DISA STIG On Rocky Linux 8 (English version)

A book from the Documentation Team

Version : 2024/04/29

Rocky Documentation Team

Table of contents

1. Licence

RockyLinux offers Linux courseware for trainers or people wishing to learn how to administer a Linux system on their own.

The documents and their sources are freely downloadable from:

- https://docs.rockylinux.org
- https://github.com/rocky-linux/documentation

Our media sources are hosted at github.com. You'll find the source code repository where the version of this document was created.

From these sources, you can generate your own personalized training material using mkdocs. You will find instructions for generating your document here.

How can I contribute to the documentation project?

You'll find all the information you need to join us on our git project home page.

We wish you all a pleasant reading and hope you enjoy the content.

2. HOWTO: STIG Rocky Linux 8 Fast - Part 1

2.1 Terminology Reference

- DISA - Defense Information Systems Agency
- RHEL8 - Red Hat Enterprise Linux 8
- STIG - Secure Technical Implementation Guide
- SCAP - Secure Content Automation Protocol
- DoD - Department of Defense

2.2 Introduction

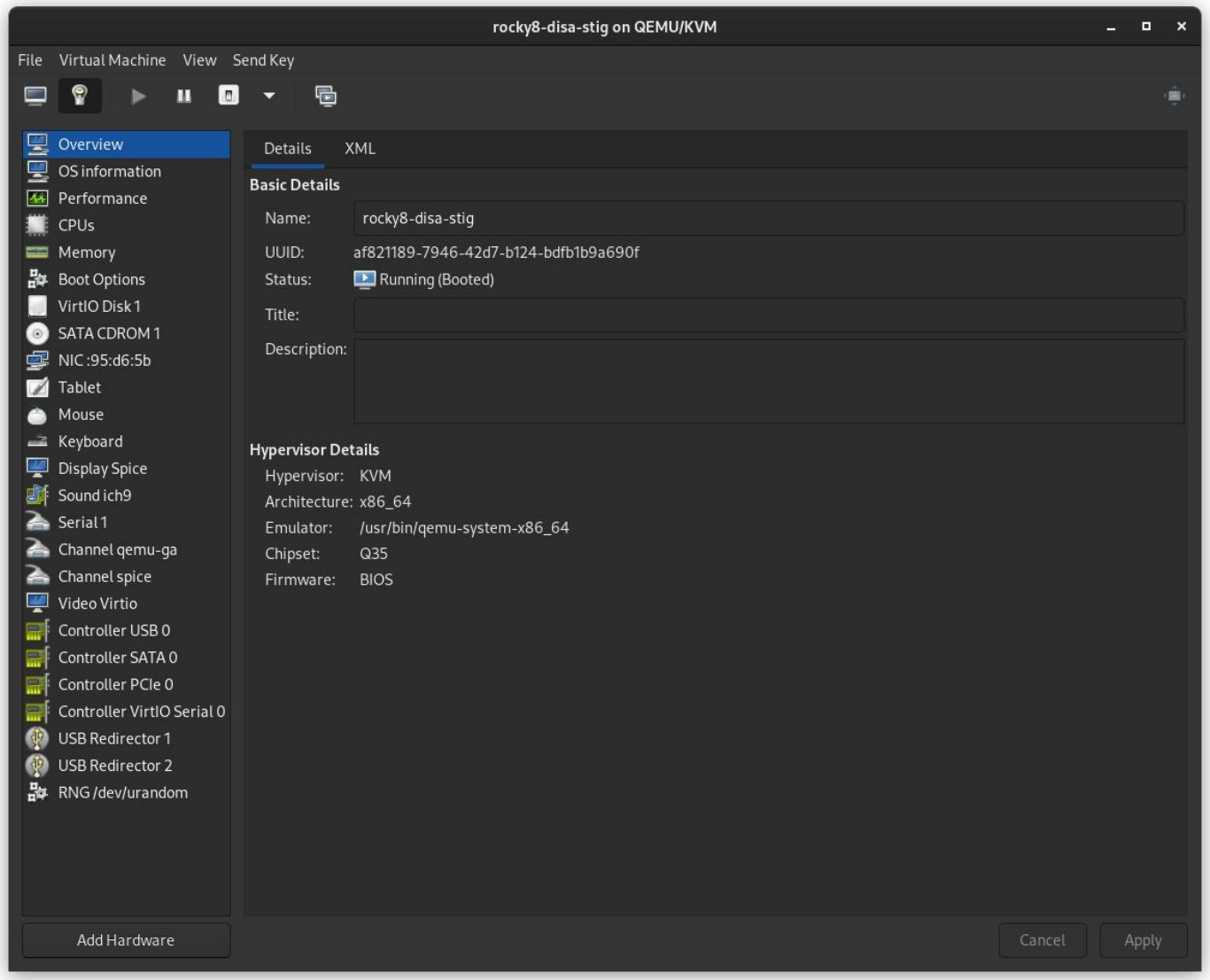
In this guide we are going to cover how to apply the DISA STIG for RHEL8 for a New Installation of Rocky Linux 8. As multi-part series, we will also be covering how to test STIG compliance, adapt STIG settings, and apply other STIG content in this environment.

