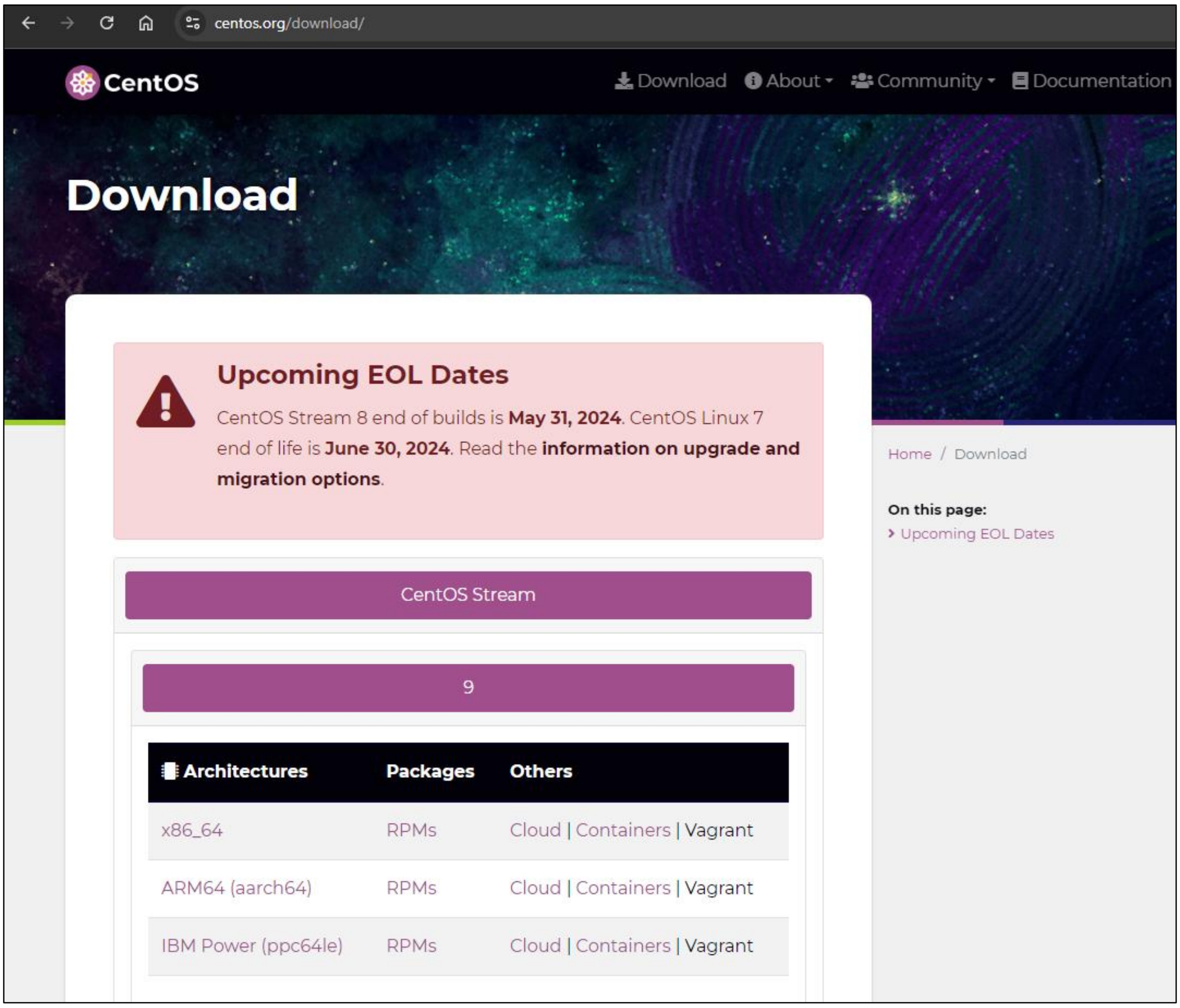
APPLICATIONS AND REPOSITORIES

1. centos-bootc/centos-bootc — 2 ★
   Last Modified: 6 days ago — activity

2. redhat-user-workloads/centos-bootc-tenant/centos-bootc-c9s/centos-bootc-c9s — 0 ★
   AppStudio repository for the user
   Last Modified: 2 days ago — activity

3. redhat-user-workloads/centos-bootc-tenant/bootc-image-builder/bootc-image-builder — 0 ★
   AppStudio repository for the user
   Last Modified: an hour ago — activity

4. centos-bootc/centos-bootc-dev — 0 ★



Download

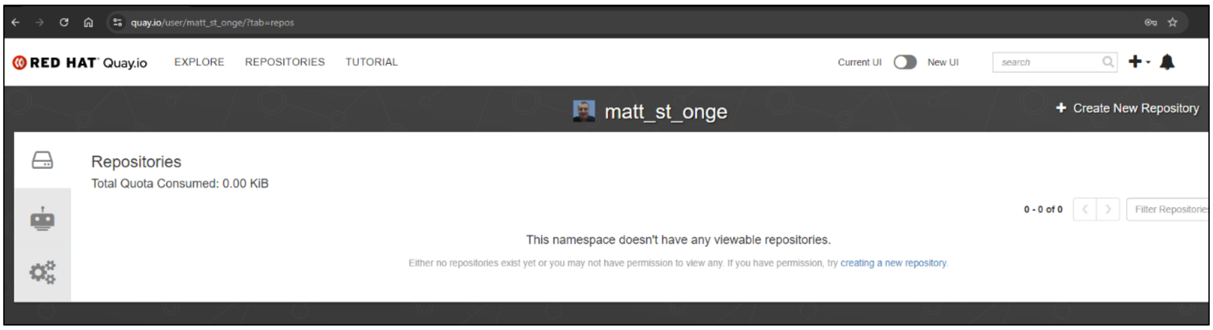
Upcoming EOL Dates

CentOS Stream 8 end of builds is **May 31, 2024**. CentOS Linux 7 end of life is **June 30, 2024**. Read the **information on upgrade and migration options**.

CentOS Stream

9

Architectures	Packages	Others
x86_64	RPMs	Cloud | Containers | Vagrant
ARM64 (aarch64)	RPMs	Cloud | Containers | Vagrant
IBM Power (ppc64le)	RPMs	Cloud | Containers | Vagrant



quay.io/user/matt_st_onge/?tab=repos

matt_st_onge

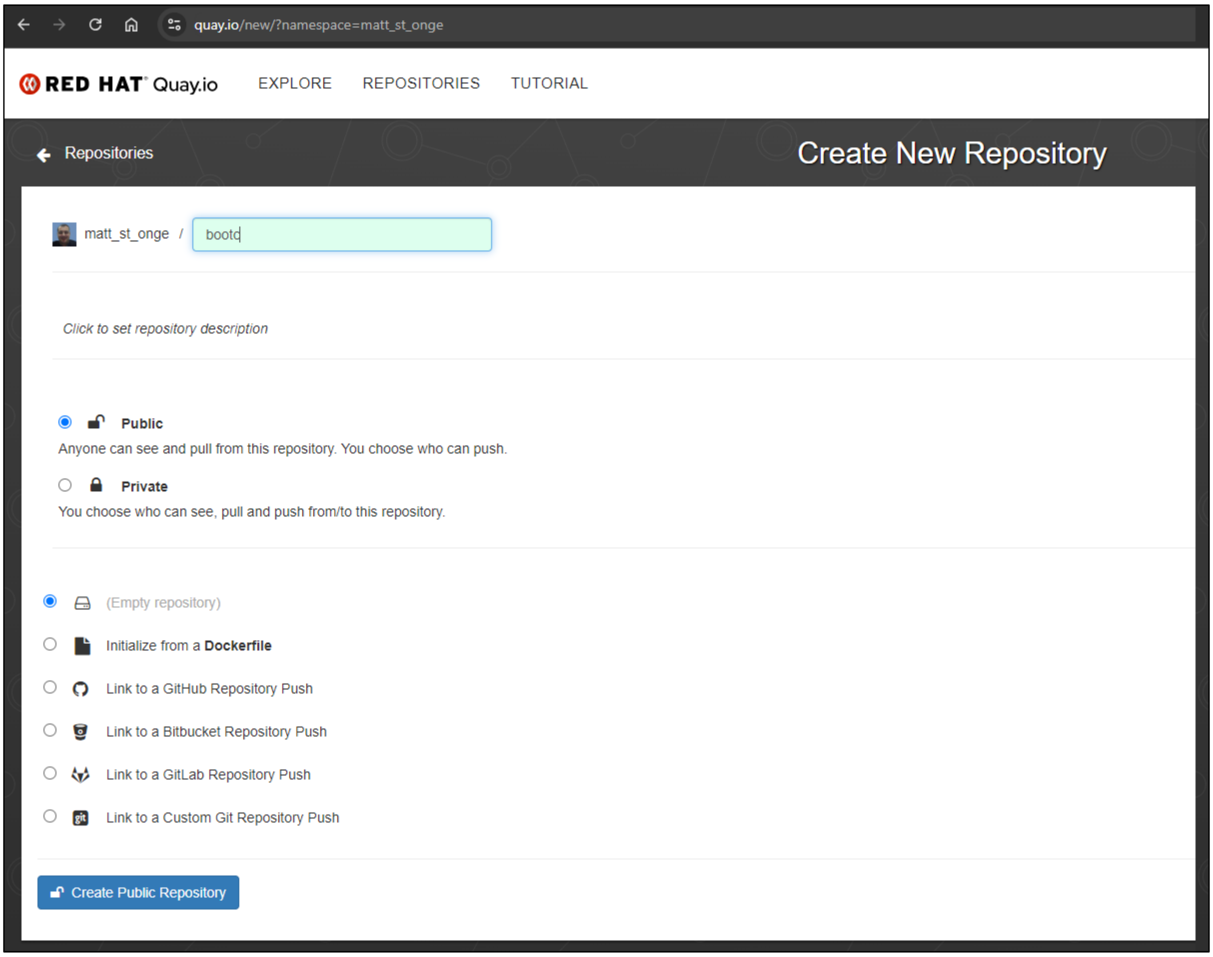
Repositories

Total Quota Consumed: 0.00 KiB

0 - 0 of 0

This namespace doesn't have any viewable repositories.

Either no repositories exist yet or you may not have permission to view any. If you have permission, try creating a new repository.



quay.io/new/?namespace=matt_st_onge

Create New Repository

matt_st_onge / bootc

Click to set repository description

● **Public**
Anyone can see and pull from this repository. You choose who can push.

○ **Private**
You choose who can see, pull and push from/to this repository.

● (Empty repository)

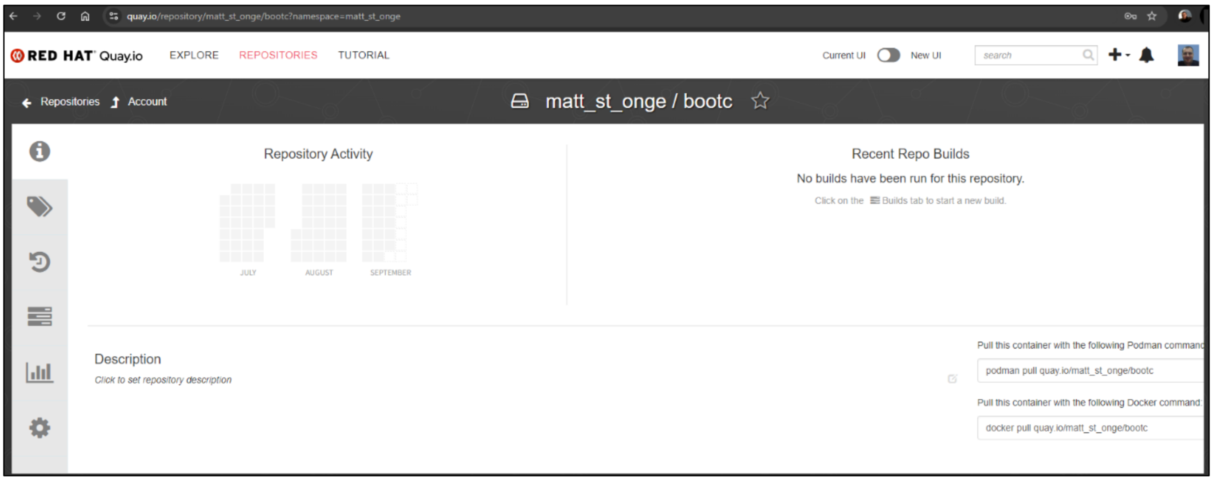
○ Initialize from a **Dockerfile**

○ Link to a GitHub Repository Push

○ Link to a Bitbucket Repository Push

○ Link to a GitLab Repository Push

○ Link to a Custom Git Repository Push



quay.io/repository/matt_st_onge/bootc?namespace=matt_st_onge

matt_st_onge / bootc

Repository Activity

Recent Repo Builds

No builds have been run for this repository.

Click on the Builds tab to start a new build.

Description

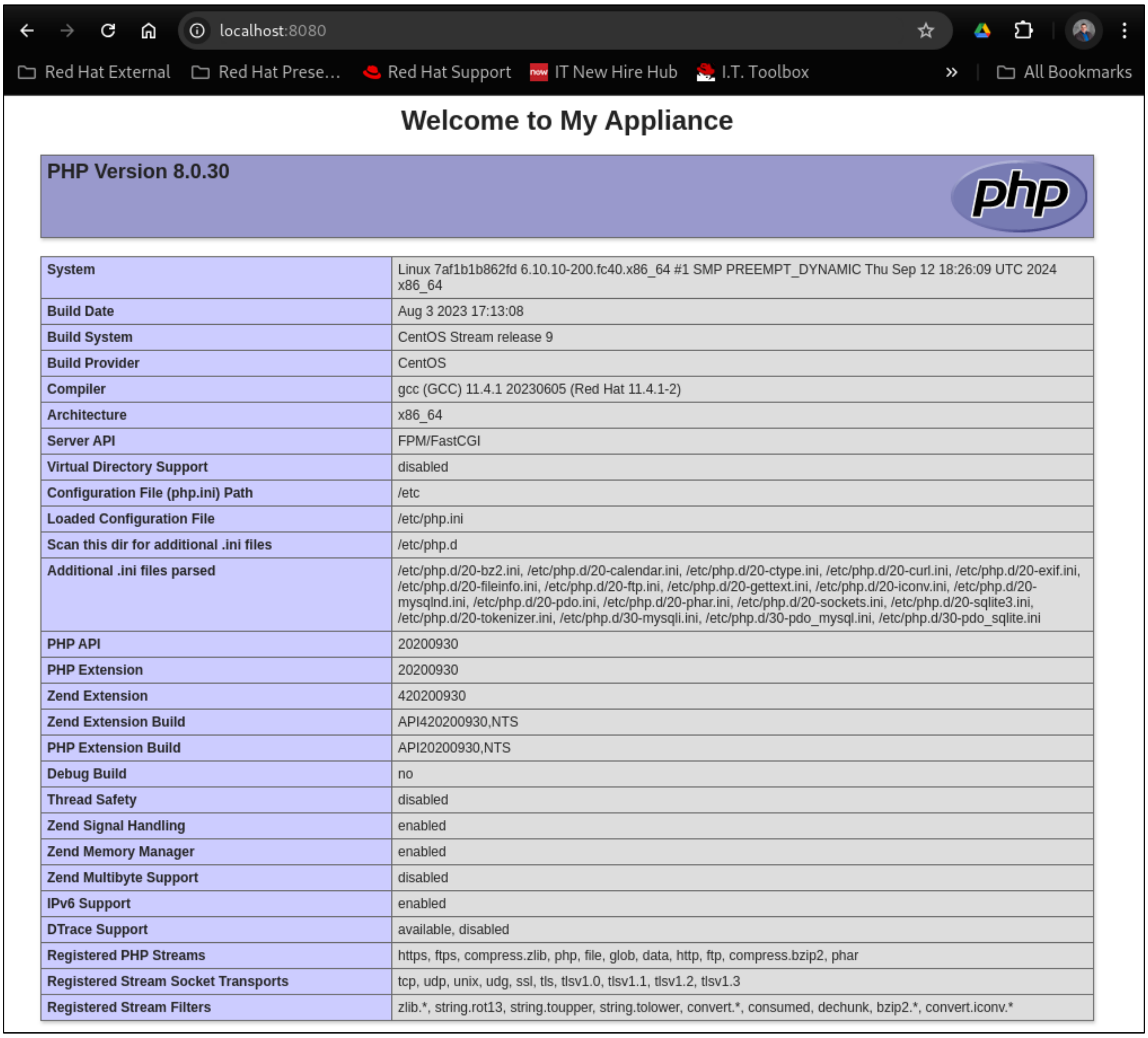
Click to set repository description

Pull this container with the following Podman command

```
podman pull quay.io/matt_st_onge/bootc
```

Pull this container with the following Docker command:

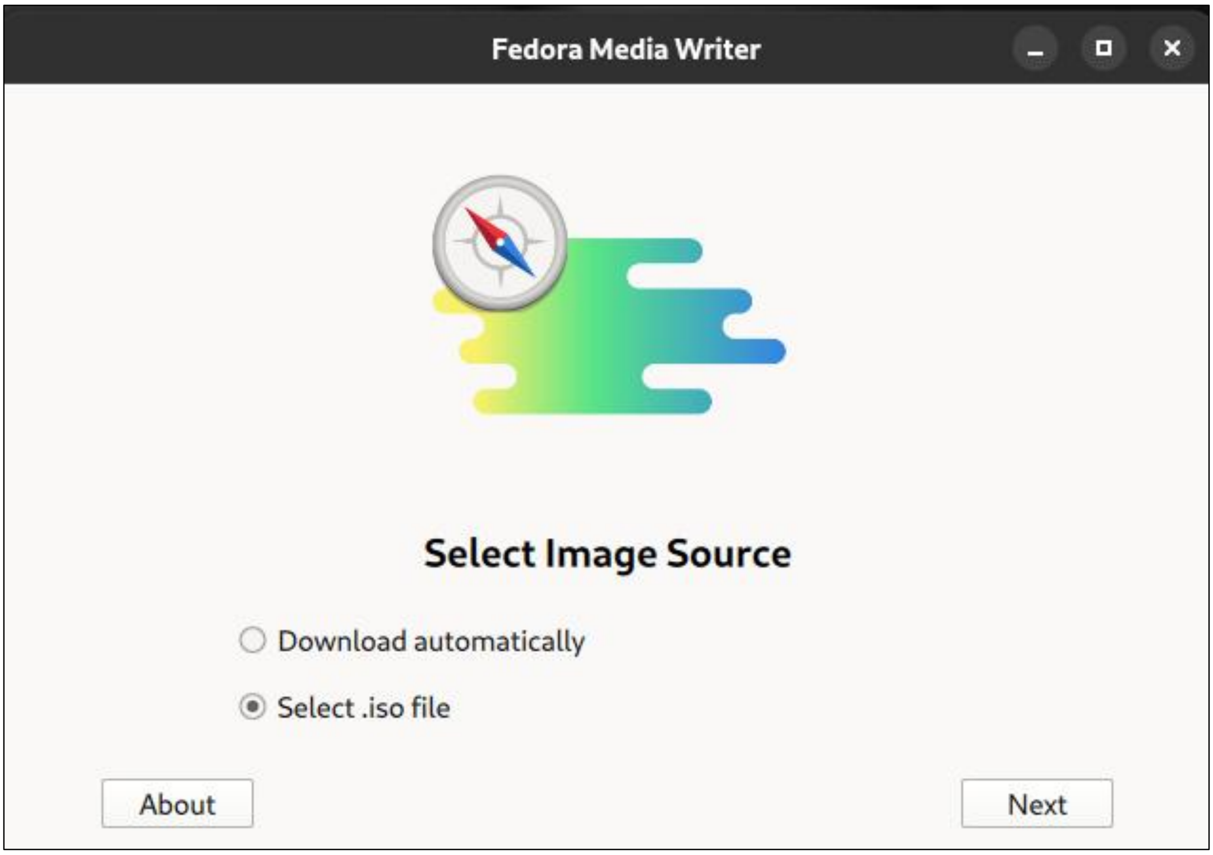
```
docker pull quay.io/matt_st_onge/bootc
```



Welcome to My Appliance

PHP Version 8.0.30

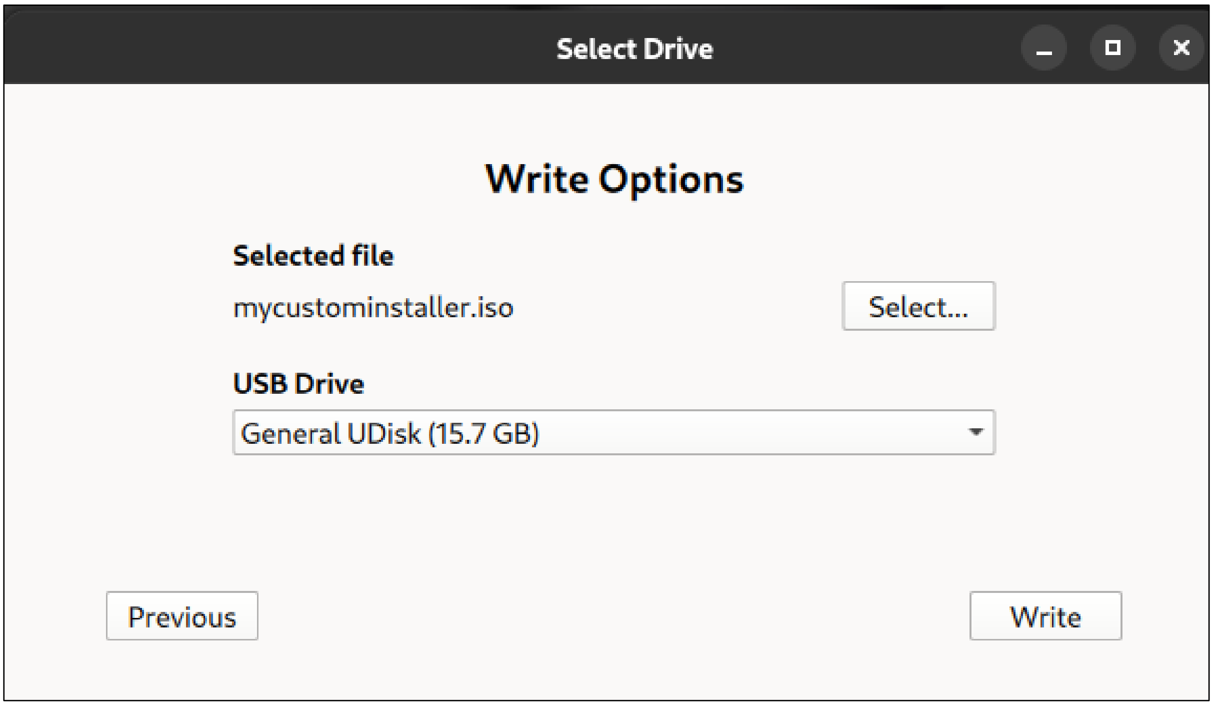
System	Linux 7af1b1b862fd 6.10.10-200.fc40.x86_64 #1 SMP PREEMPT_DYNAMIC Thu Sep 12 18:26:09 UTC 2024 x86_64
Build Date	Aug 3 2023 17:13:08
Build System	CentOS Stream release 9
Build Provider	CentOS
Compiler	gcc (GCC) 11.4.1 20230605 (Red Hat 11.4.1-2)
Architecture	x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,NTS
PHP Extension Build	API20200930,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*



Select Image Source

○ Download automatically

● Select .iso file



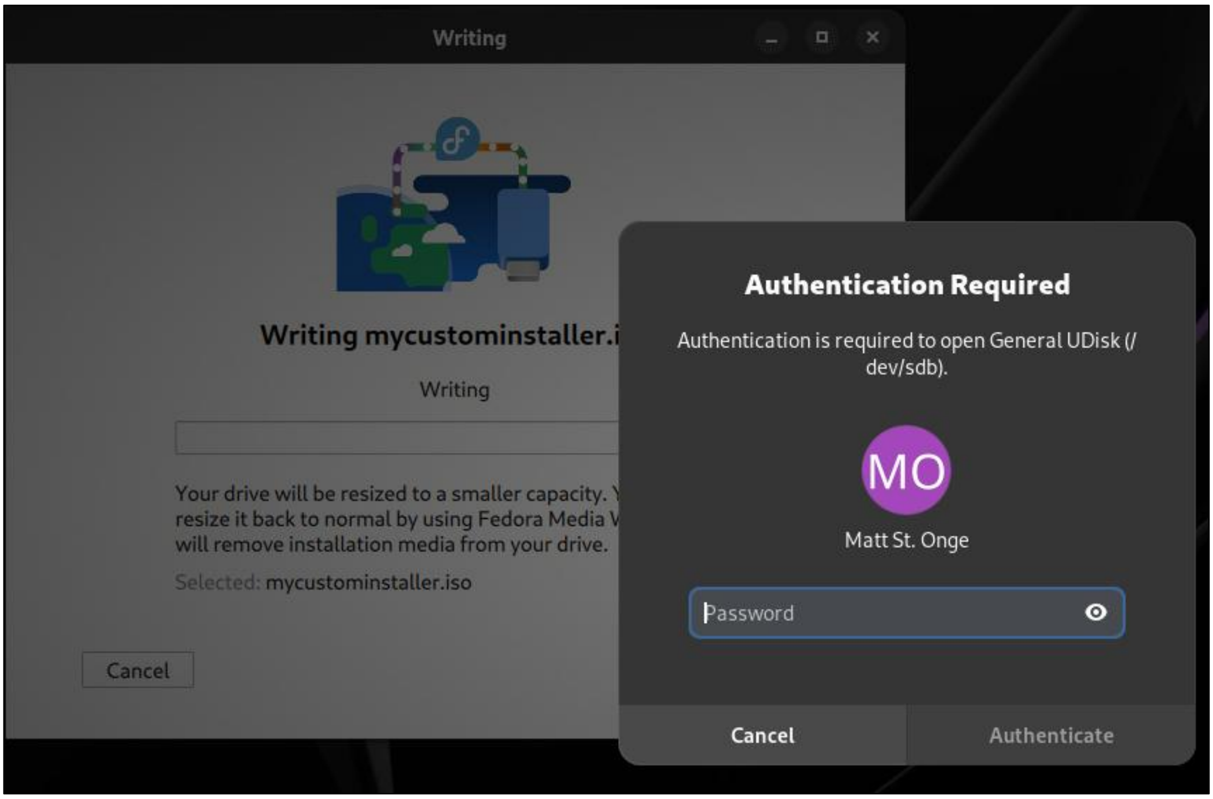
Write Options

Selected file

mycustominstaller.iso

USB Drive

General UDisk (15.7 GB)



Writing

Writing mycustominstaller.i

Writing

Your drive will be resized to a smaller capacity. Y
resize it back to normal by using Fedora Media W
will remove installation media from your drive.

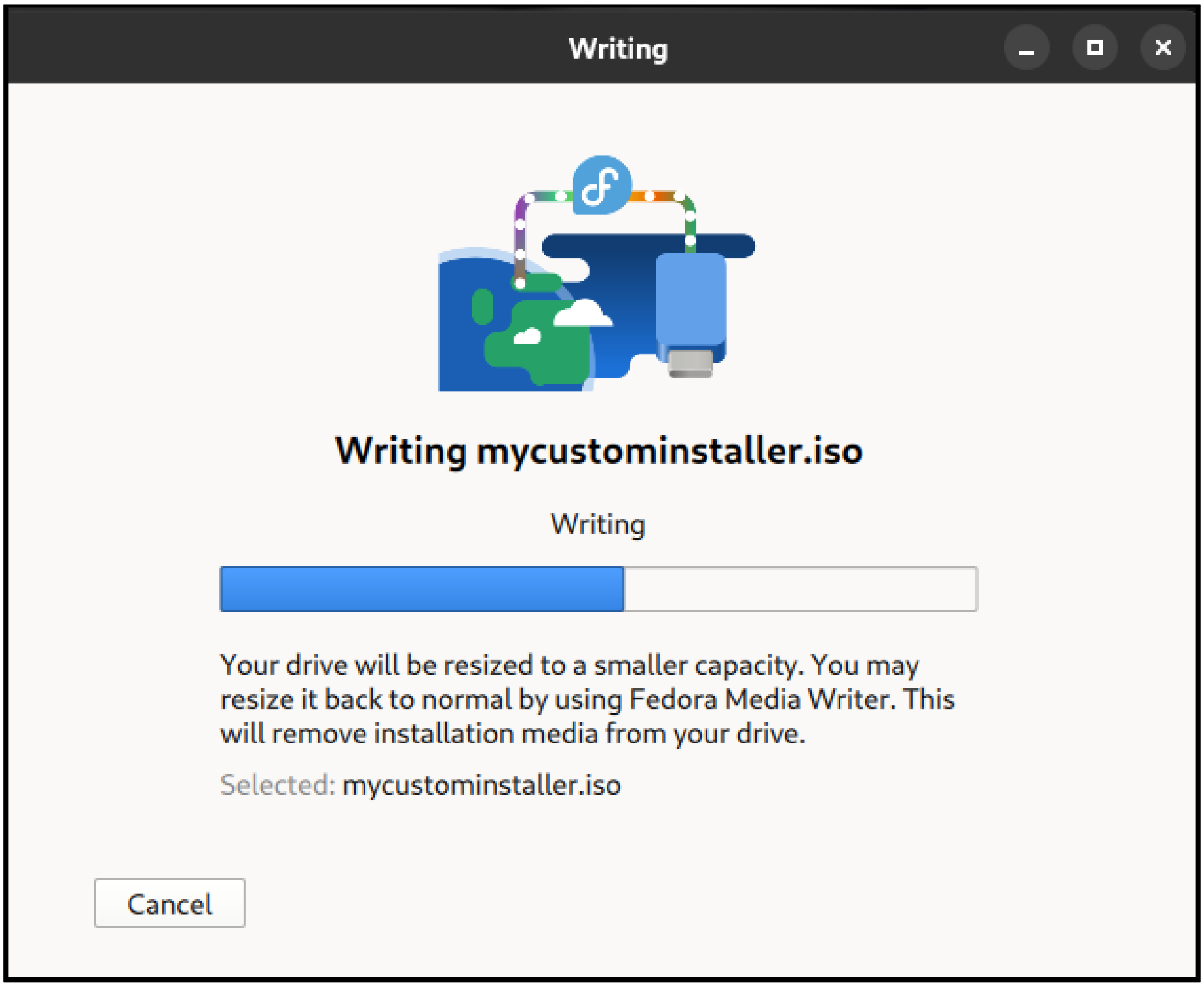
Selected: mycustominstaller.iso

Authentication Required

Authentication is required to open General UDisk (/dev/sdb).

Matt St. Onge

Password



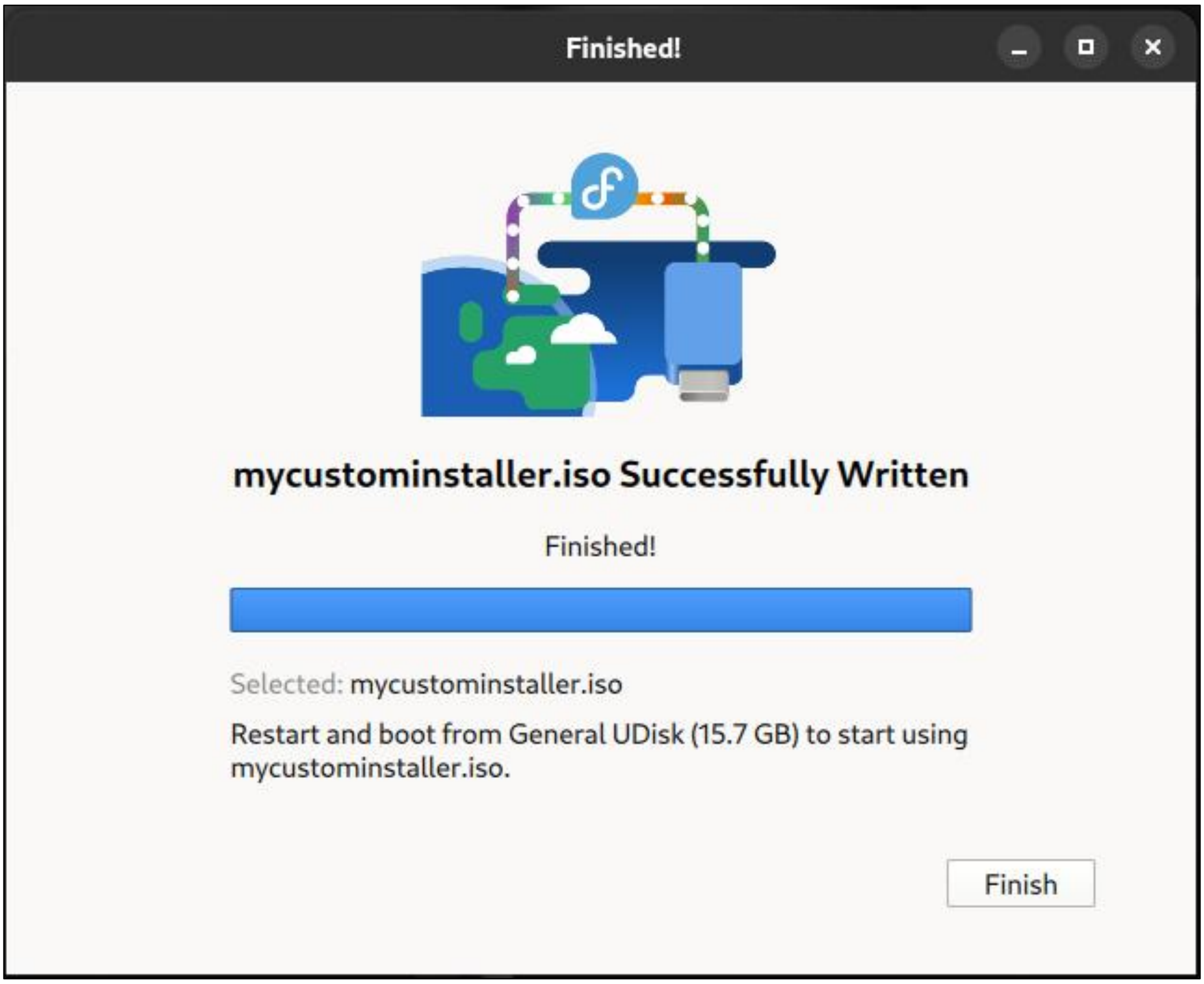
Writing

Writing mycustominstaller.iso

Writing

Your drive will be resized to a smaller capacity. You may resize it back to normal by using Fedora Media Writer. This will remove installation media from your drive.

Selected: mycustominstaller.iso

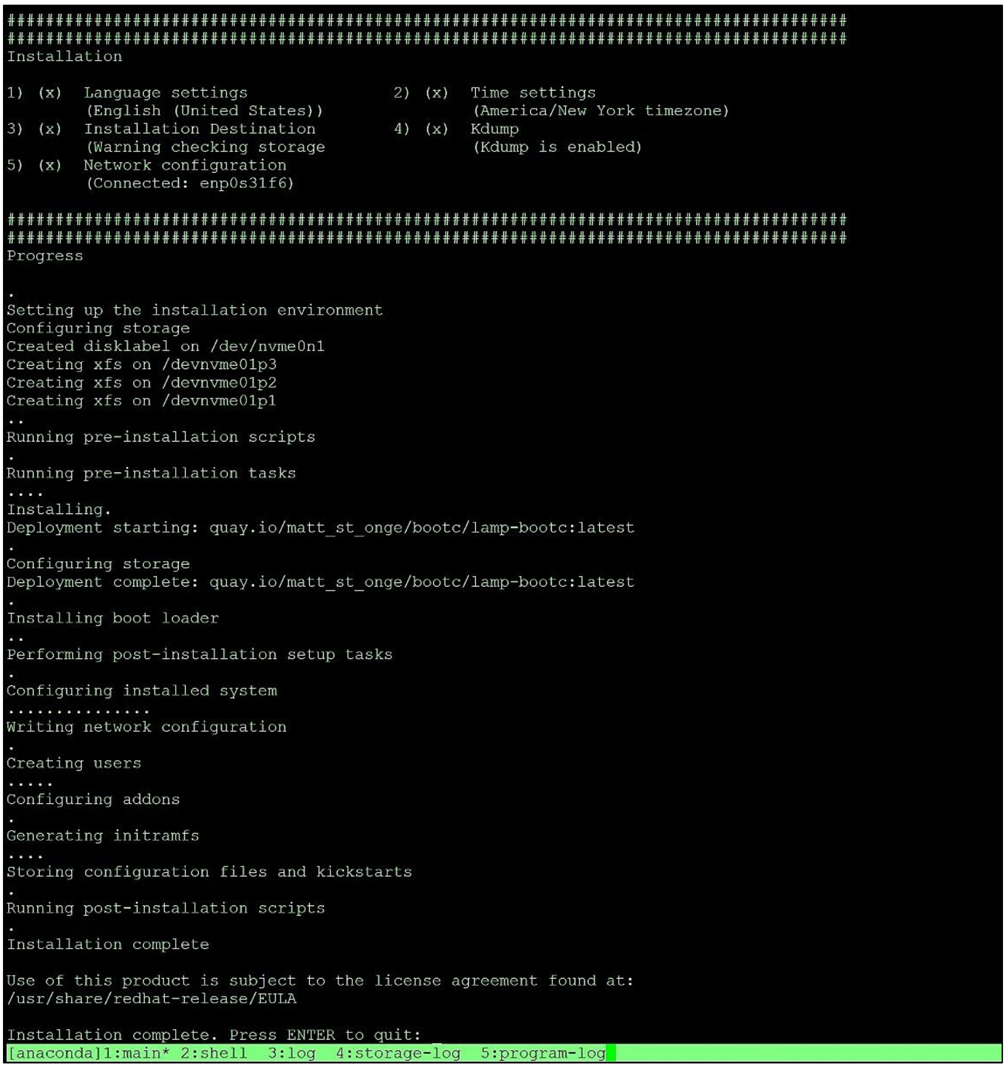


mycustominstaller.iso Successfully Written

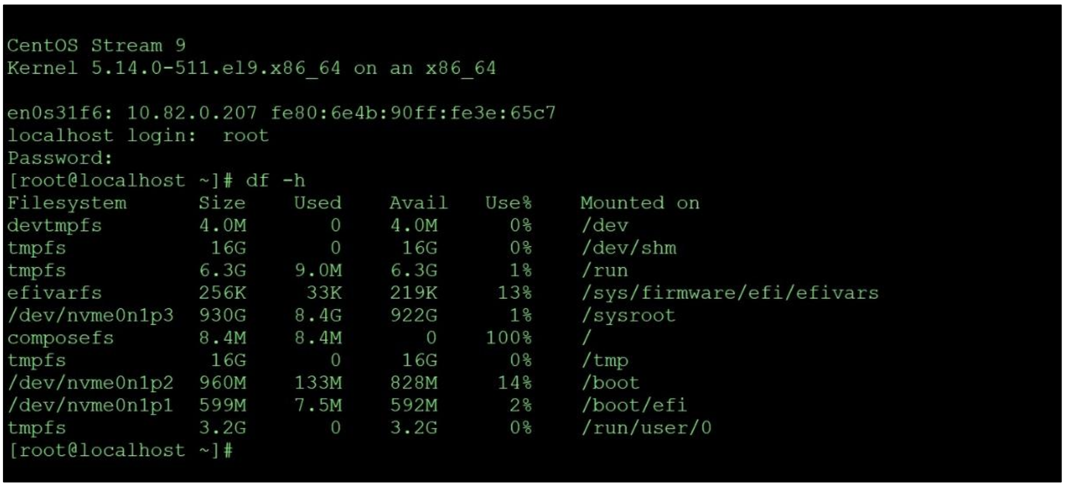
Finished!

Selected: mycustominstaller.iso

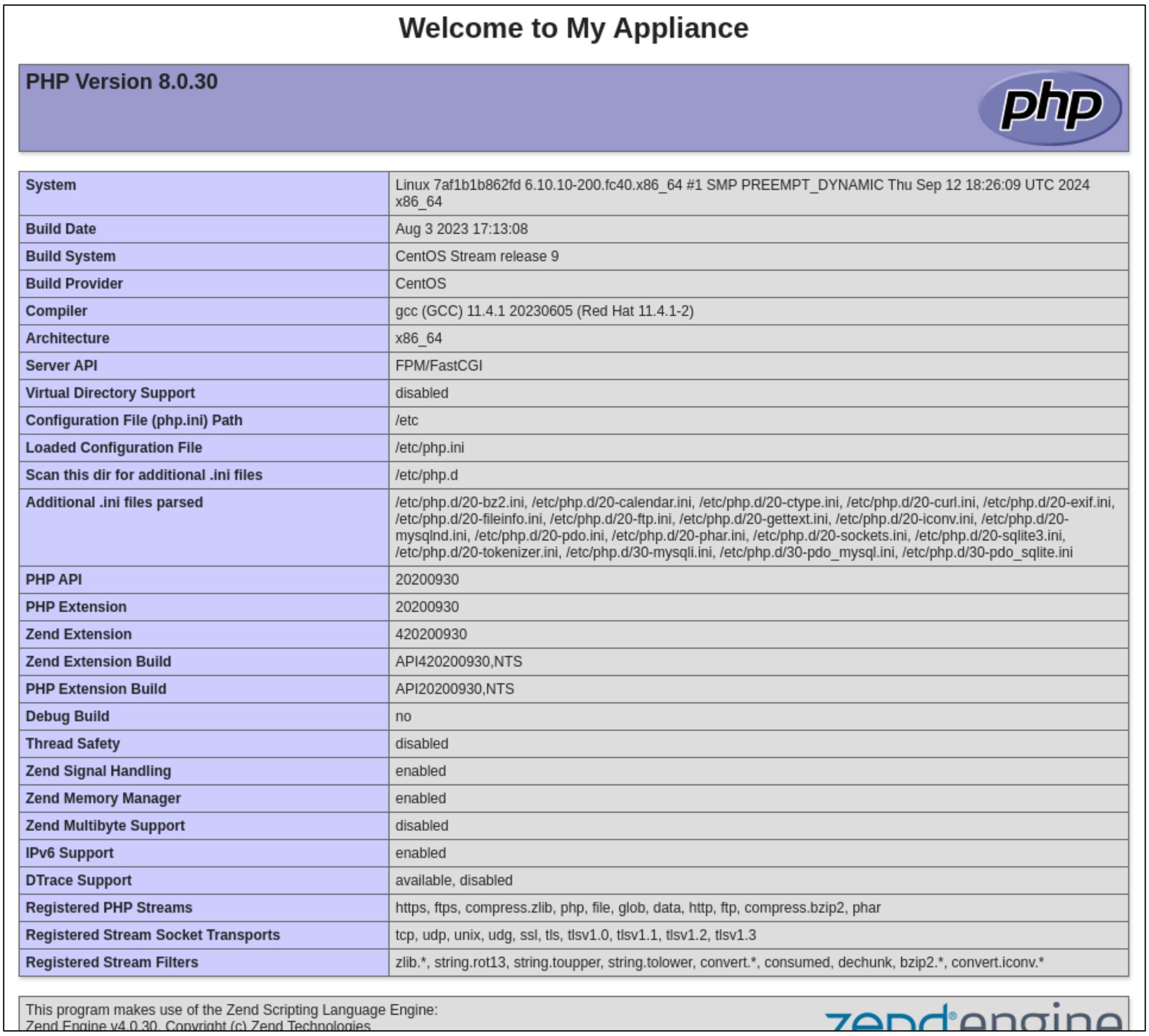
Restart and boot from General UDisk (15.7 GB) to start using mycustominstaller.iso.



```
#######################################################################################
#######################################################################################
Installation

1) (x)  Language settings               2) (x)  Time settings
        (English (United States))               (America/New York timezone)
3) (x)  Installation Destination        4) (x)  Kdump
        (Warning checking storage               (Kdump is enabled)
5) (x)  Network configuration
        (Connected: enp0s31f6)

#######################################################################################
#######################################################################################
Progress

.
Setting up the installation environment
Configuring storage
Created disklabel on /dev/nvme0n1
Creating xfs on /devnvme01p3
Creating xfs on /devnvme01p2
Creating xfs on /devnvme01p1
..
Running pre-installation scripts
.
Running pre-installation tasks
....
Installing.
Deployment starting: quay.io/matt_st_onge/bootc/lamp-bootc:latest
.
Configuring storage
Deployment complete: quay.io/matt_st_onge/bootc/lamp-bootc:latest
.
Installing boot loader
..
Performing post-installation setup tasks
.
Configuring installed system
...............
Writing network configuration
.
Creating users
.....
Configuring addons
.
Generating initramfs
....
Storing configuration files and kickstarts
.
Running post-installation scripts
.
Installation complete

Use of this product is subject to the license agreement found at:
/usr/share/redhat-release/EULA

Installation complete. Press ENTER to quit:
[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log
```



```
CentOS Stream 9
Kernel 5.14.0-511.el9.x86_64 on an x86_64

en0s31f6: 10.82.0.207 fe80:6e4b:90ff:fe3e:65c7
localhost login:  root
Password:
[root@localhost ~]# df -h
Filesystem       Size    Used    Avail   Use%    Mounted on
devtmpfs         4.0M       0    4.0M      0%    /dev
tmpfs             16G       0     16G      0%    /dev/shm
tmpfs            6.3G    9.0M    6.3G      1%    /run
efivarfs         256K     33K    219K     13%    /sys/firmware/efi/efivars
/dev/nvme0n1p3   930G    8.4G    922G      1%    /sysroot
composefs        8.4M    8.4M       0    100%    /
tmpfs             16G       0     16G      0%    /tmp
/dev/nvme0n1p2   960M    133M    828M     14%    /boot
/dev/nvme0n1p1   599M    7.5M    592M      2%    /boot/efi
tmpfs            3.2G       0    3.2G      0%    /run/user/0
[root@localhost ~]#
```