Rocky Linux is a bug for bug derivative of RHEL and as such the content published for the DISA RHEL8 STIG is in parity for both operating systems. Even better news, applying STIG settings is built into the Rocky Linux 8 anaconda installer, under Security Profiles. Under the hood this is all powered by a tool called OpenSCAP, which lets you both configure the system to be compliant with the DISA STIG (fast!), and also test the systems compliance after you've installed.

I'll be doing this on a virtual machine in my environment, but everything here would apply the exact same way on bare iron.

2.2.1 Step 1: Create the Virtual Machine

- 2G memory
- 30G disk
- 1 core



2.2.2 Step 2: Download the Rocky Linux 8 DVD ISO

Download Rocky Linux DVD. **Note:** The minimal ISO does not contain the content needed to apply the STIG for Rocky Linux 8, you need to use the DVD or a network install.

Downloads

Download the official release of Rocky Linux from one of our trusted mirrors.

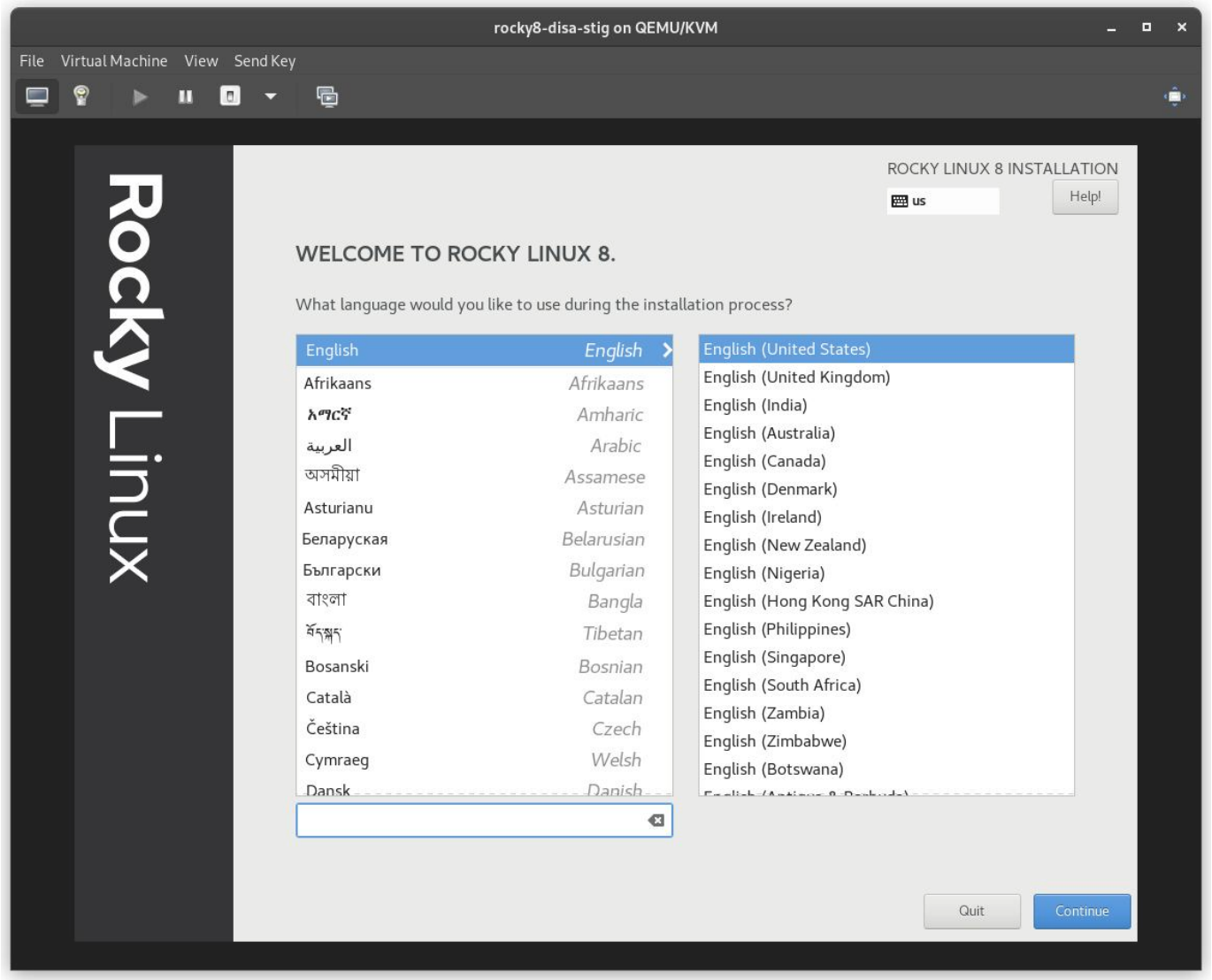
Rocky Linux 8 (Current)