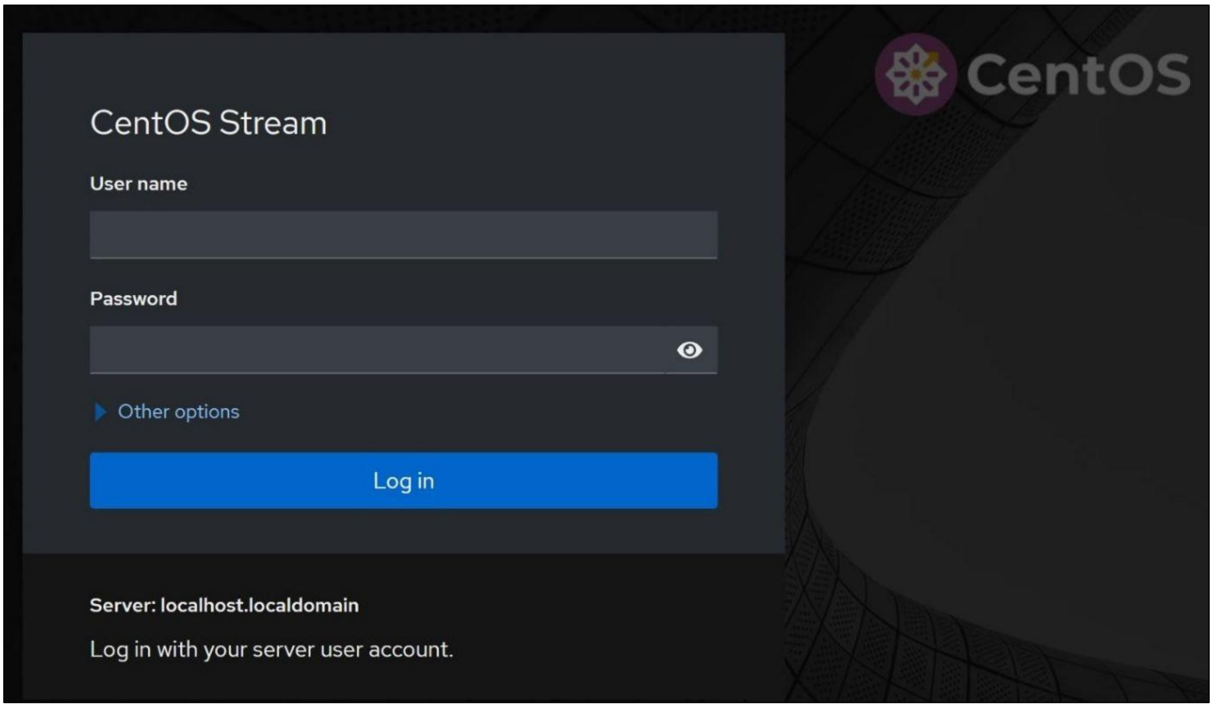


Welcome to My Appliance

PHP Version 8.0.30

System	Linux 7af1b1b862fd 6.10.10-200.fc40.x86_64 #1 SMP PREEMPT_DYNAMIC Thu Sep 12 18:26:09 UTC 2024 x86_64
Build Date	Aug 3 2023 17:13:08
Build System	CentOS Stream release 9
Build Provider	CentOS
Compiler	gcc (GCC) 11.4.1 20230605 (Red Hat 11.4.1-2)
Architecture	x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,NTS
PHP Extension Build	API20200930,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

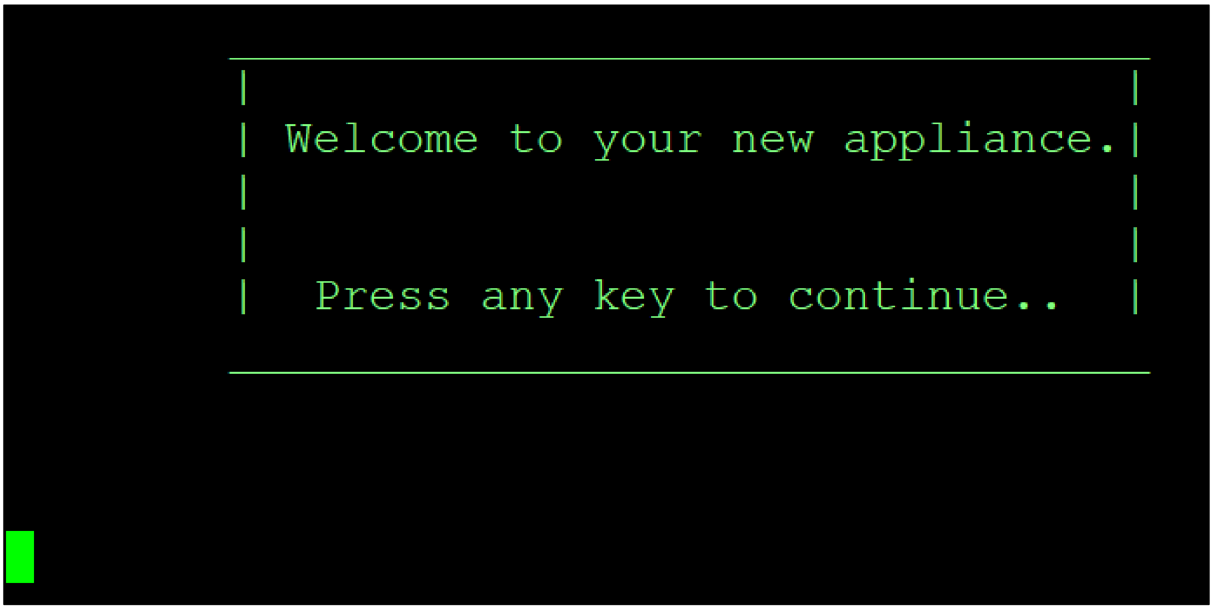
This program makes use of the Zend Scripting Language Engine:
Zend Engine v4.0.30, Copyright (c) Zend Technologies



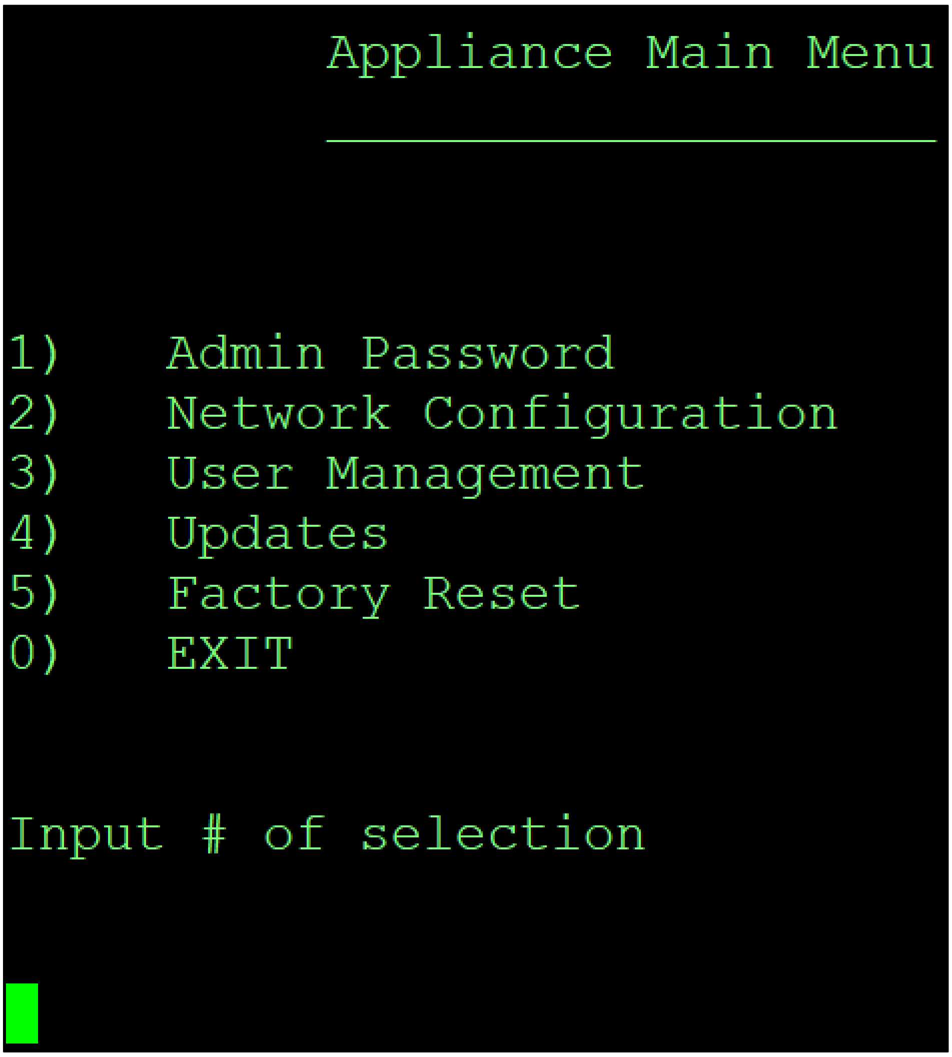
Server: localhost.localdomain

Log in with your server user account.

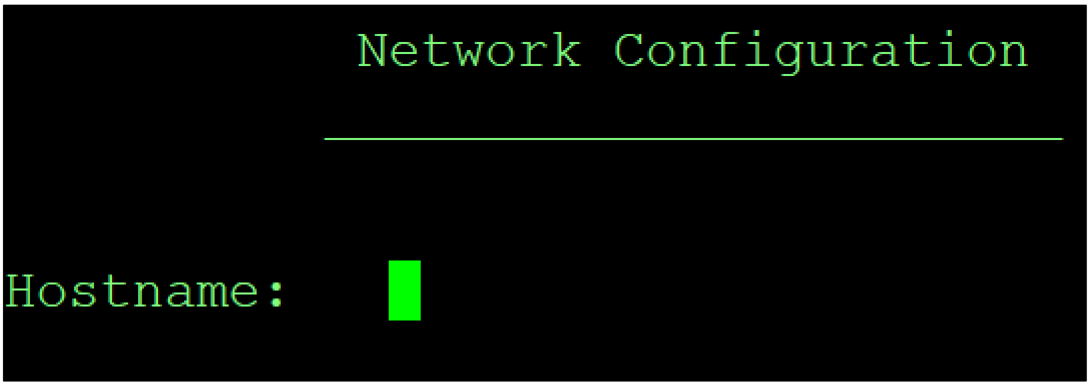
Chapter 10: Childproofing the Solution: Protection from the End-User and Their Environment



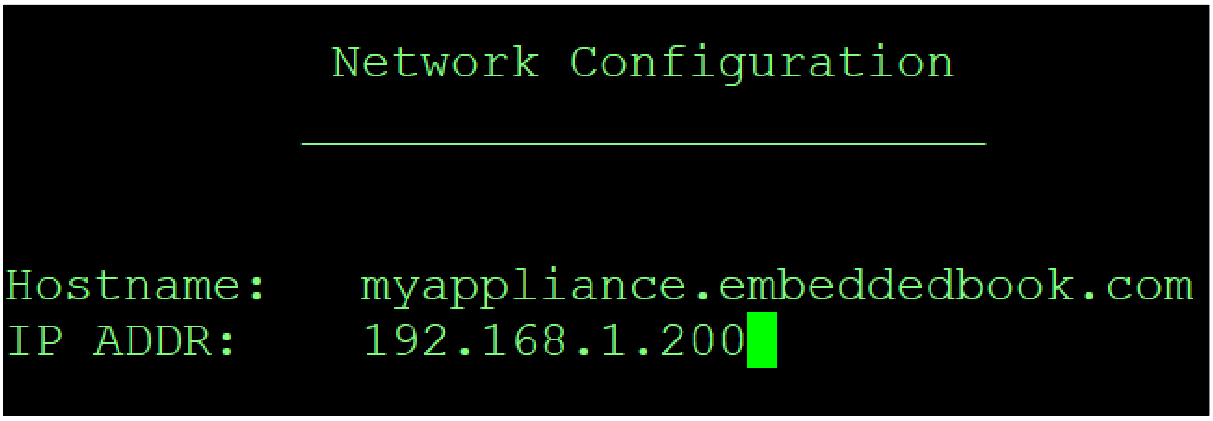
```
 ______________________________
|                              |
| Welcome to your new appliance.|
|                              |
|                              |
|  Press any key to continue.. |
 ______________________________
```



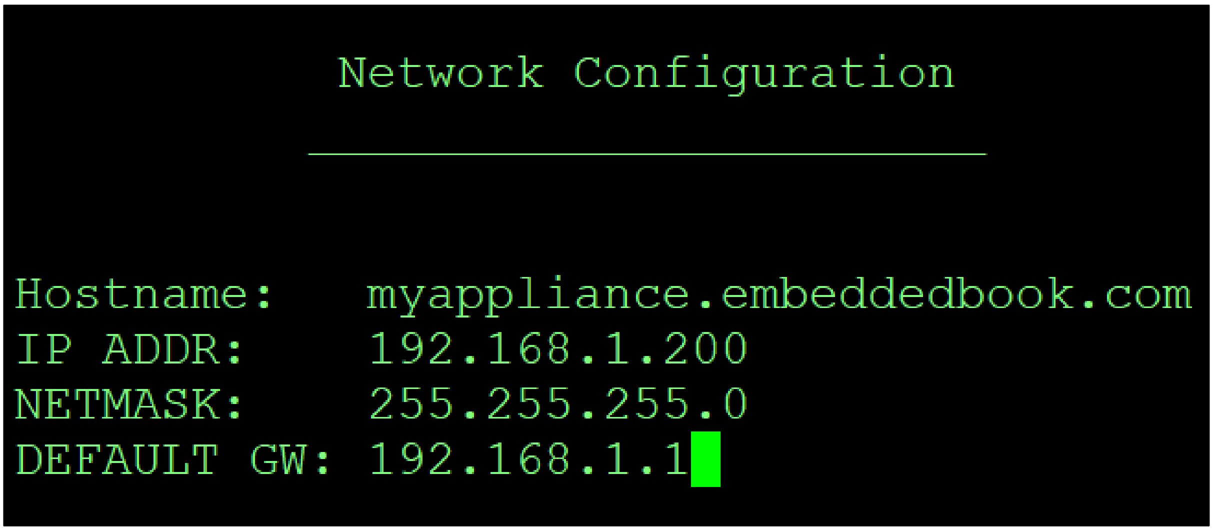
```
          Appliance Main Menu
          ___________________



1)    Admin Password
2)    Network Configuration
3)    User Management
4)    Updates
5)    Factory Reset
0)    EXIT


Input # of selection
```



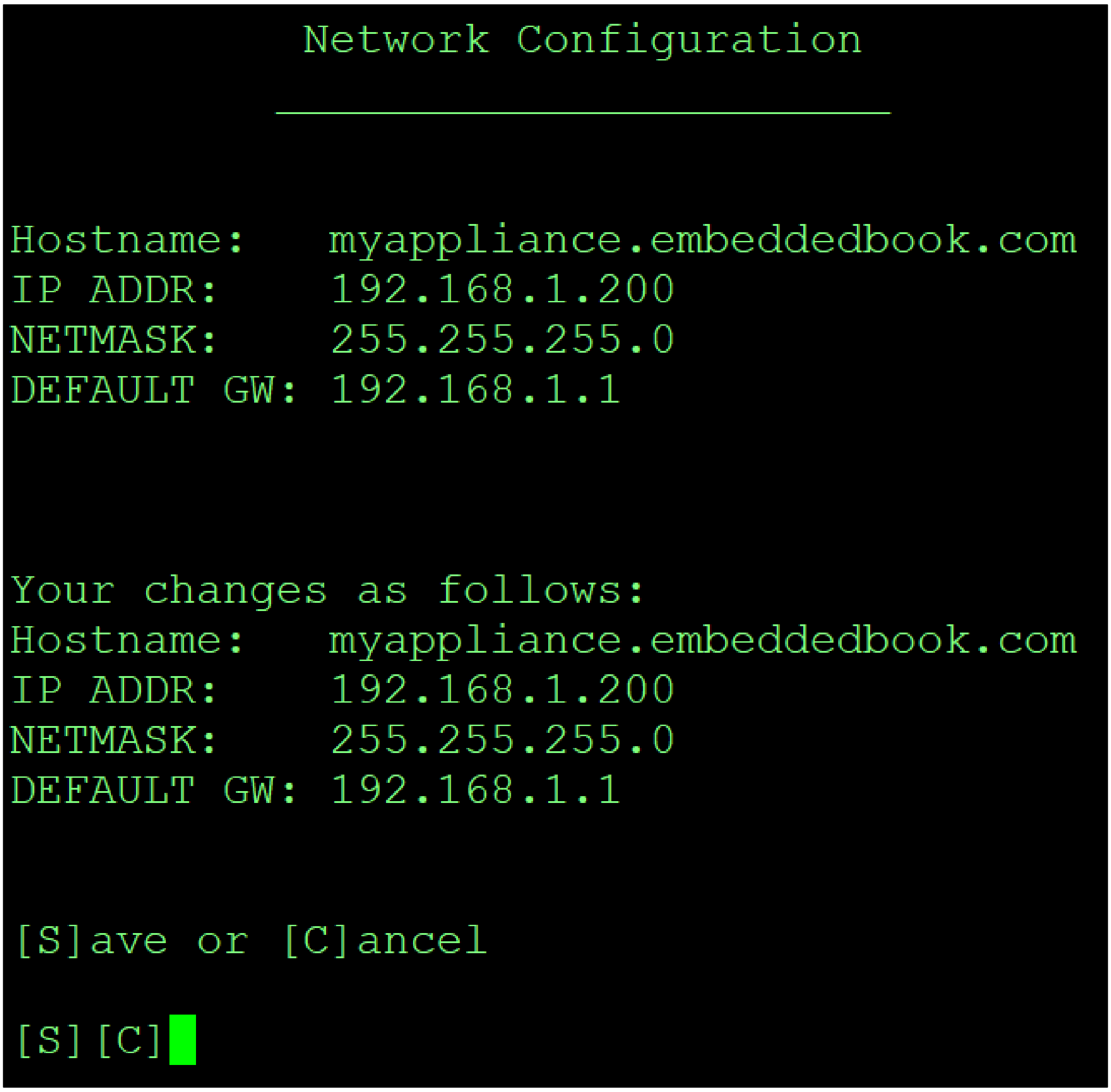
```
                Network Configuration
              _________________________________

Hostname:
```



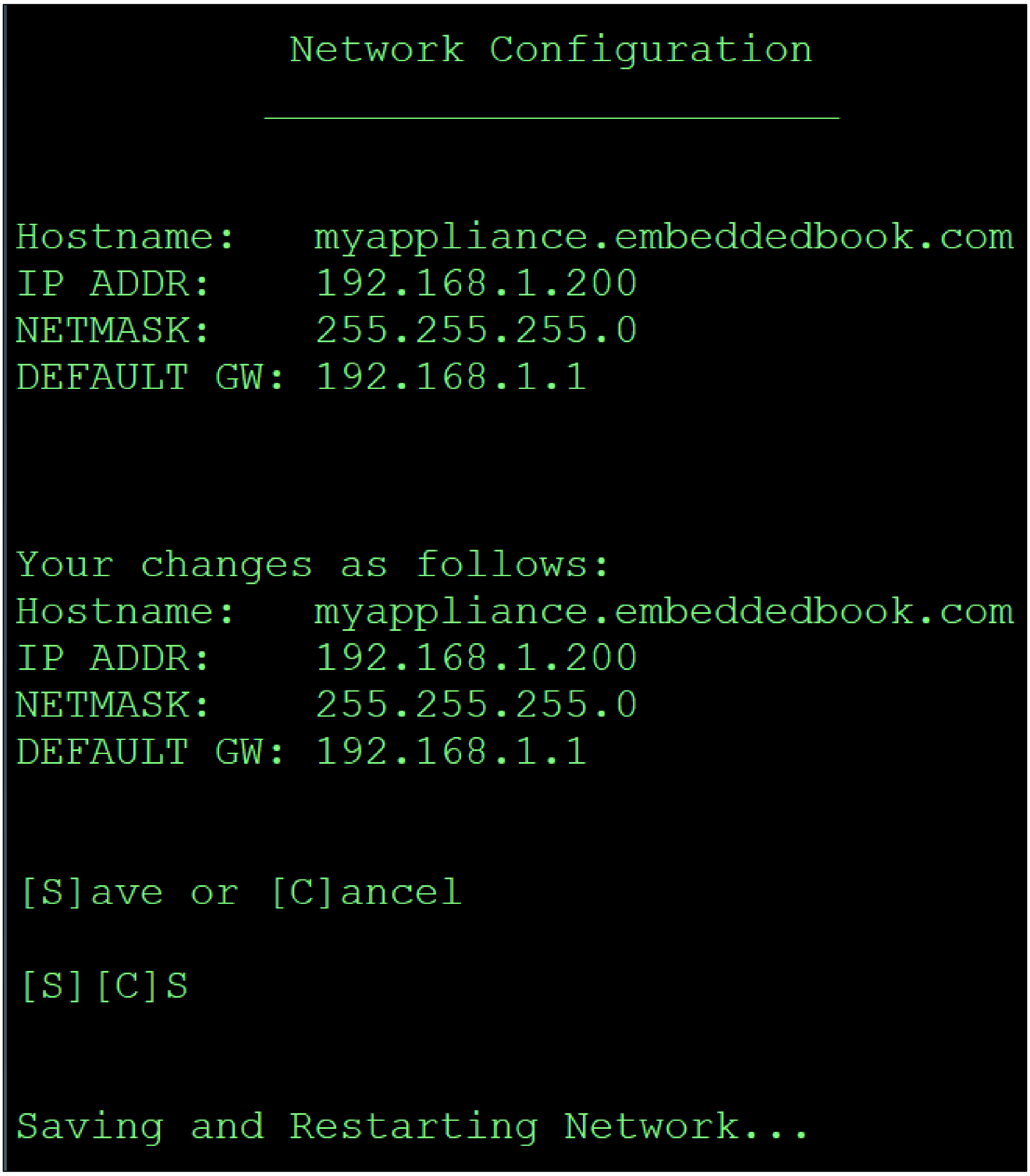
```
                Network Configuration
              _________________________________

Hostname:    myappliance.embeddedbook.com
IP ADDR:     192.168.1.200
```



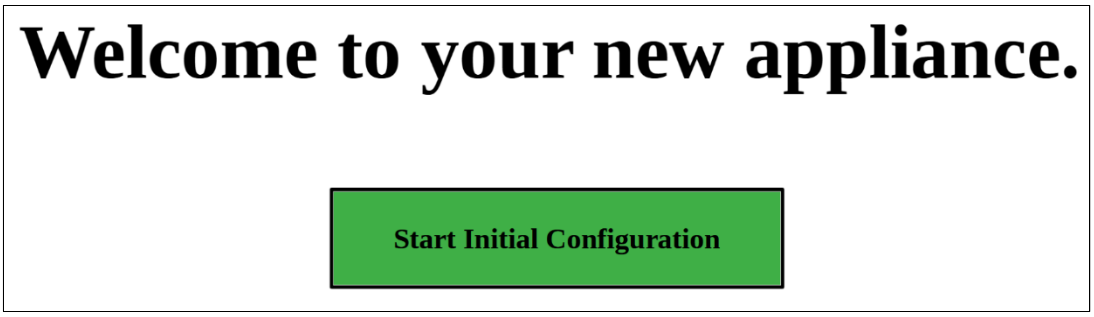
```
                Network Configuration
              _________________________________

Hostname:    myappliance.embeddedbook.com
IP ADDR:     192.168.1.200
NETMASK:     255.255.255.0
DEFAULT GW:  192.168.1.1
```



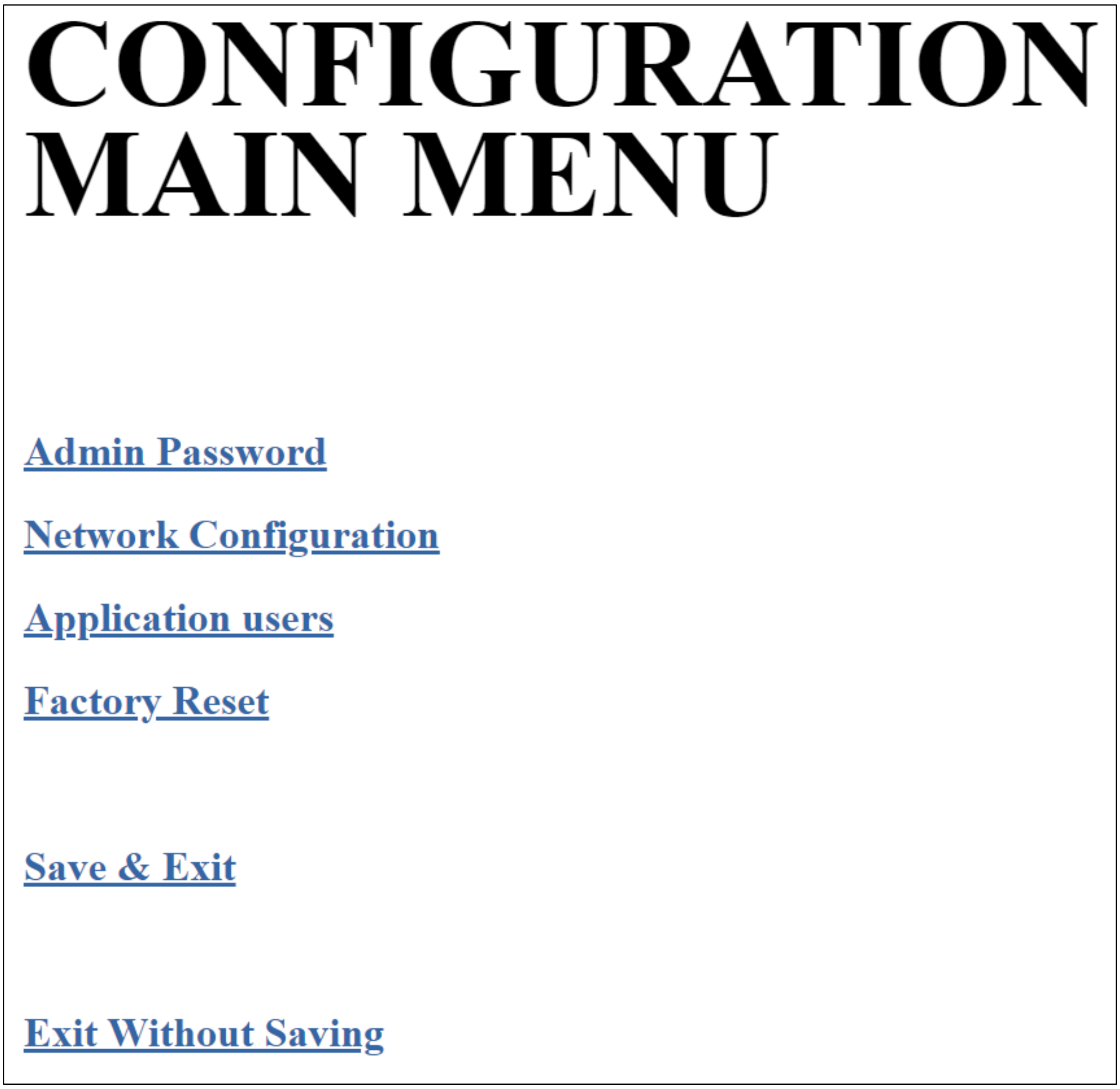
```
                 Network Configuration
                ________________________


Hostname:   myappliance.embeddedbook.com
IP ADDR:    192.168.1.200
NETMASK:    255.255.255.0
DEFAULT GW: 192.168.1.1




Your changes as follows:
Hostname:   myappliance.embeddedbook.com
IP ADDR:    192.168.1.200
NETMASK:    255.255.255.0
DEFAULT GW: 192.168.1.1


[S]ave or [C]ancel

[S][C]
```



```
            Network Configuration
           _______________________

Hostname:    myappliance.embeddedbook.com
IP ADDR:     192.168.1.200
NETMASK:     255.255.255.0
DEFAULT GW:  192.168.1.1



Your changes as follows:
Hostname:    myappliance.embeddedbook.com
IP ADDR:     192.168.1.200
NETMASK:     255.255.255.0
DEFAULT GW:  192.168.1.1


[S]ave or [C]ancel

[S][C]S


Saving and Restarting Network...
```



Welcome to your new appliance.



CONFIGURATION MAIN MENU

Admin Password

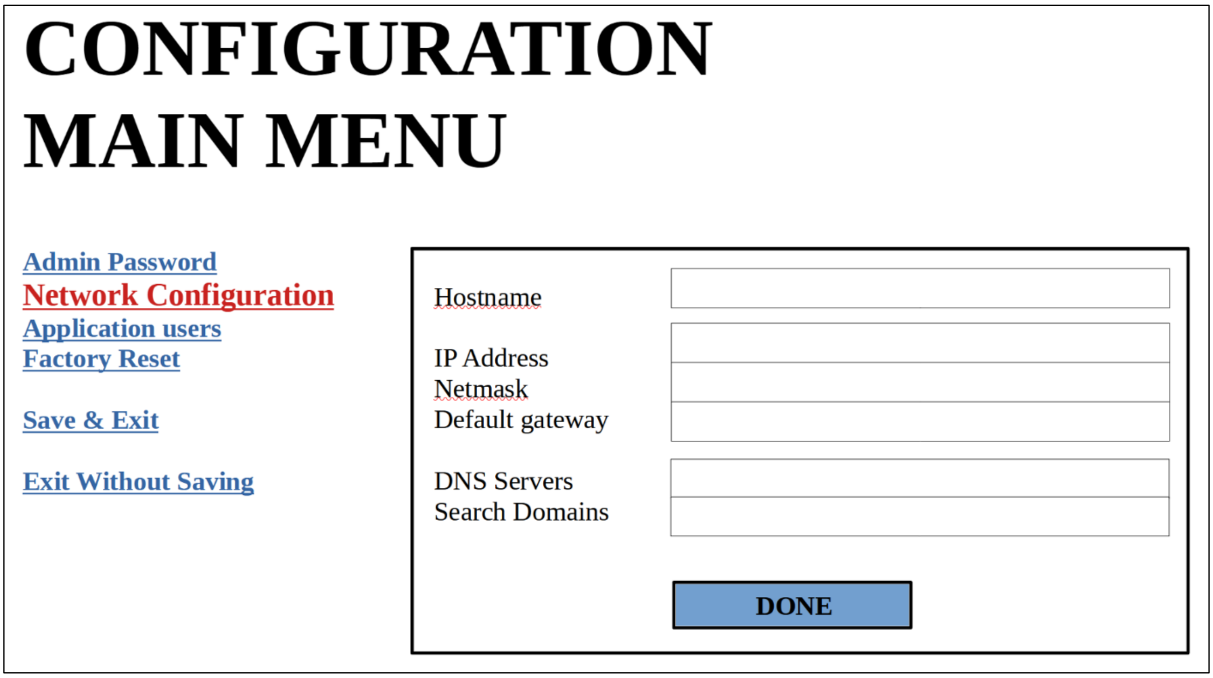
Network Configuration

Application users

Factory Reset

Save & Exit

Exit Without Saving

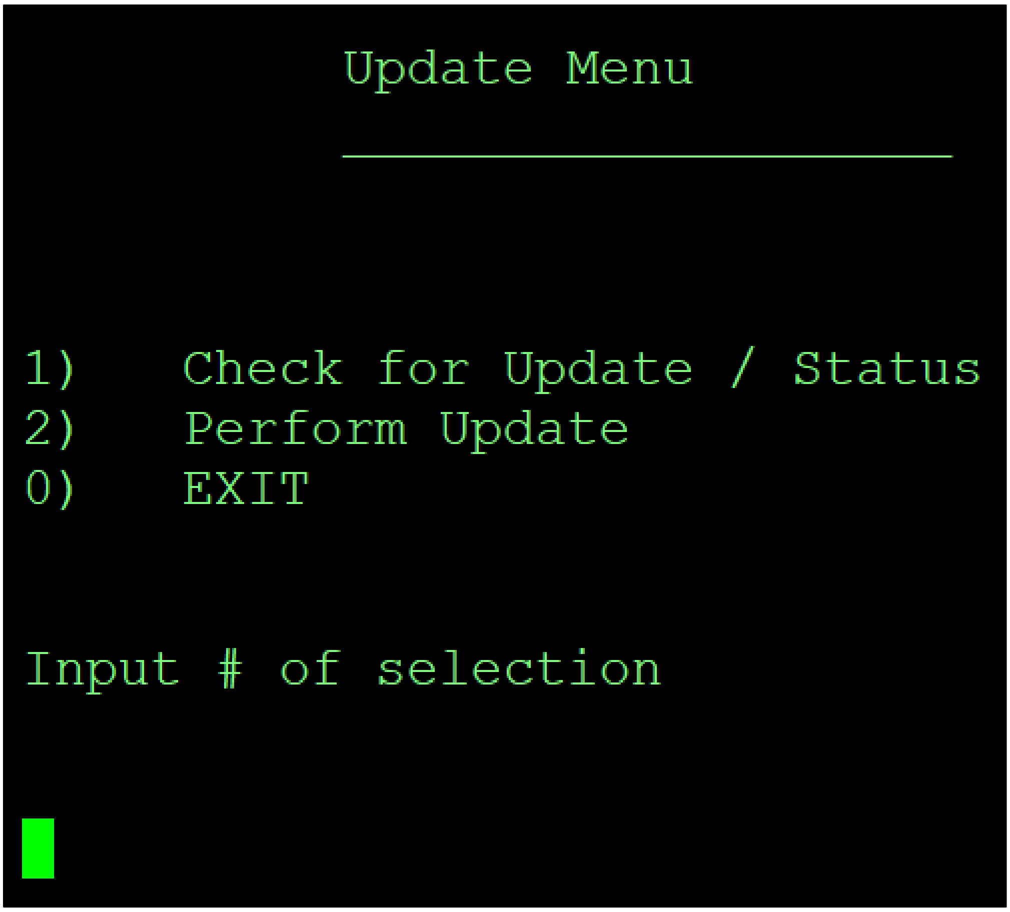


CONFIGURATION
MAIN MENU

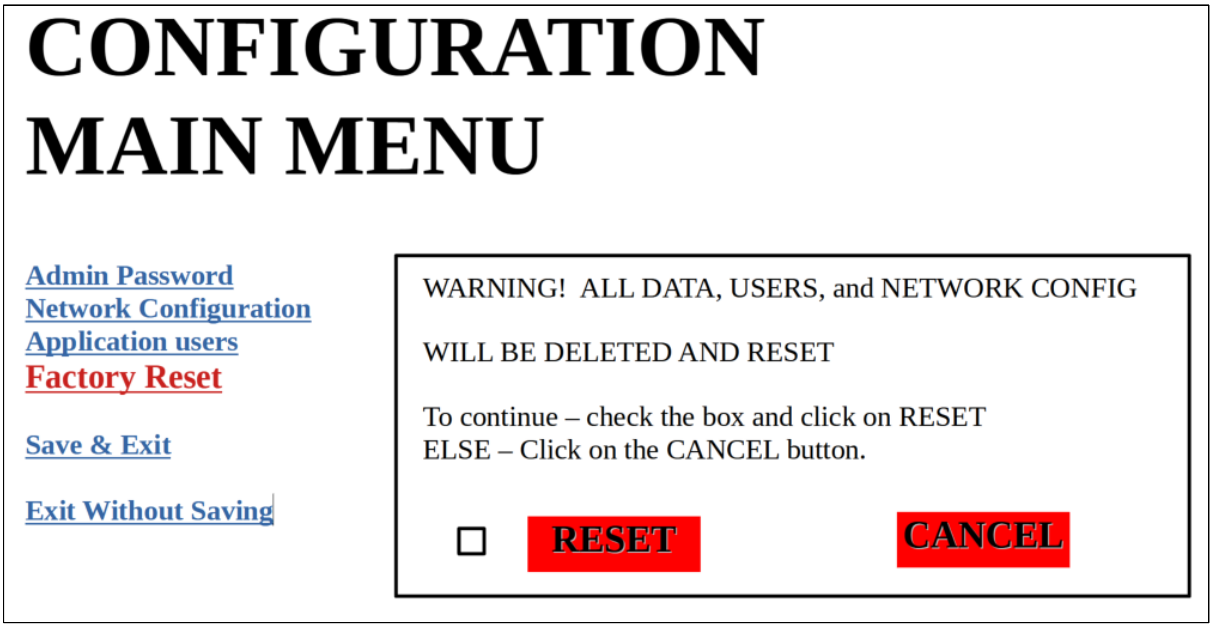
- Admin Password
- **Network Configuration**
- Application users
- Factory Reset
- Save & Exit
- Exit Without Saving

Hostname	
IP Address	
Netmask	
Default gateway	
DNS Servers	
Search Domains	

DONE



```
            Update Menu
            ____________________

1)    Check for Update / Status
2)    Perform Update
0)    EXIT

Input # of selection

█
```

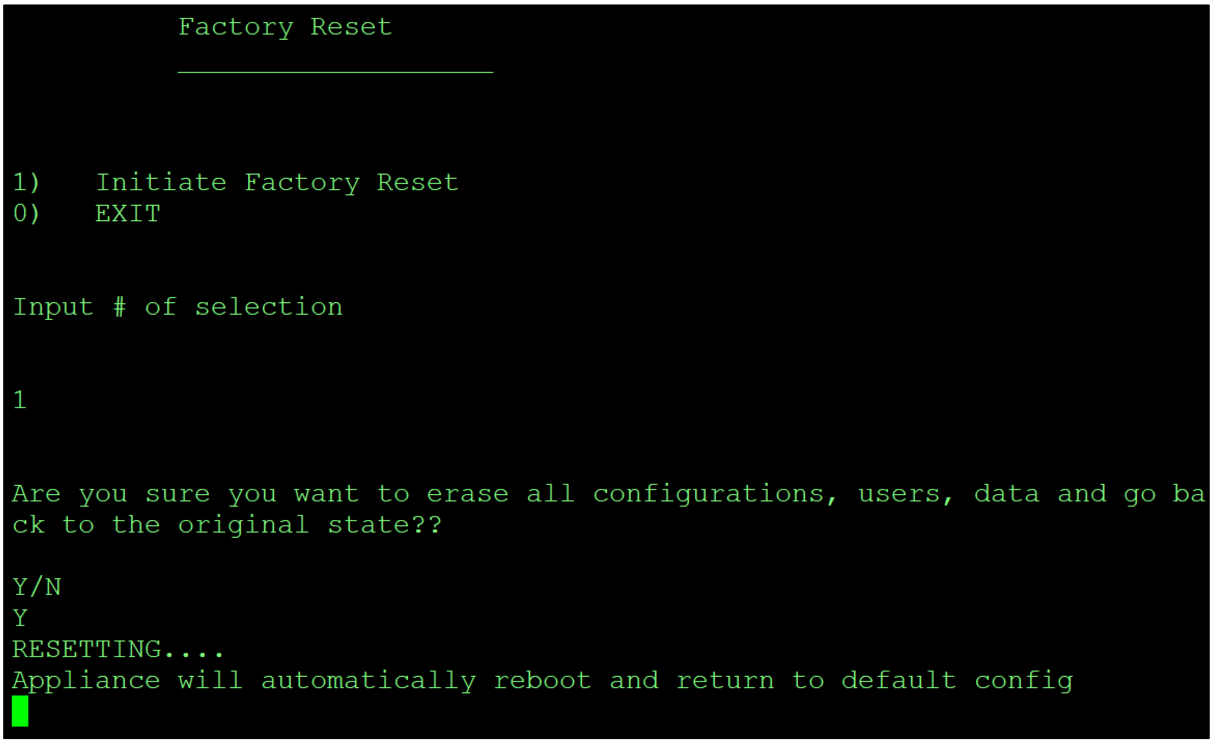


CONFIGURATION MAIN MENU

WARNING! ALL DATA, USERS, and NETWORK CONFIG

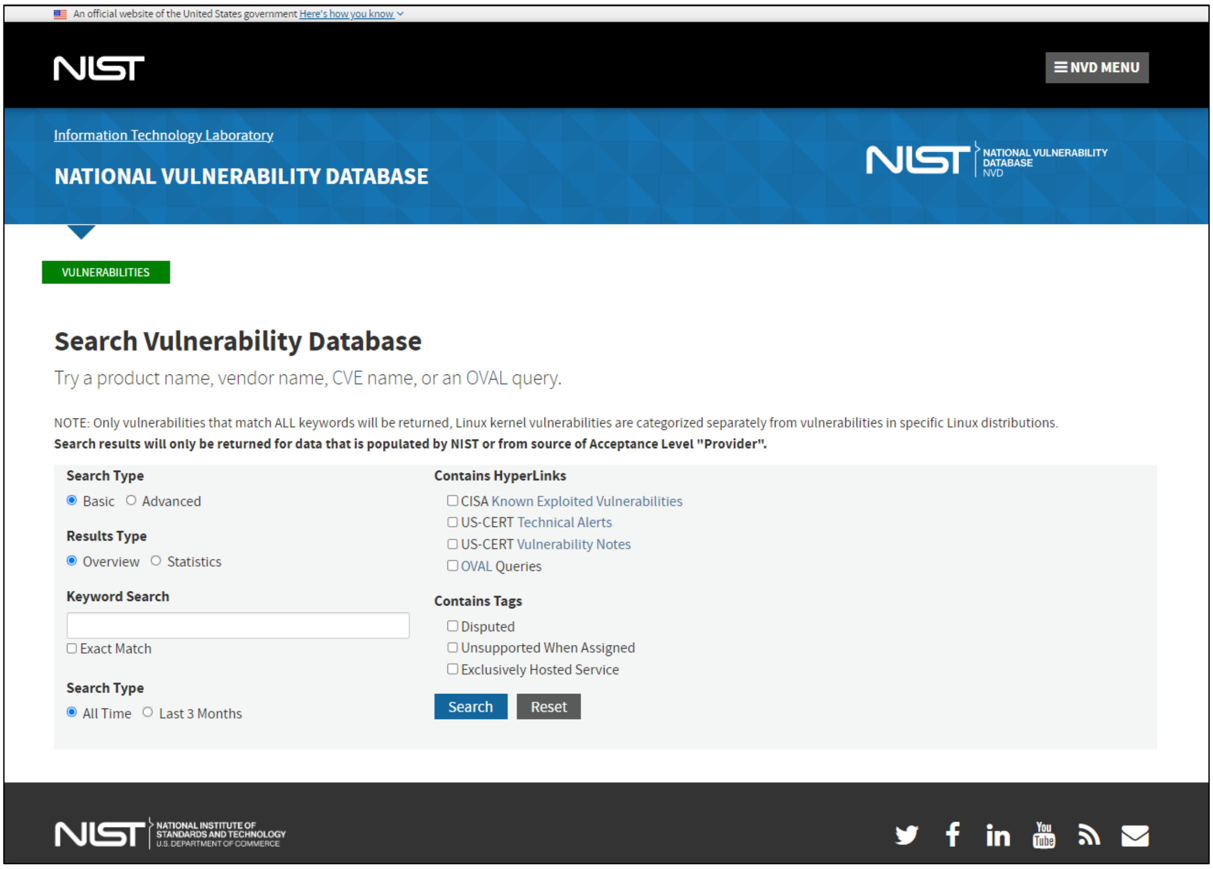
WILL BE DELETED AND RESET

To continue – check the box and click on RESET
ELSE – Click on the CANCEL button.



```
          Factory Reset
          ___________________



1)    Initiate Factory Reset
0)    EXIT


Input # of selection


1


Are you sure you want to erase all configurations, users, data and go ba
ck to the original state??

Y/N
Y
RESETTING....
Appliance will automatically reboot and return to default config
```

Chapter 11: Knowing the Threat Landscape – Staying Informed



An official website of the United States government Here's how you know
NIST
NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.
Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type
● Basic ○ Advanced

Results Type
● Overview ○ Statistics

Keyword Search

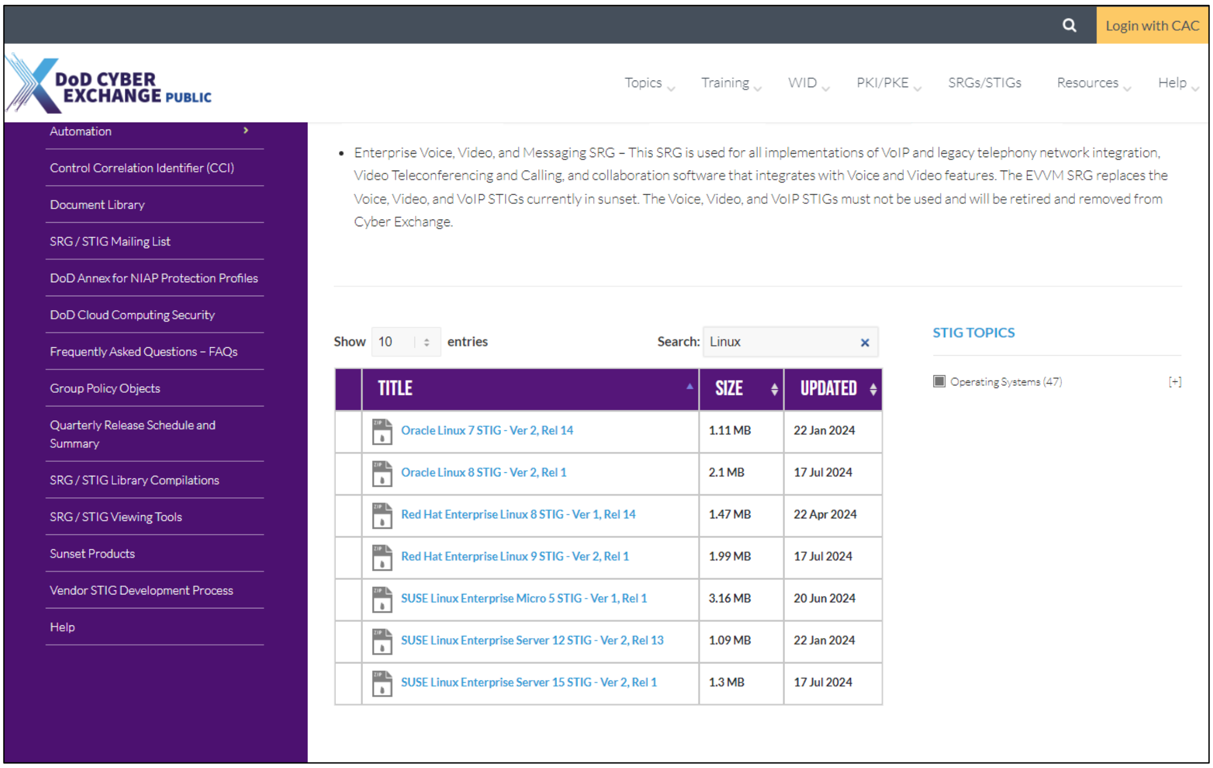
□ Exact Match

Search Type
● All Time ○ Last 3 Months

Contains HyperLinks
□ CISA Known Exploited Vulnerabilities
□ US-CERT Technical Alerts
□ US-CERT Vulnerability Notes
□ OVAL Queries

Contains Tags
□ Disputed
□ Unsupported When Assigned
□ Exclusively Hosted Service

Search
Reset
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



Login with CAC
DoD CYBER EXCHANGE PUBLIC
Topics
Training
WID
PKI/PKE
SRGs/STIGs
Resources
Help
Automation
Control Correlation Identifier (CCI)
Document Library
SRG / STIG Mailing List
DoD Annex for NIAP Protection Profiles
DoD Cloud Computing Security
Frequently Asked Questions – FAQs
Group Policy Objects
Quarterly Release Schedule and Summary
SRG / STIG Library Compilations
SRG / STIG Viewing Tools
Sunset Products
Vendor STIG Development Process
Help

- Enterprise Voice, Video, and Messaging SRG – This SRG is used for all implementations of VoIP and legacy telephony network integration, Video Teleconferencing and Calling, and collaboration software that integrates with Voice and Video features. The EVVM SRG replaces the Voice, Video, and VoIP STIGs currently in sunset. The Voice, Video, and VoIP STIGs must not be used and will be retired and removed from Cyber Exchange.

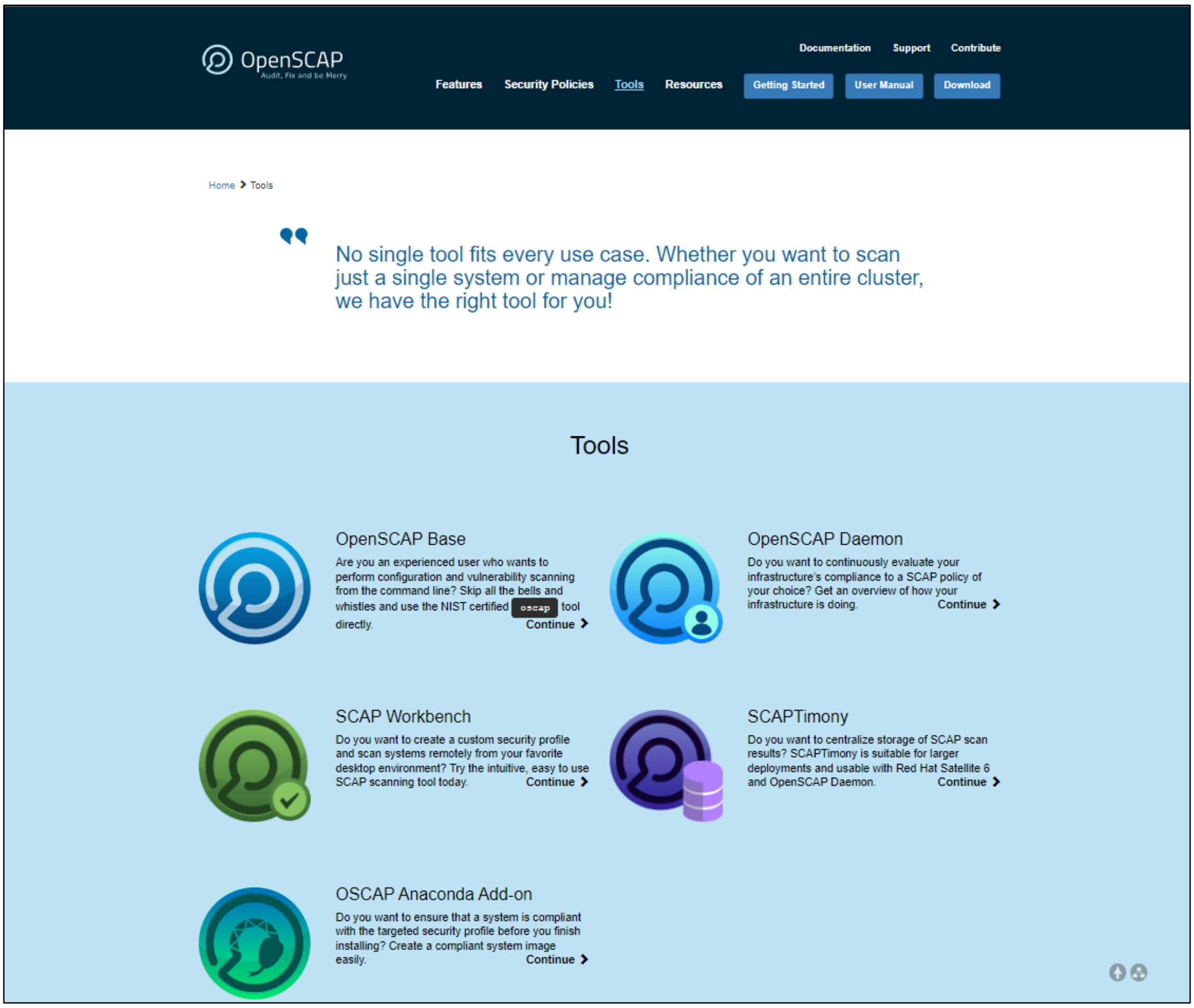
Show 10 entries

Search: Linux

TITLE	SIZE	UPDATED
Oracle Linux 7 STIG - Ver 2, Rel 14	1.11 MB	22 Jan 2024
Oracle Linux 8 STIG - Ver 2, Rel 1	2.1 MB	17 Jul 2024
Red Hat Enterprise Linux 8 STIG - Ver 1, Rel 14	1.47 MB	22 Apr 2024
Red Hat Enterprise Linux 9 STIG - Ver 2, Rel 1	1.99 MB	17 Jul 2024
SUSE Linux Enterprise Micro 5 STIG - Ver 1, Rel 1	3.16 MB	20 Jun 2024
SUSE Linux Enterprise Server 12 STIG - Ver 2, Rel 13	1.09 MB	22 Jan 2024
SUSE Linux Enterprise Server 15 STIG - Ver 2, Rel 1	1.3 MB	17 Jul 2024

STIG TOPICS

▨ Operating Systems (47) [+]



> No single tool fits every use case. Whether you want to scan just a single system or manage compliance of an entire cluster, we have the right tool for you!

Tools

OpenSCAP Base

Are you an experienced user who wants to perform configuration and vulnerability scanning from the command line? Skip all the bells and whistles and use the NIST certified `oscap` tool directly.

Continue >

OpenSCAP Daemon

Do you want to continuously evaluate your infrastructure's compliance to a SCAP policy of your choice? Get an overview of how your infrastructure is doing.

Continue >

SCAP Workbench

Do you want to create a custom security profile and scan systems remotely from your favorite desktop environment? Try the intuitive, easy to use SCAP scanning tool today.

Continue >

SCAPTimony

Do you want to centralize storage of SCAP scan results? SCAPTimony is suitable for larger deployments and usable with Red Hat Satellite 6 and OpenSCAP Daemon.

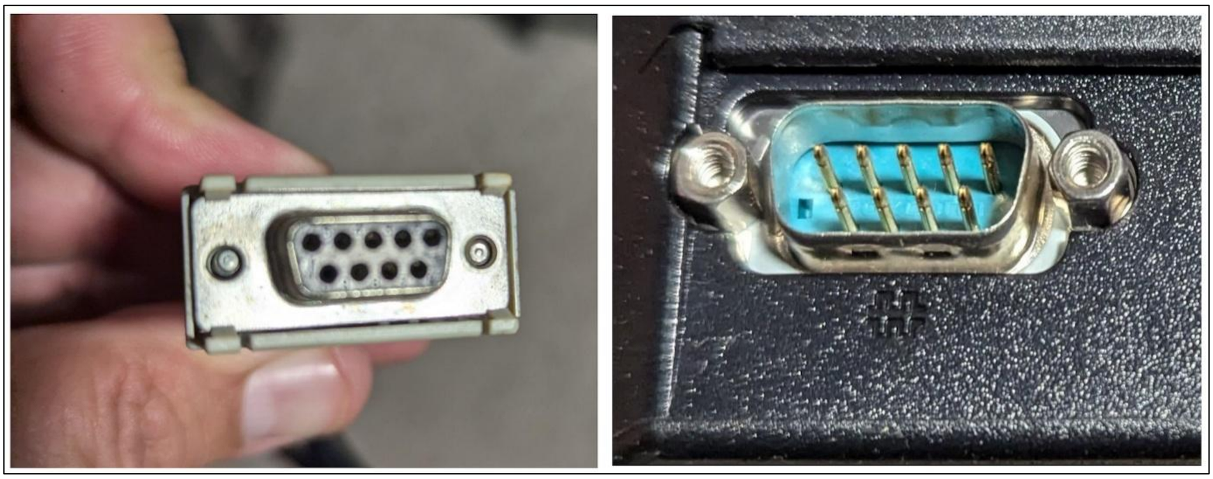
Continue >

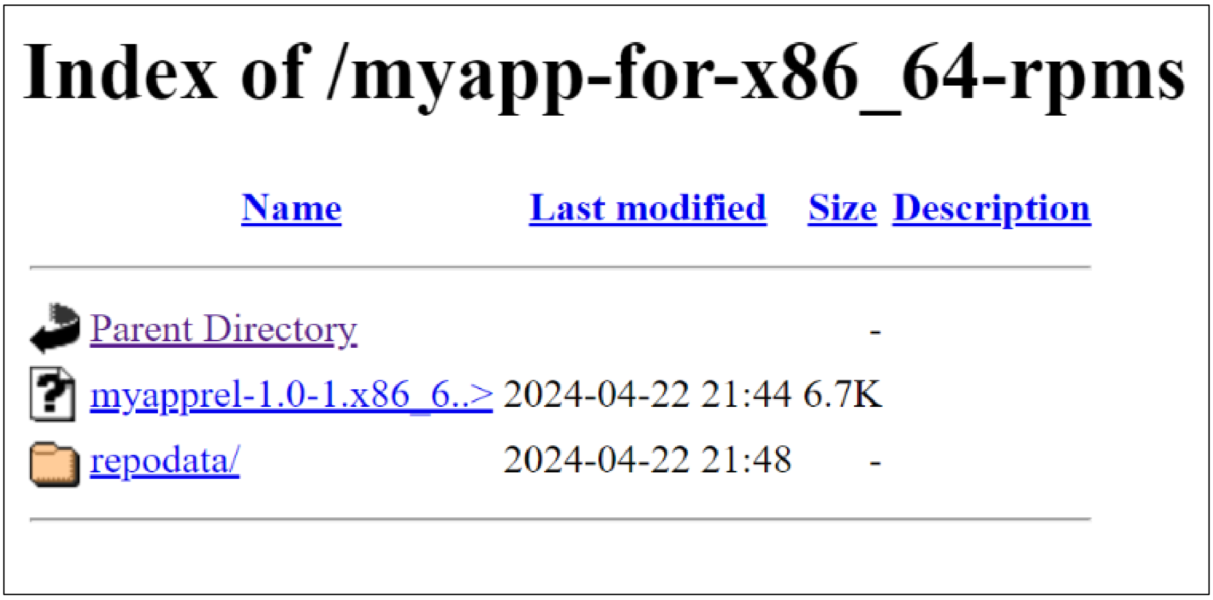
OSCAP Anaconda Add-on

Do you want to ensure that a system is compliant with the targeted security profile before you finish installing? Create a compliant system image easily.

Continue >

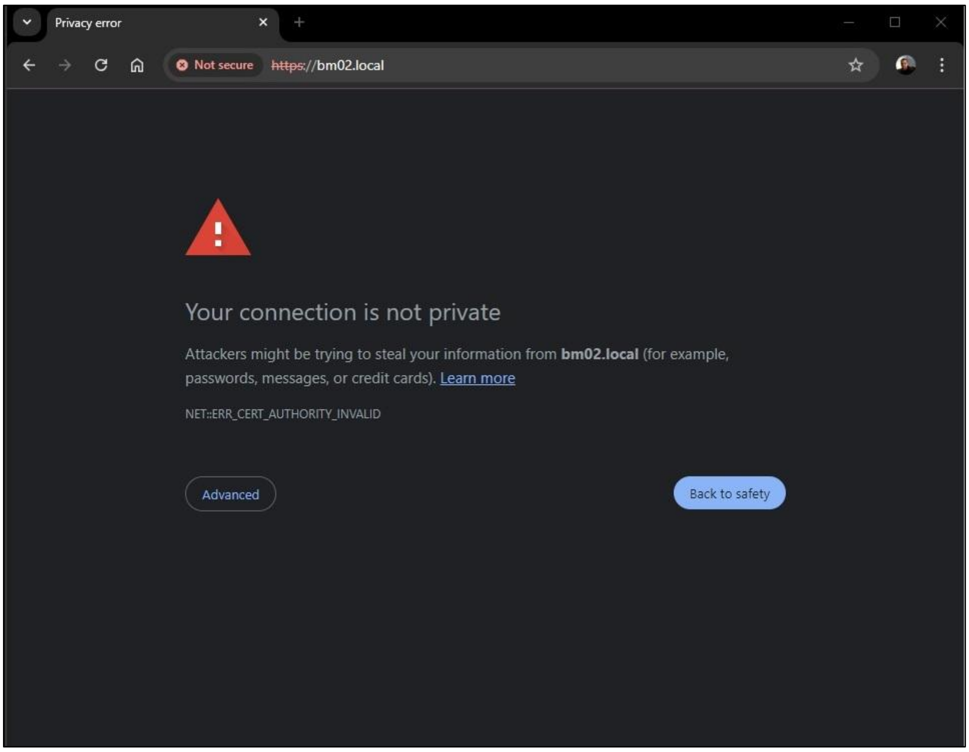
Chapter 12: Are My Devices' Communications and Interactions Secure?





Index of /myapp-for-x86_64-rpms

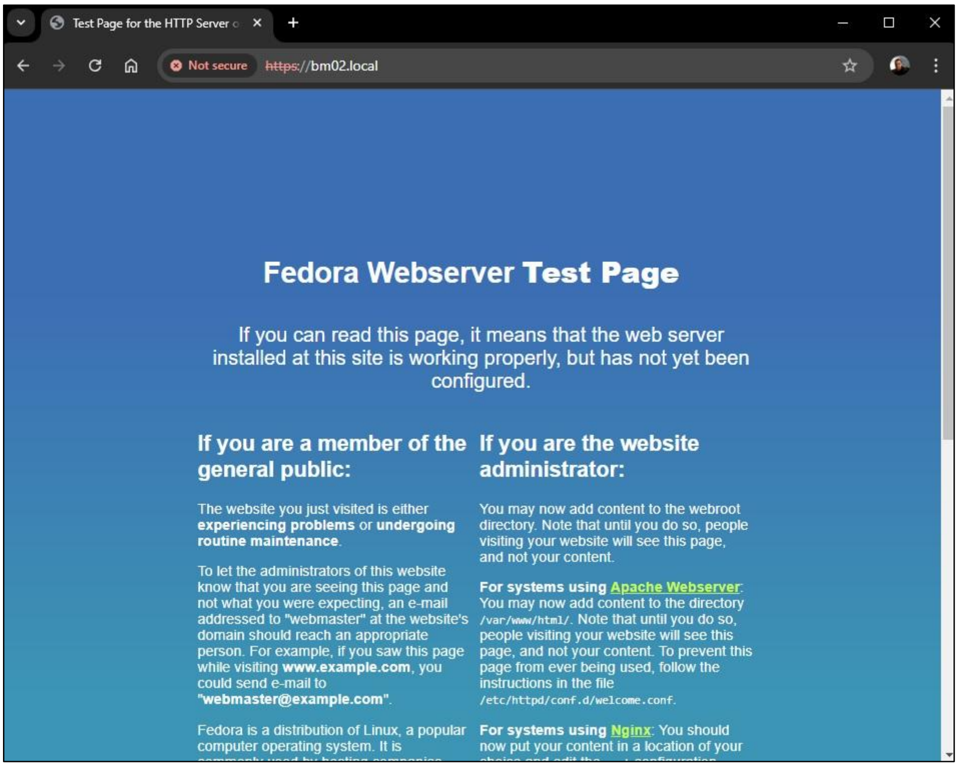
Name	Last modified	Size	Description
Parent Directory		-	
myapprel-1.0-1.x86_6..>	2024-04-22 21:44	6.7K	
repodata/	2024-04-22 21:48	-	



Your connection is not private

Attackers might be trying to steal your information from **bm02.local** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID



Fedora Webserver Test Page

If you can read this page, it means that the web server installed at this site is working properly, but has not yet been configured.

If you are a member of the general public:

The website you just visited is either **experiencing problems** or **undergoing routine maintenance**.

To let the administrators of this website know that you are seeing this page and not what you were expecting, an e-mail addressed to "webmaster" at the website's domain should reach an appropriate person. For example, if you saw this page while visiting **www.example.com**, you could send e-mail to **"webmaster@example.com"**.

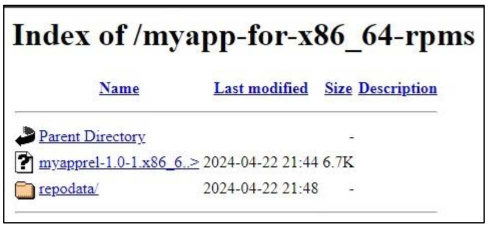
Fedora is a distribution of Linux, a popular computer operating system. It is

If you are the website administrator:

You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

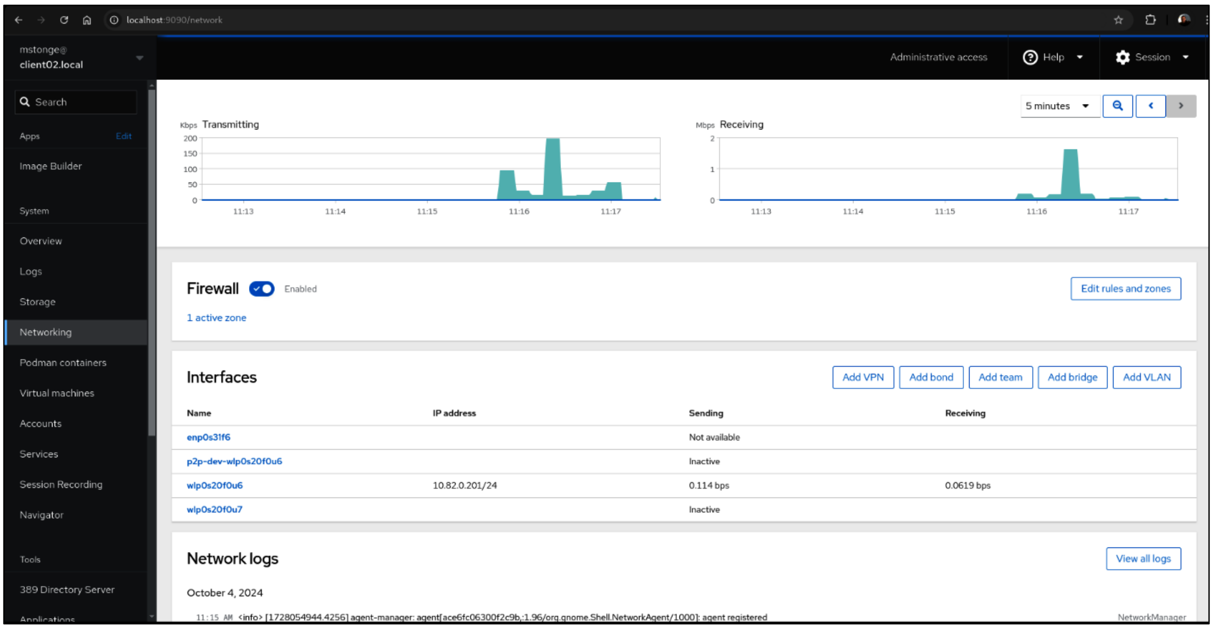
For systems using Apache Webserver: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using Nginx: You should now put your content in a location of your



Index of /myapp-for-x86_64-rpms

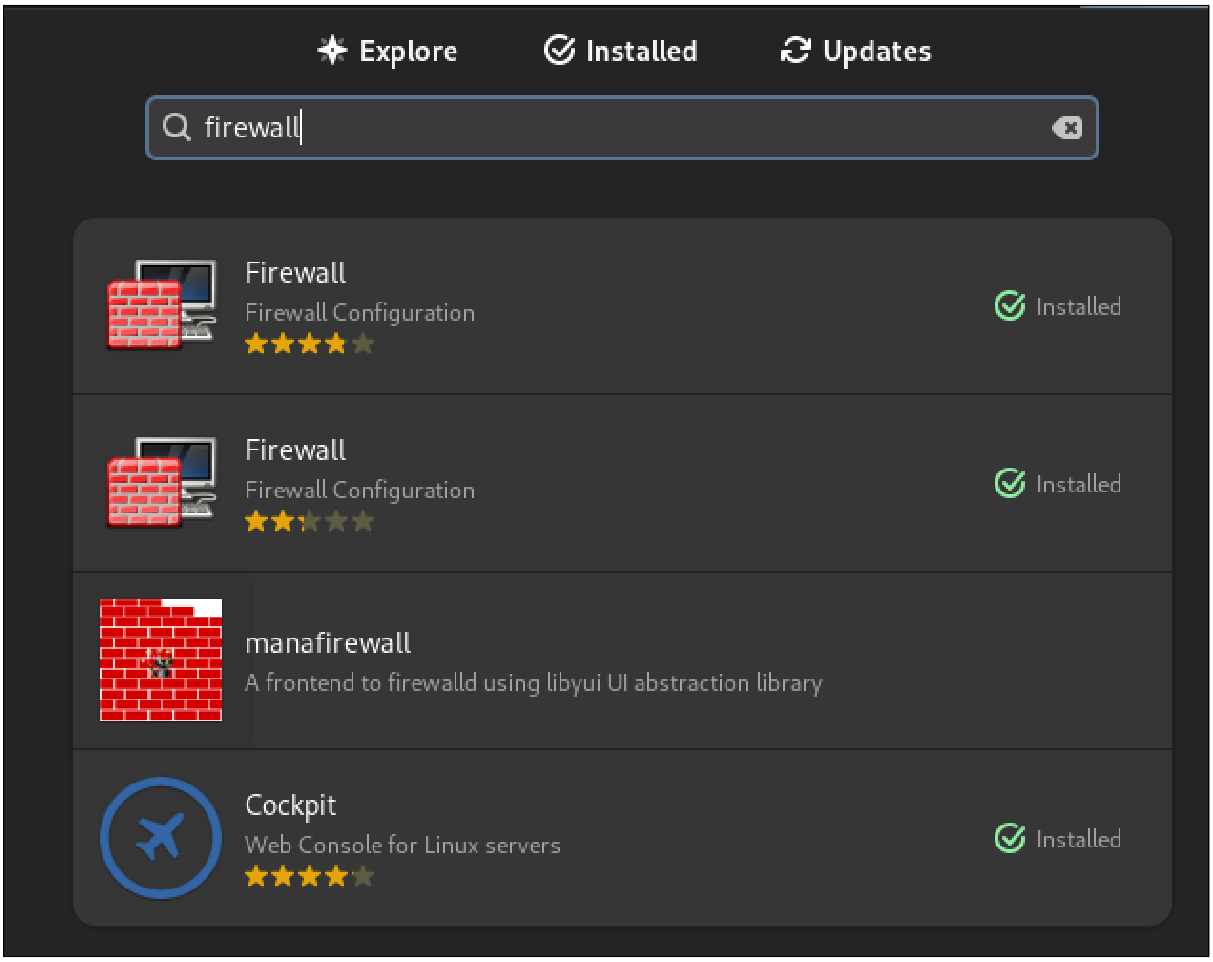
Name	Last modified	Size	Description
Parent Directory		-	
myapprel-1.0-1.x86_6..>	2024-04-22 21:44	6.7K	
repodata/	2024-04-22 21:48	-	



Name	IP address	Sending	Receiving
enp0s31f6		Not available	
p2p-dev-wlp0s20f0u6		Inactive	
wlp0s20f0u6	10.82.0.201/24	0.114 bps	0.0619 bps
wlp0s20f0u7		Inactive	

October 4, 2024

```
11:15 AM <info> [1728054944.4256] agent-manager: agent[ace6fc06300f2c9b,:1.96/org.gnome.Shell.NetworkAgent/1000]: agent registered        NetworkManager
```



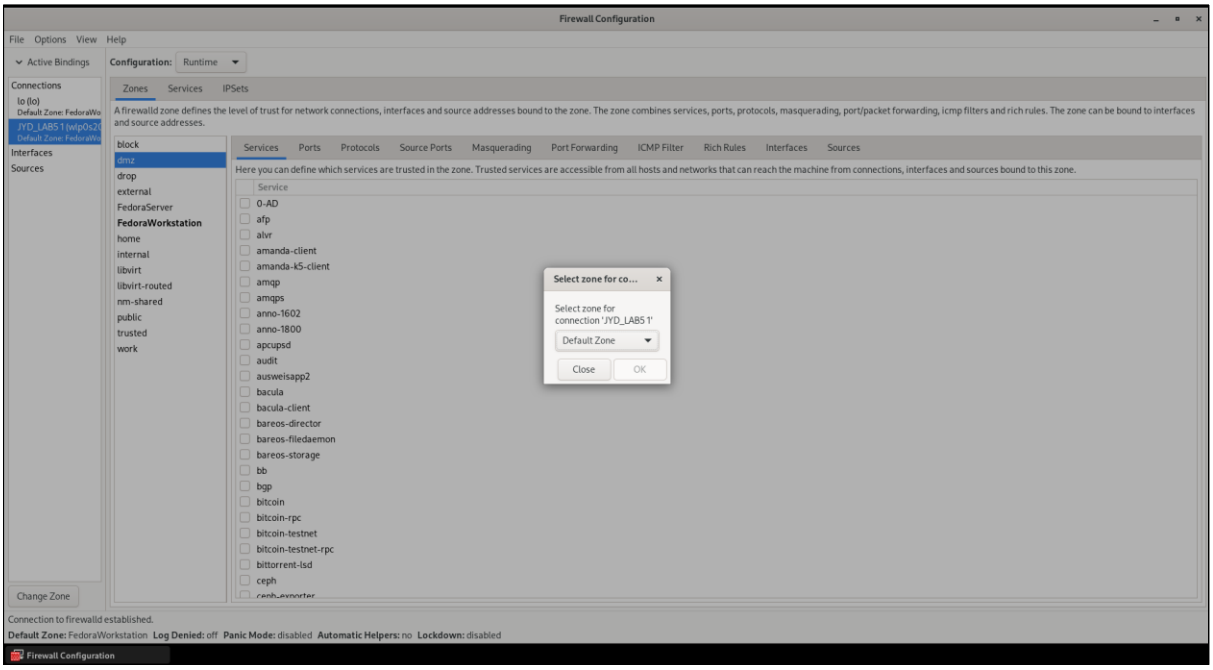
firewall

Firewall
Firewall Configuration
★★★★☆
Installed

Firewall
Firewall Configuration
★★½☆☆
Installed

manafirewall
A frontend to firewalld using libyui UI abstraction library

Cockpit
Web Console for Linux servers
★★★★☆
Installed



Configuration: Runtime

lo (lo)
Default Zone: FedoraWo

JYD_LAB5 1 (wlp0s2(
Default Zone: FedoraWo

A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, icmp filters and rich rules. The zone can be bound to interfaces and source addresses.

block
dmz
drop
external
FedoraServer
FedoraWorkstation
home
internal
libvirt
libvirt-routed
nm-shared
public
trusted
work

Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone.

Service

□ 0-AD
□ afp
□ alvr
□ amanda-client
□ amanda-k5-client
□ amqp
□ amqps
□ anno-1602
□ anno-1800
□ apcupsd
□ audit
□ ausweisapp2
□ bacula
□ bacula-client
□ bareos-director
□ bareos-filedaemon
□ bareos-storage
□ bb
□ bgp
□ bitcoin
□ bitcoin-rpc
□ bitcoin-testnet
□ bitcoin-testnet-rpc
□ bittorrent-lsd
□ ceph
□ ceph-exporter

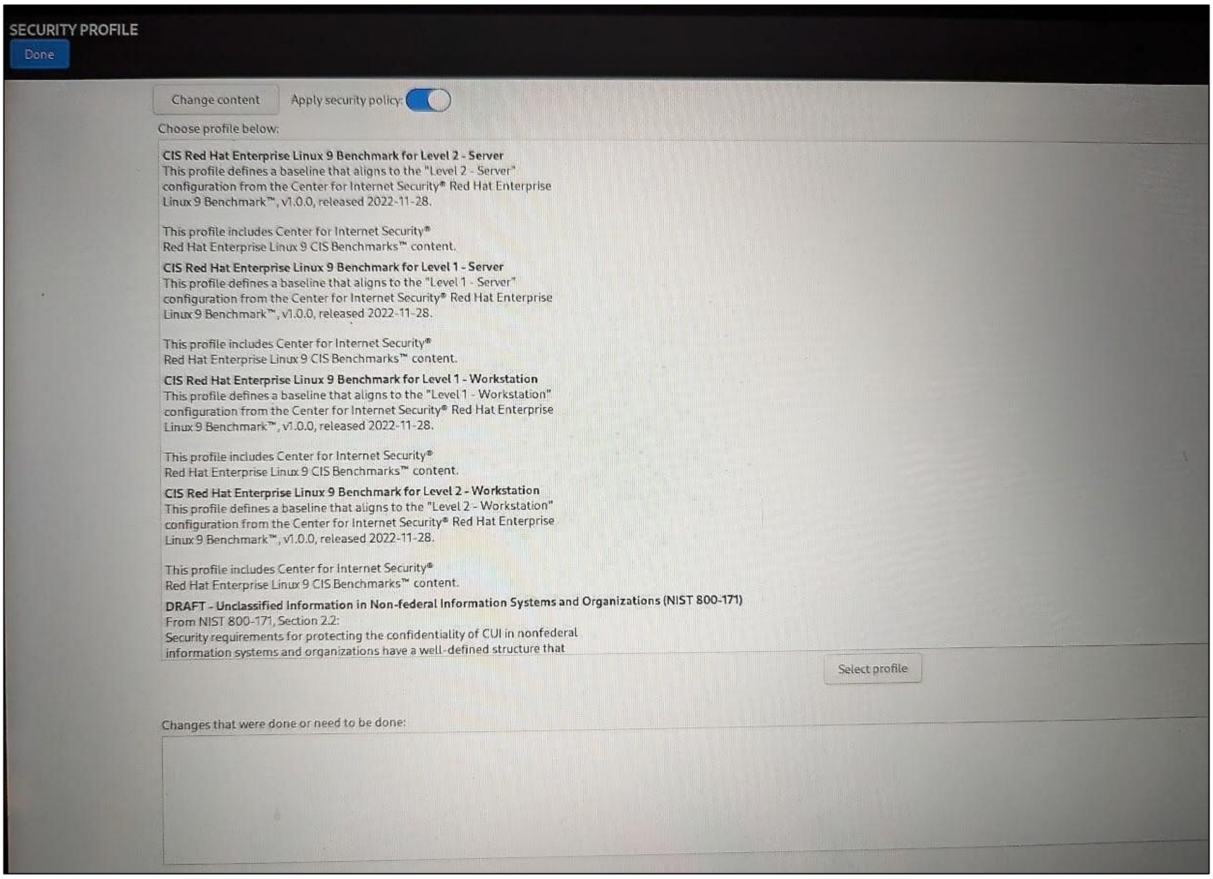
Select zone for connection 'JYD_LAB5 1'

Default Zone

Connection to firewalld established.

Default Zone: FedoraWorkstation **Log Denied:** off **Panic Mode:** disabled **Automatic Helpers:** no **Lockdown:** disabled

Chapter 13: Applying Government Security Standards – System Hardening



SECURITY PROFILE

Done

Change content   Apply security policy:

Choose profile below:

CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Server
This profile defines a baseline that aligns to the "Level 2 - Server" configuration from the Center for Internet Security® Red Hat Enterprise Linux 9 Benchmark™, v1.0.0, released 2022-11-28.

This profile includes Center for Internet Security® Red Hat Enterprise Linux 9 CIS Benchmarks™ content.

CIS Red Hat Enterprise Linux 9 Benchmark for Level 1 - Server
This profile defines a baseline that aligns to the "Level 1 - Server" configuration from the Center for Internet Security® Red Hat Enterprise Linux 9 Benchmark™, v1.0.0, released 2022-11-28.

This profile includes Center for Internet Security® Red Hat Enterprise Linux 9 CIS Benchmarks™ content.

CIS Red Hat Enterprise Linux 9 Benchmark for Level 1 - Workstation
This profile defines a baseline that aligns to the "Level 1 - Workstation" configuration from the Center for Internet Security® Red Hat Enterprise Linux 9 Benchmark™, v1.0.0, released 2022-11-28.

This profile includes Center for Internet Security® Red Hat Enterprise Linux 9 CIS Benchmarks™ content.

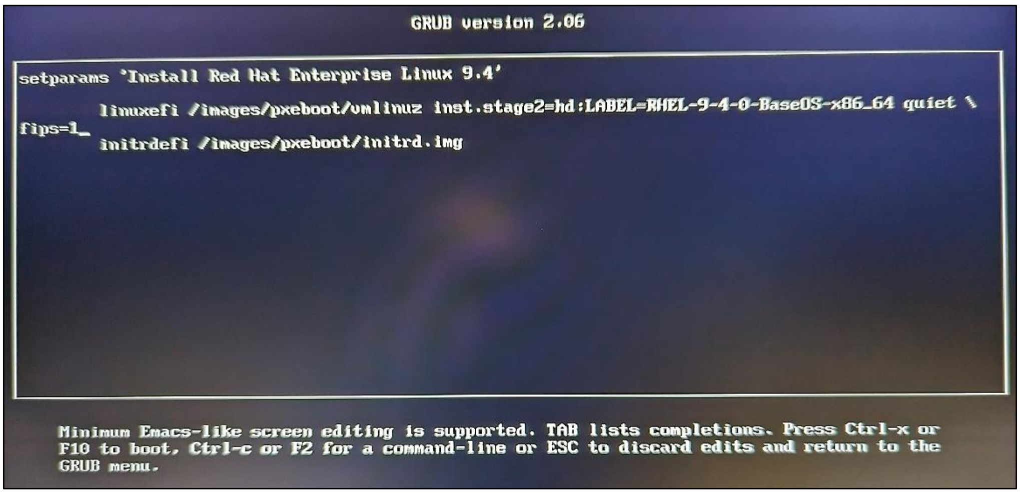
CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Workstation
This profile defines a baseline that aligns to the "Level 2 - Workstation" configuration from the Center for Internet Security® Red Hat Enterprise Linux 9 Benchmark™, v1.0.0, released 2022-11-28.

This profile includes Center for Internet Security® Red Hat Enterprise Linux 9 CIS Benchmarks™ content.

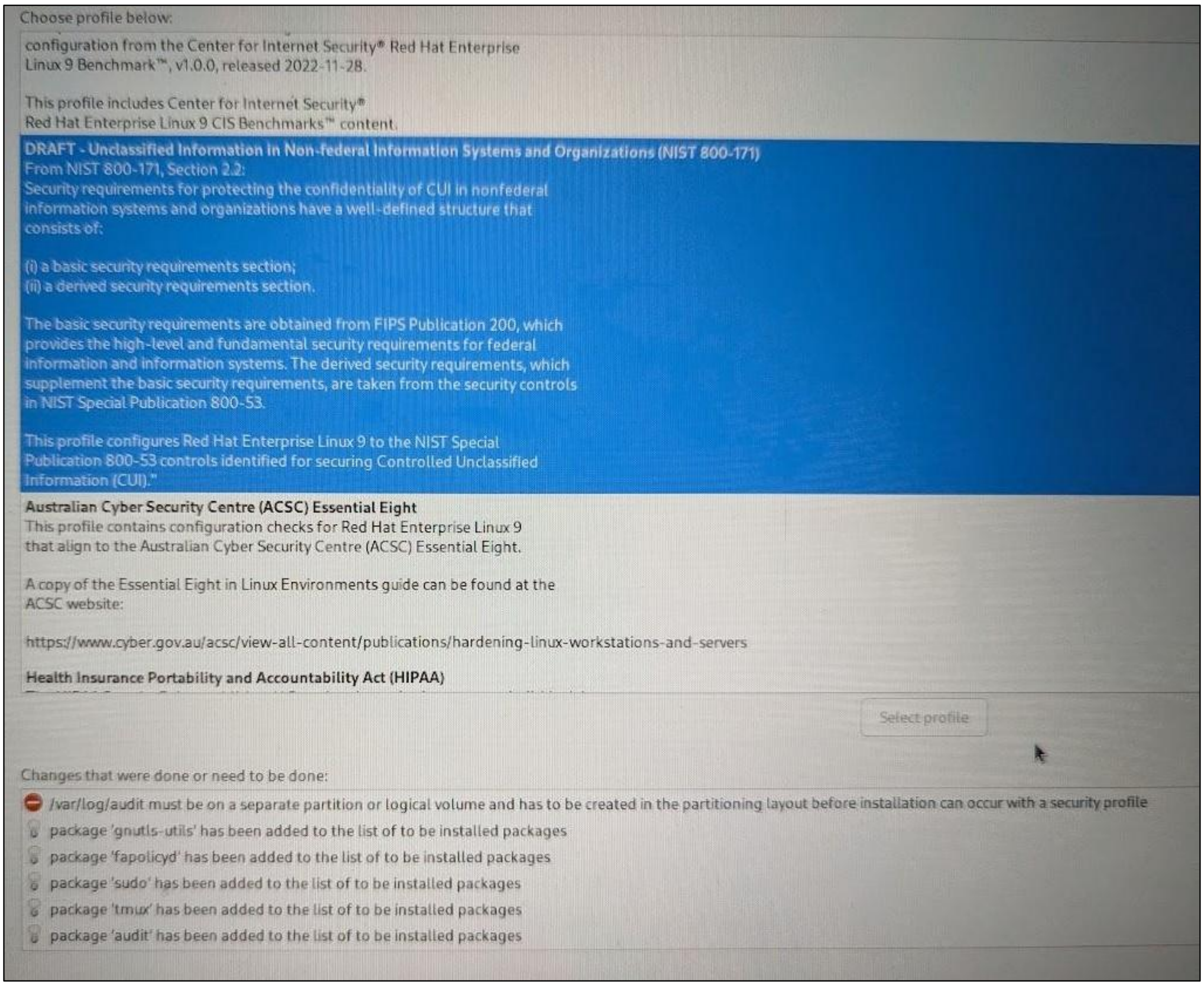
DRAFT - Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
From NIST 800-171, Section 2.2:
Security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations have a well-defined structure that

Select profile

Changes that were done or need to be done:



```
                        GRUB version 2.06

setparams 'Install Red Hat Enterprise Linux 9.4'
        linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=RHEL-9-4-0-BaseOS-x86_64 quiet \
fips=1_
        initrdefi /images/pxeboot/initrd.img

    Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or
    F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the
    GRUB menu.
```



Choose profile below:

configuration from the Center for Internet Security® Red Hat Enterprise Linux 9 Benchmark™, v1.0.0, released 2022-11-28.

This profile includes Center for Internet Security® Red Hat Enterprise Linux 9 CIS Benchmarks™ content.

DRAFT - Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
From NIST 800-171, Section 2.2:
Security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations have a well-defined structure that consists of:

(i) a basic security requirements section;
(ii) a derived security requirements section.

The basic security requirements are obtained from FIPS Publication 200, which provides the high-level and fundamental security requirements for federal information and information systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST Special Publication 800-53.

This profile configures Red Hat Enterprise Linux 9 to the NIST Special Publication 800-53 controls identified for securing Controlled Unclassified Information (CUI)."

Australian Cyber Security Centre (ACSC) Essential Eight
This profile contains configuration checks for Red Hat Enterprise Linux 9 that align to the Australian Cyber Security Centre (ACSC) Essential Eight.

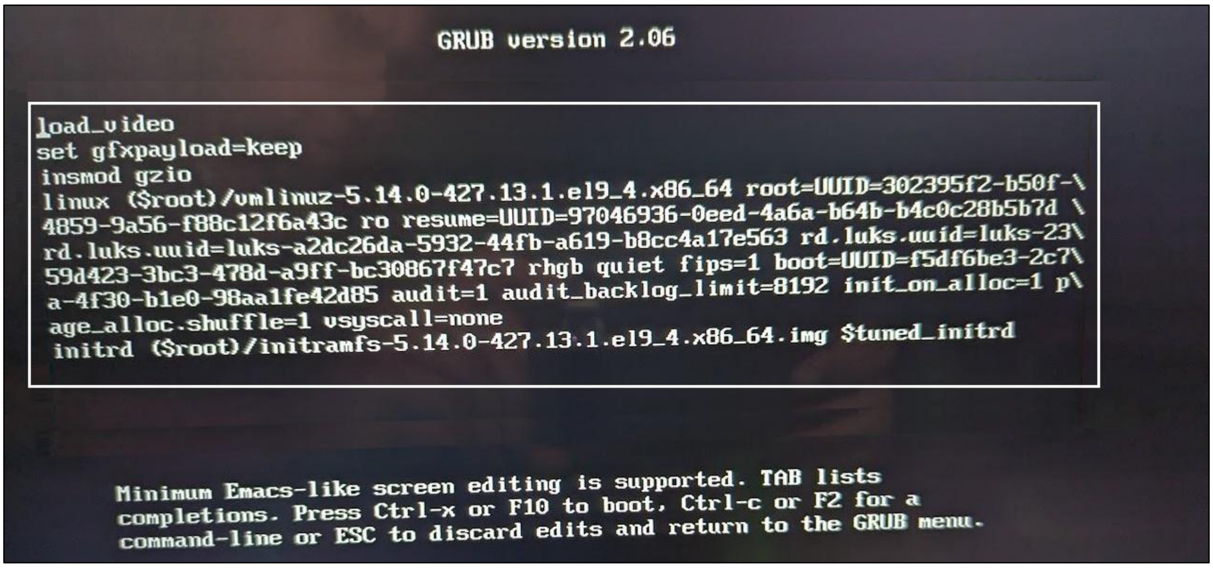
A copy of the Essential Eight in Linux Environments guide can be found at the ACSC website:

https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-linux-workstations-and-servers

Health Insurance Portability and Accountability Act (HIPAA)

Changes that were done or need to be done:

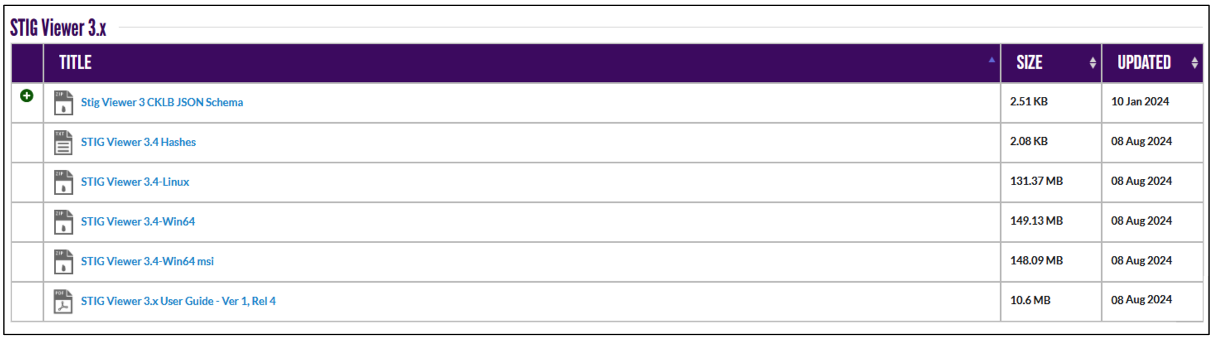
- /var/log/audit must be on a separate partition or logical volume and has to be created in the partitioning layout before installation can occur with a security profile
- package 'gnutls-utils' has been added to the list of to be installed packages
- package 'fapolicyd' has been added to the list of to be installed packages
- package 'sudo' has been added to the list of to be installed packages
- package 'tmux' has been added to the list of to be installed packages
- package 'audit' has been added to the list of to be installed packages



GRUB version 2.06

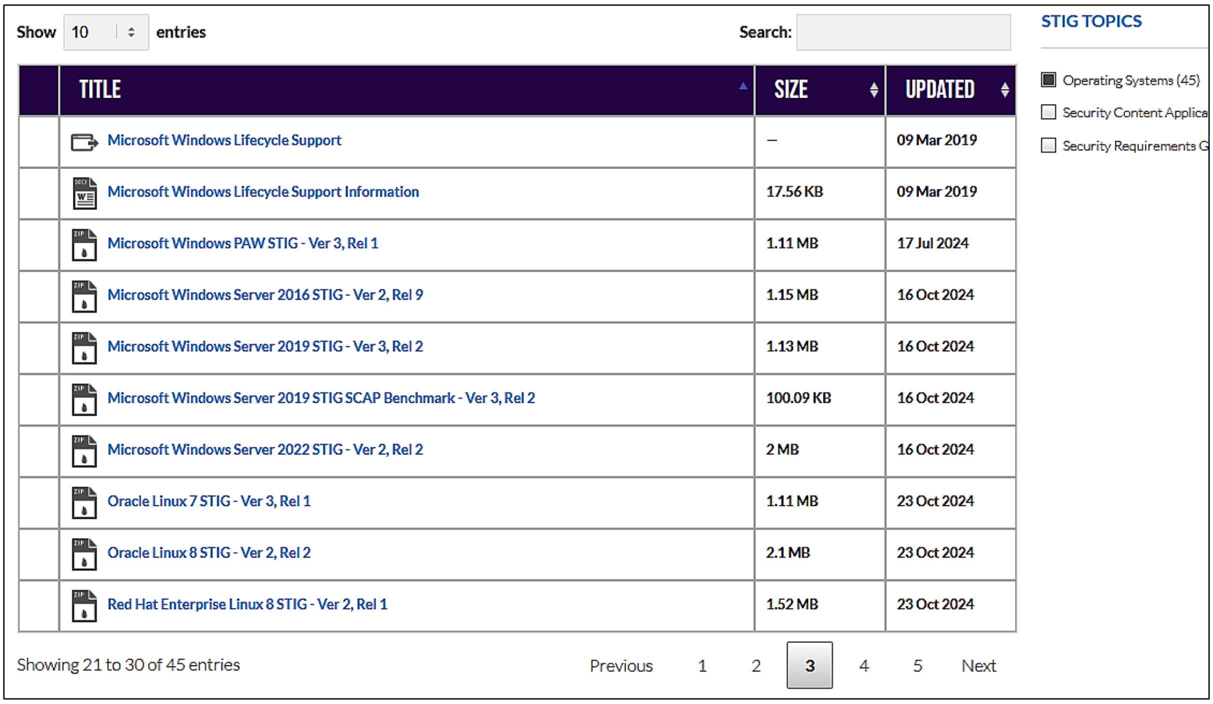
```
load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-5.14.0-427.13.1.el9_4.x86_64 root=UUID=302395f2-b50f-\
4859-9a56-f88c12f6a43c ro resume=UUID=97046936-0eed-4a6a-b64b-b4c0c28b5b7d \
rd.luks.uuid=luks-a2dc26da-5932-44fb-a619-b8cc4a17e563 rd.luks.uuid=luks-23\
59d423-3bc3-478d-a9ff-bc30867f47c7 rhgb quiet fips=1 boot=UUID=f5df6be3-2c7\
a-4f30-b1e0-98aa1fe42d85 audit=1 audit_backlog_limit=8192 init_on_alloc=1 p\
age_alloc.shuffle=1 vsyscall=none
initrd ($root)/initramfs-5.14.0-427.13.1.el9_4.x86_64.img $tuned_initrd
```

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.



STIG Viewer 3.x

	TITLE	SIZE	UPDATED
⊕	Stig Viewer 3 CKLB JSON Schema	2.51 KB	10 Jan 2024
	STIG Viewer 3.4 Hashes	2.08 KB	08 Aug 2024
	STIG Viewer 3.4-Linux	131.37 MB	08 Aug 2024
	STIG Viewer 3.4-Win64	149.13 MB	08 Aug 2024
	STIG Viewer 3.4-Win64 msi	148.09 MB	08 Aug 2024
	STIG Viewer 3.x User Guide - Ver 1, Rel 4	10.6 MB	08 Aug 2024



Show 10 entries

Search:

	TITLE	SIZE	UPDATED
	Microsoft Windows Lifecycle Support	–	09 Mar 2019
	Microsoft Windows Lifecycle Support Information	17.56 KB	09 Mar 2019
	Microsoft Windows PAW STIG - Ver 3, Rel 1	1.11 MB	17 Jul 2024
	Microsoft Windows Server 2016 STIG - Ver 2, Rel 9	1.15 MB	16 Oct 2024
	Microsoft Windows Server 2019 STIG - Ver 3, Rel 2	1.13 MB	16 Oct 2024
	Microsoft Windows Server 2019 STIG SCAP Benchmark - Ver 3, Rel 2	100.09 KB	16 Oct 2024
	Microsoft Windows Server 2022 STIG - Ver 2, Rel 2	2 MB	16 Oct 2024
	Oracle Linux 7 STIG - Ver 3, Rel 1	1.11 MB	23 Oct 2024
	Oracle Linux 8 STIG - Ver 2, Rel 2	2.1 MB	23 Oct 2024
	Red Hat Enterprise Linux 8 STIG - Ver 2, Rel 1	1.52 MB	23 Oct 2024

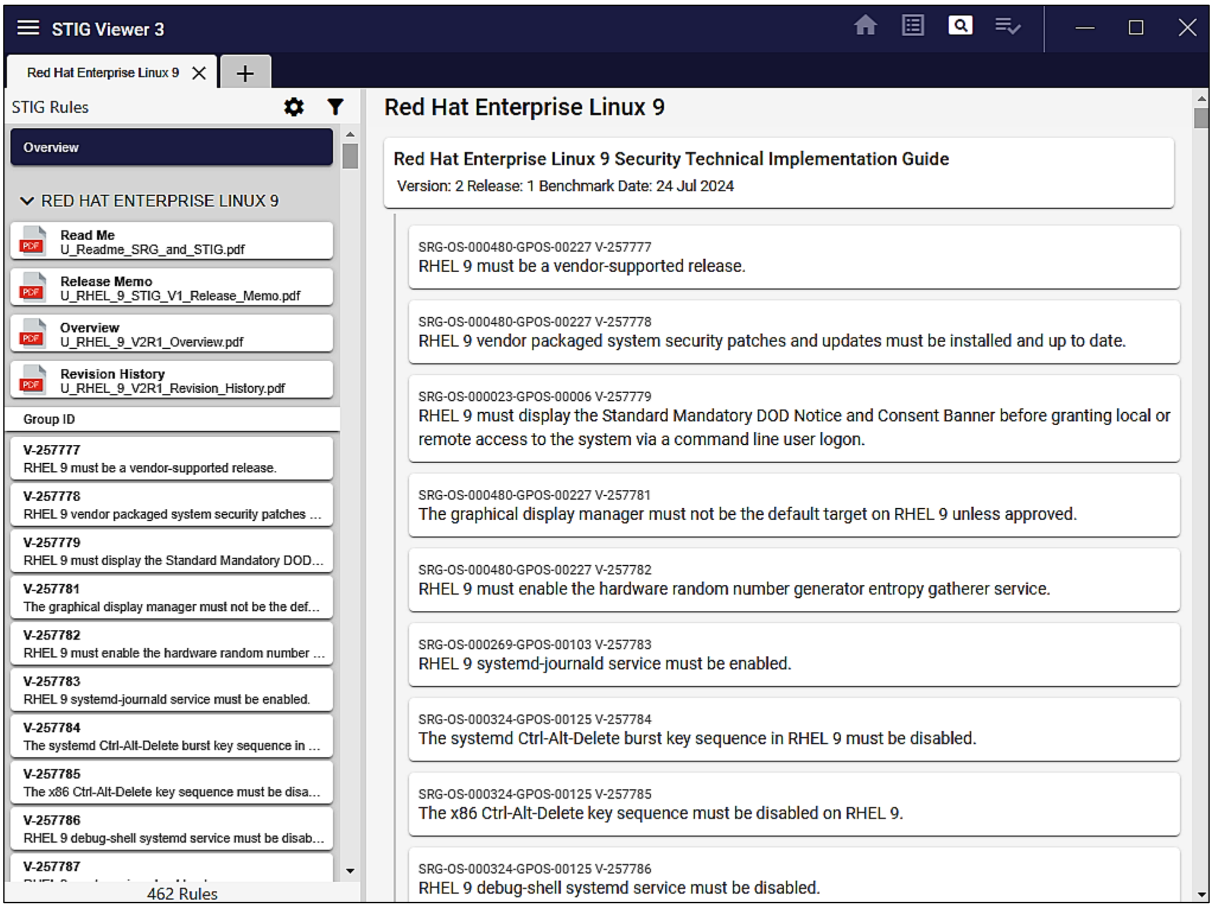
Showing 21 to 30 of 45 entries

STIG TOPICS

☒ Operating Systems (45)

☐ Security Content Applica

☐ Security Requirements G



RED HAT ENTERPRISE LINUX 9

Read Me
U_Readme_SRG_and_STIG.pdf

Release Memo
U_RHEL_9_STIG_V1_Release_Memo.pdf

Overview
U_RHEL_9_V2R1_Overview.pdf

Revision History
U_RHEL_9_V2R1_Revision_History.pdf

Group ID

V-257777
RHEL 9 must be a vendor-supported release.

V-257778
RHEL 9 vendor packaged system security patches ...

V-257779
RHEL 9 must display the Standard Mandatory DOD...

V-257781
The graphical display manager must not be the def...

V-257782
RHEL 9 must enable the hardware random number ...

V-257783
RHEL 9 systemd-journald service must be enabled.

V-257784
The systemd Ctrl-Alt-Delete burst key sequence in ...

V-257785
The x86 Ctrl-Alt-Delete key sequence must be disa...

V-257786
RHEL 9 debug-shell systemd service must be disab...

V-257787

462 Rules

Red Hat Enterprise Linux 9

Red Hat Enterprise Linux 9 Security Technical Implementation Guide
Version: 2 Release: 1 Benchmark Date: 24 Jul 2024

SRG-OS-000480-GPOS-00227 V-257777
RHEL 9 must be a vendor-supported release.

SRG-OS-000480-GPOS-00227 V-257778
RHEL 9 vendor packaged system security patches and updates must be installed and up to date.

SRG-OS-000023-GPOS-00006 V-257779
RHEL 9 must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.

SRG-OS-000480-GPOS-00227 V-257781
The graphical display manager must not be the default target on RHEL 9 unless approved.

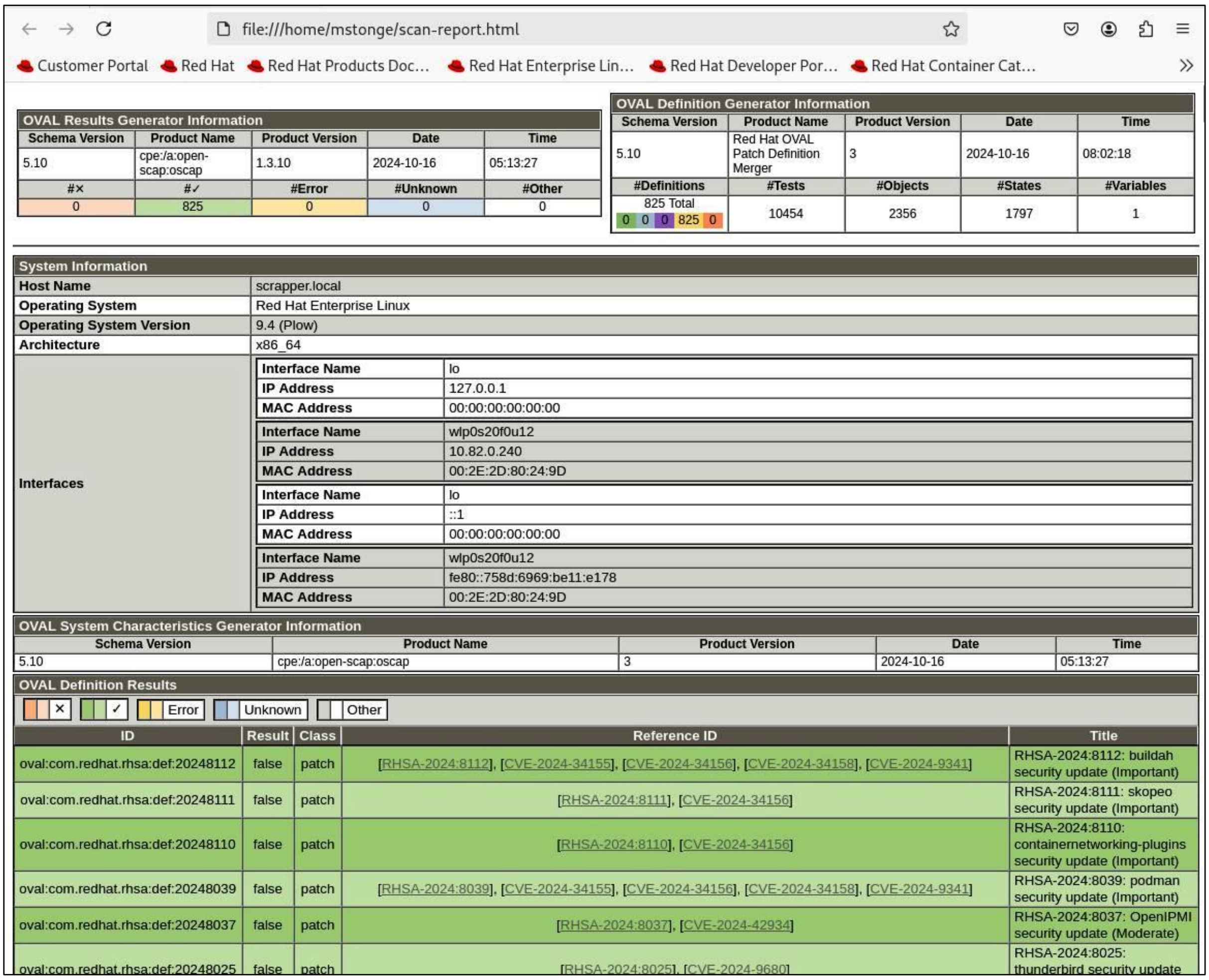
SRG-OS-000480-GPOS-00227 V-257782
RHEL 9 must enable the hardware random number generator entropy gatherer service.

SRG-OS-000269-GPOS-00103 V-257783
RHEL 9 systemd-journald service must be enabled.

SRG-OS-000324-GPOS-00125 V-257784
The systemd Ctrl-Alt-Delete burst key sequence in RHEL 9 must be disabled.

SRG-OS-000324-GPOS-00125 V-257785
The x86 Ctrl-Alt-Delete key sequence must be disabled on RHEL 9.

SRG-OS-000324-GPOS-00125 V-257786
RHEL 9 debug-shell systemd service must be disabled.



file:///home/mstonge/scan-report.html

OVAL Results Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap	1.3.10	2024-10-16	05:13:27
#×	**#✓**	**#Error**	**#Unknown**	**#Other**
0	825	0	0	0

OVAL Definition Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	Red Hat OVAL Patch Definition Merger	3	2024-10-16	08:02:18
#Definitions	**#Tests**	**#Objects**	**#States**	**#Variables**
825 Total 0 0 0 825 0	10454	2356	1797	1

System Information

Host Name	scrapper.local
Operating System	Red Hat Enterprise Linux
Operating System Version	9.4 (Plow)
Architecture	x86_64
Interfaces	**Interface Name** lo **IP Address** 127.0.0.1 **MAC Address** 00:00:00:00:00:00 **Interface Name** wlp0s20f0u12 **IP Address** 10.82.0.240 **MAC Address** 00:2E:2D:80:24:9D **Interface Name** lo **IP Address** ::1 **MAC Address** 00:00:00:00:00:00 **Interface Name** wlp0s20f0u12 **IP Address** fe80::758d:6969:be11:e178 **MAC Address** 00:2E:2D:80:24:9D

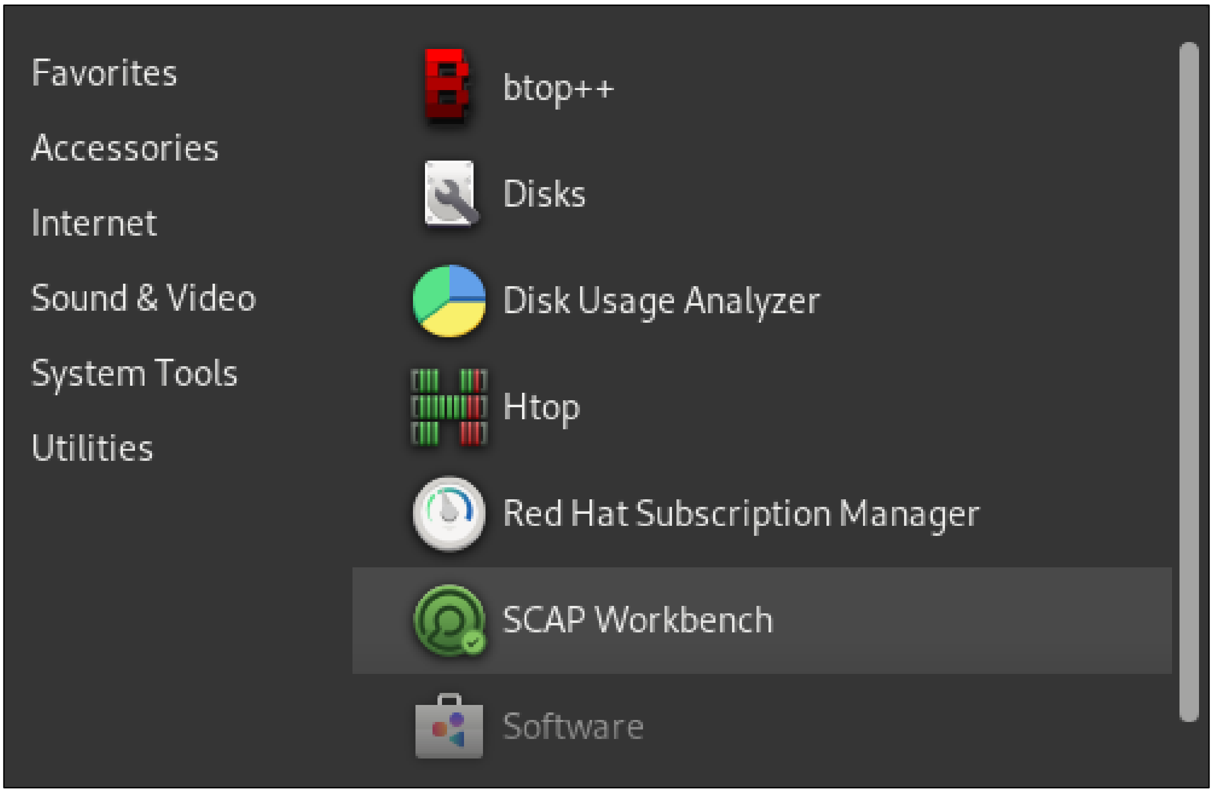
OVAL System Characteristics Generator Information

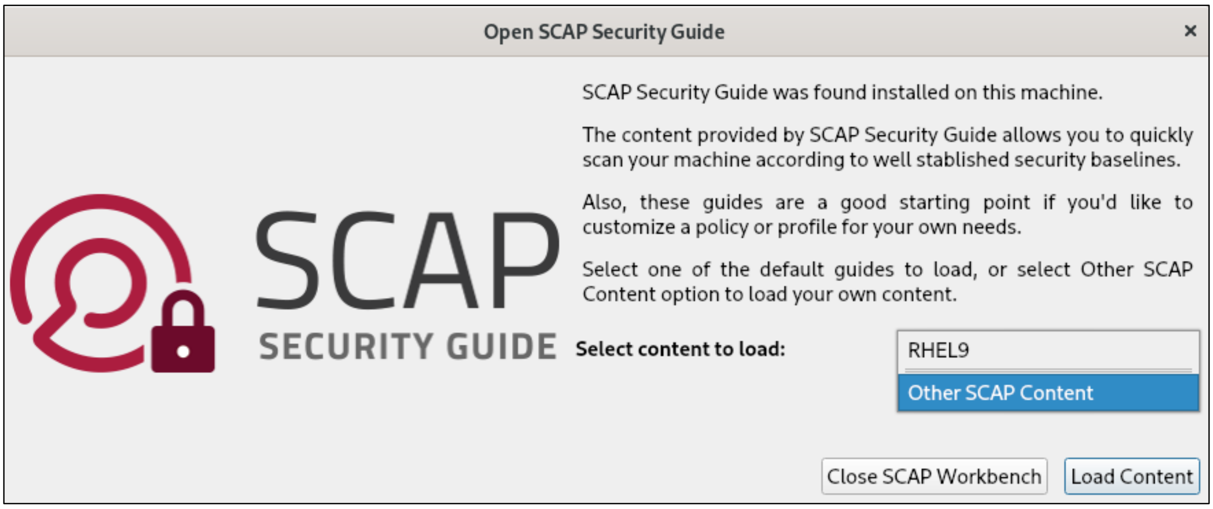
Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap	3	2024-10-16	05:13:27

OVAL Definition Results

× ✓ Error Unknown Other

ID	Result	Class	Reference ID	Title
oval:com.redhat.rhsa:def:20248112	false	patch	[RHSA-2024:8112], [CVE-2024-34155], [CVE-2024-34156], [CVE-2024-34158], [CVE-2024-9341]	RHSA-2024:8112: buildah security update (Important)
oval:com.redhat.rhsa:def:20248111	false	patch	[RHSA-2024:8111], [CVE-2024-34156]	RHSA-2024:8111: skopeo security update (Important)
oval:com.redhat.rhsa:def:20248110	false	patch	[RHSA-2024:8110], [CVE-2024-34156]	RHSA-2024:8110: containernetworking-plugins security update (Important)
oval:com.redhat.rhsa:def:20248039	false	patch	[RHSA-2024:8039], [CVE-2024-34155], [CVE-2024-34156], [CVE-2024-34158], [CVE-2024-9341]	RHSA-2024:8039: podman security update (Important)
oval:com.redhat.rhsa:def:20248037	false	patch	[RHSA-2024:8037], [CVE-2024-42934]	RHSA-2024:8037: OpenIPMI security update (Moderate)
oval:com.redhat.rhsa:def:20248025	false	patch	[RHSA-2024:8025], [CVE-2024-9680]	RHSA-2024:8025: thunderbird security update





Open SCAP Security Guide

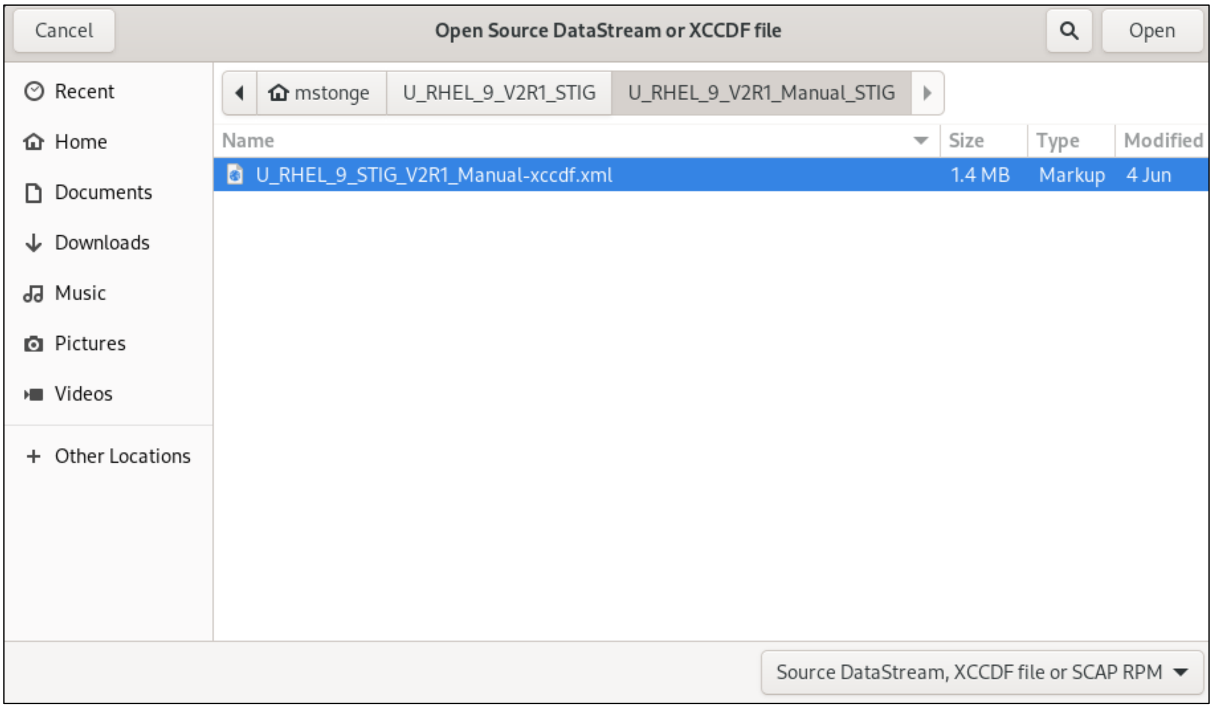
SCAP Security Guide was found installed on this machine.

The content provided by SCAP Security Guide allows you to quickly scan your machine according to well stablished security baselines.

Also, these guides are a good starting point if you'd like to customize a policy or profile for your own needs.

Select one of the default guides to load, or select Other SCAP Content option to load your own content.

Select content to load: RHEL9 / Other SCAP Content

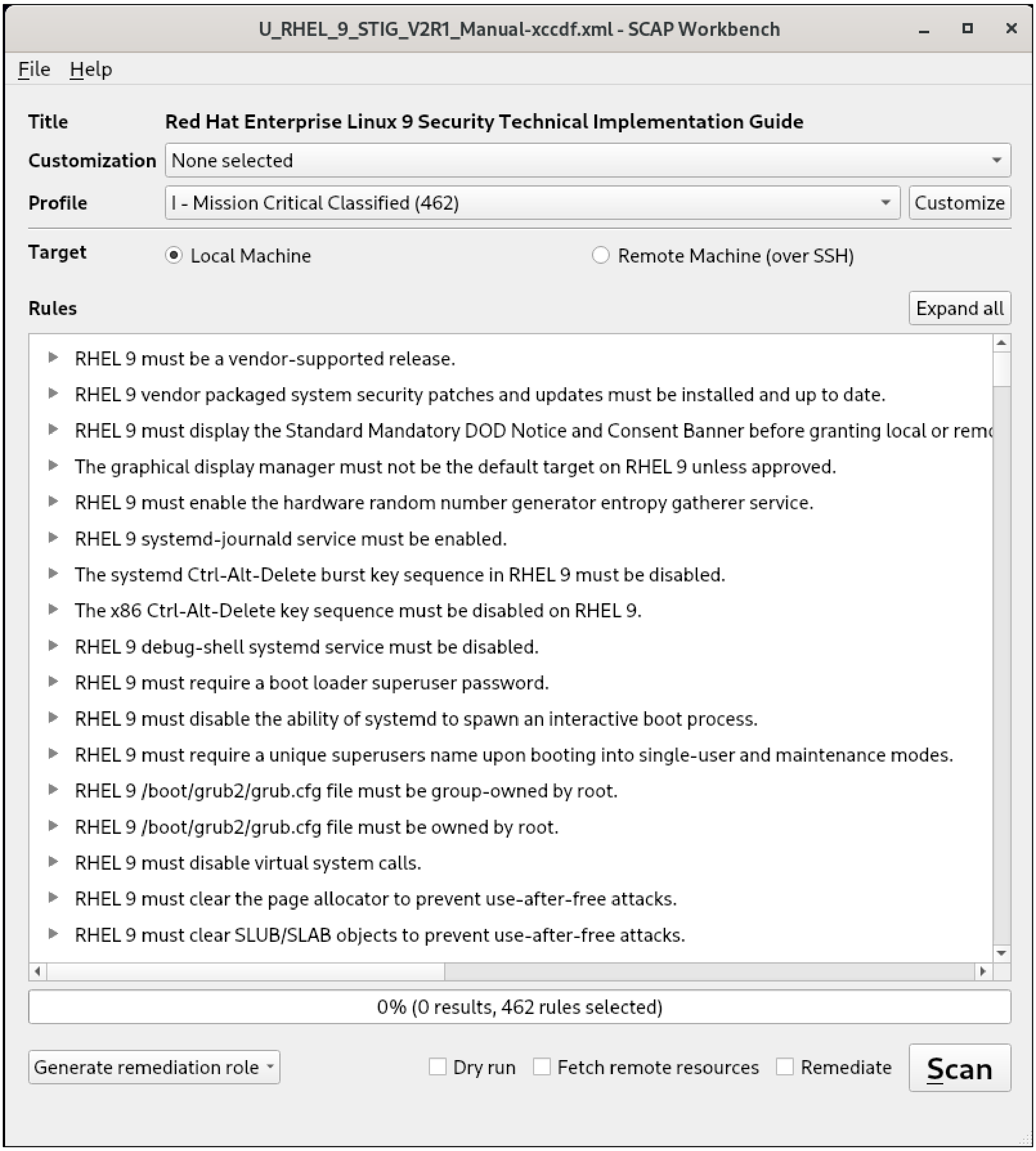


Open Source DataStream or XCCDF file

mstonge U_RHEL_9_V2R1_STIG U_RHEL_9_V2R1_Manual_STIG

Name	Size	Type	Modified
U_RHEL_9_STIG_V2R1_Manual-xccdf.xml	1.4 MB	Markup	4 Jun

Source DataStream, XCCDF file or SCAP RPM



U_RHEL_9_STIG_V2R1_Manual-xccdf.xml - SCAP Workbench
File
Help
Customize
Expand all
Generate remediation role
Scan

Title: Red Hat Enterprise Linux 9 Security Technical Implementation Guide

Customization: None selected

Profile: I - Mission Critical Classified (462)

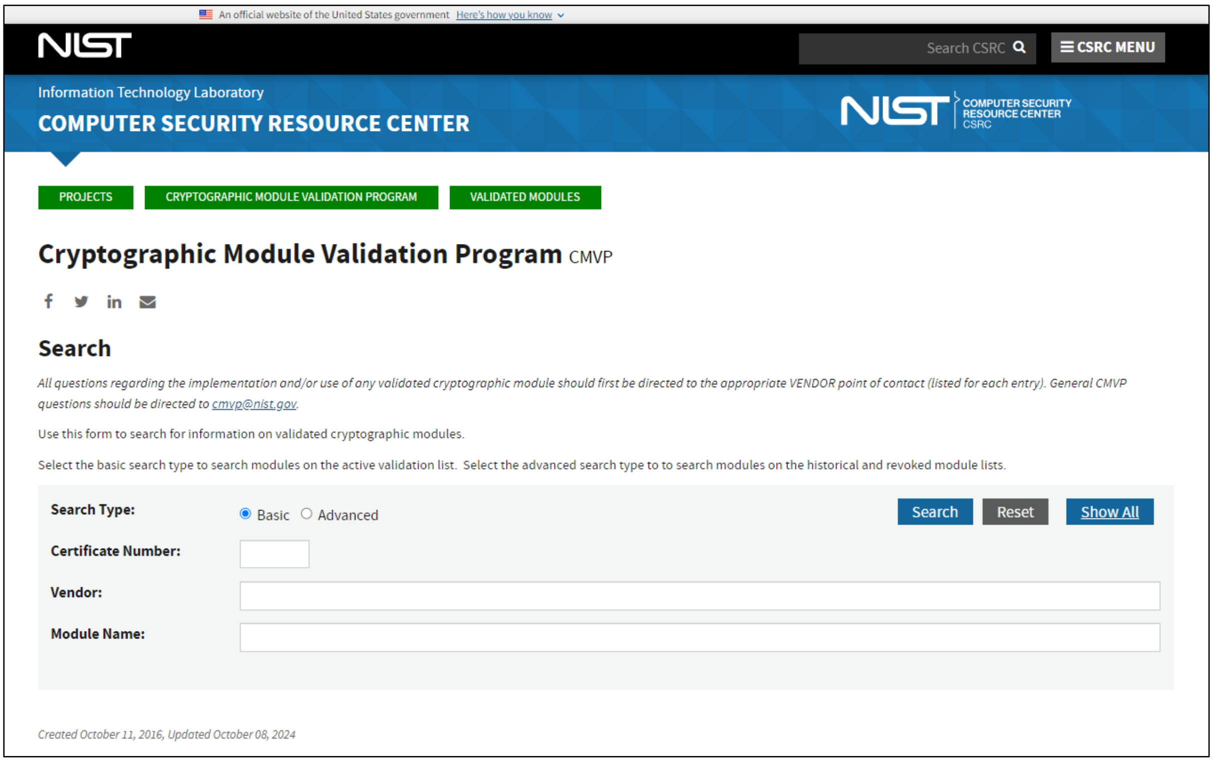
Target: ● Local Machine ○ Remote Machine (over SSH)

Rules

- RHEL 9 must be a vendor-supported release.
- RHEL 9 vendor packaged system security patches and updates must be installed and up to date.
- RHEL 9 must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remo
- The graphical display manager must not be the default target on RHEL 9 unless approved.
- RHEL 9 must enable the hardware random number generator entropy gatherer service.
- RHEL 9 systemd-journald service must be enabled.
- The systemd Ctrl-Alt-Delete burst key sequence in RHEL 9 must be disabled.
- The x86 Ctrl-Alt-Delete key sequence must be disabled on RHEL 9.
- RHEL 9 debug-shell systemd service must be disabled.
- RHEL 9 must require a boot loader superuser password.
- RHEL 9 must disable the ability of systemd to spawn an interactive boot process.
- RHEL 9 must require a unique superusers name upon booting into single-user and maintenance modes.
- RHEL 9 /boot/grub2/grub.cfg file must be group-owned by root.
- RHEL 9 /boot/grub2/grub.cfg file must be owned by root.
- RHEL 9 must disable virtual system calls.
- RHEL 9 must clear the page allocator to prevent use-after-free attacks.
- RHEL 9 must clear SLUB/SLAB objects to prevent use-after-free attacks.

0% (0 results, 462 rules selected)

☐ Dry run ☐ Fetch remote resources ☐ Remediate


An official website of the United States government Here's how you know
NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
PROJECTS
CRYPTOGRAPHIC MODULE VALIDATION PROGRAM
VALIDATED MODULES

Cryptographic Module Validation Program CMVP

Search

All questions regarding the implementation and/or use of any validated cryptographic module should first be directed to the appropriate VENDOR point of contact (listed for each entry). General CMVP questions should be directed to cmvp@nist.gov.

Use this form to search for information on validated cryptographic modules.

Select the basic search type to search modules on the active validation list. Select the advanced search type to to search modules on the historical and revoked module lists.

Search Type: ● Basic ○ Advanced

Certificate Number:

Vendor:

Module Name:

Created October 11, 2016, Updated October 08, 2024

Chapter 14: Customer and Community Feedback Loops