Planned EOL: May 31 2029

ARCHITECTURE	ISOS	PACKAGES
x86_64	Minimal | DVD | Boot | Torrent | Checksum	BaseOS
ARM64 (aarch64)	Minimal | DVD | Boot | Torrent | Checksum	BaseOS

Alternative Images | Cloud Images | Archived Releases | Documentation | Report Bug

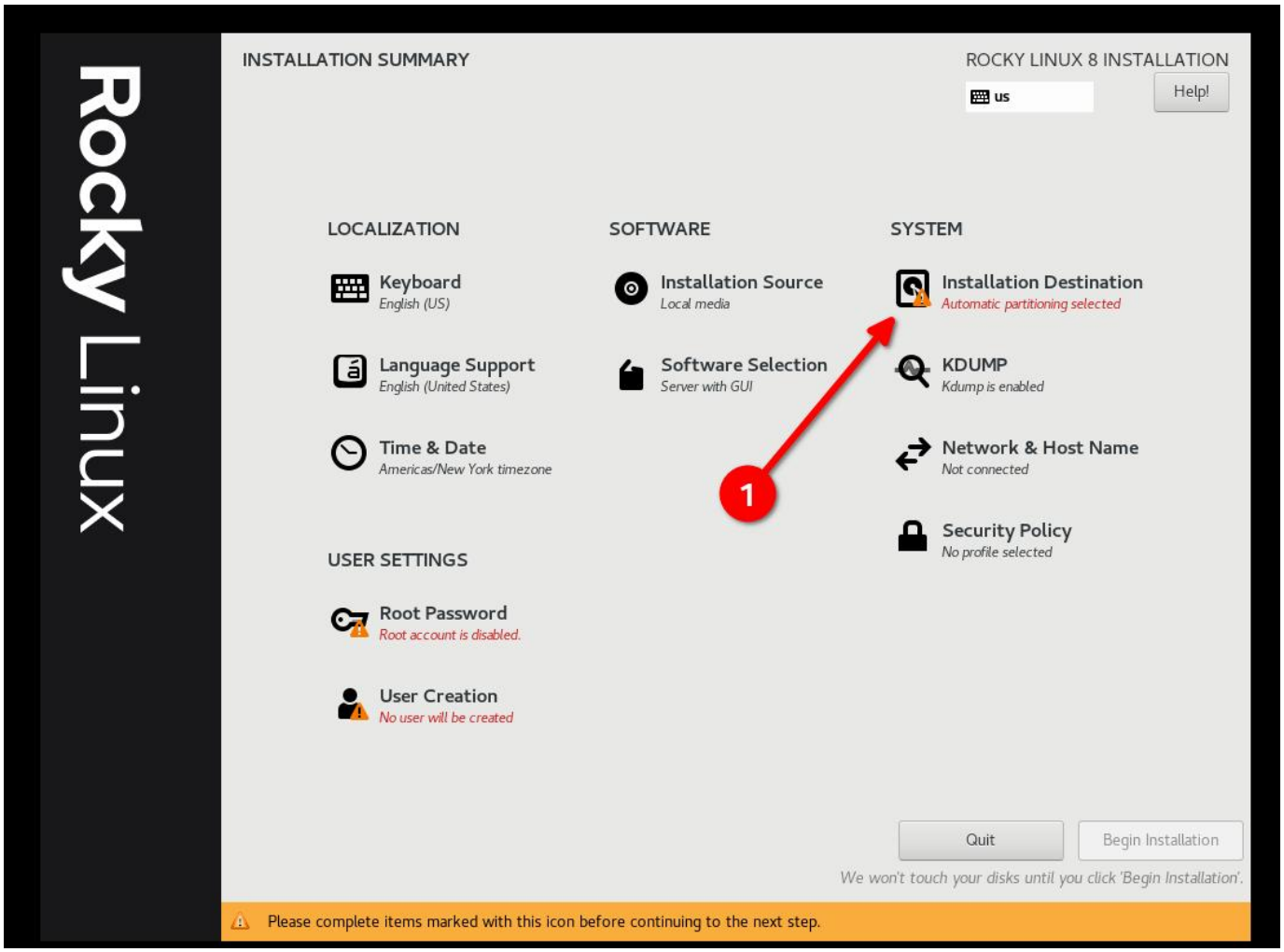
2.2.3 Step 3: Boot the Installer



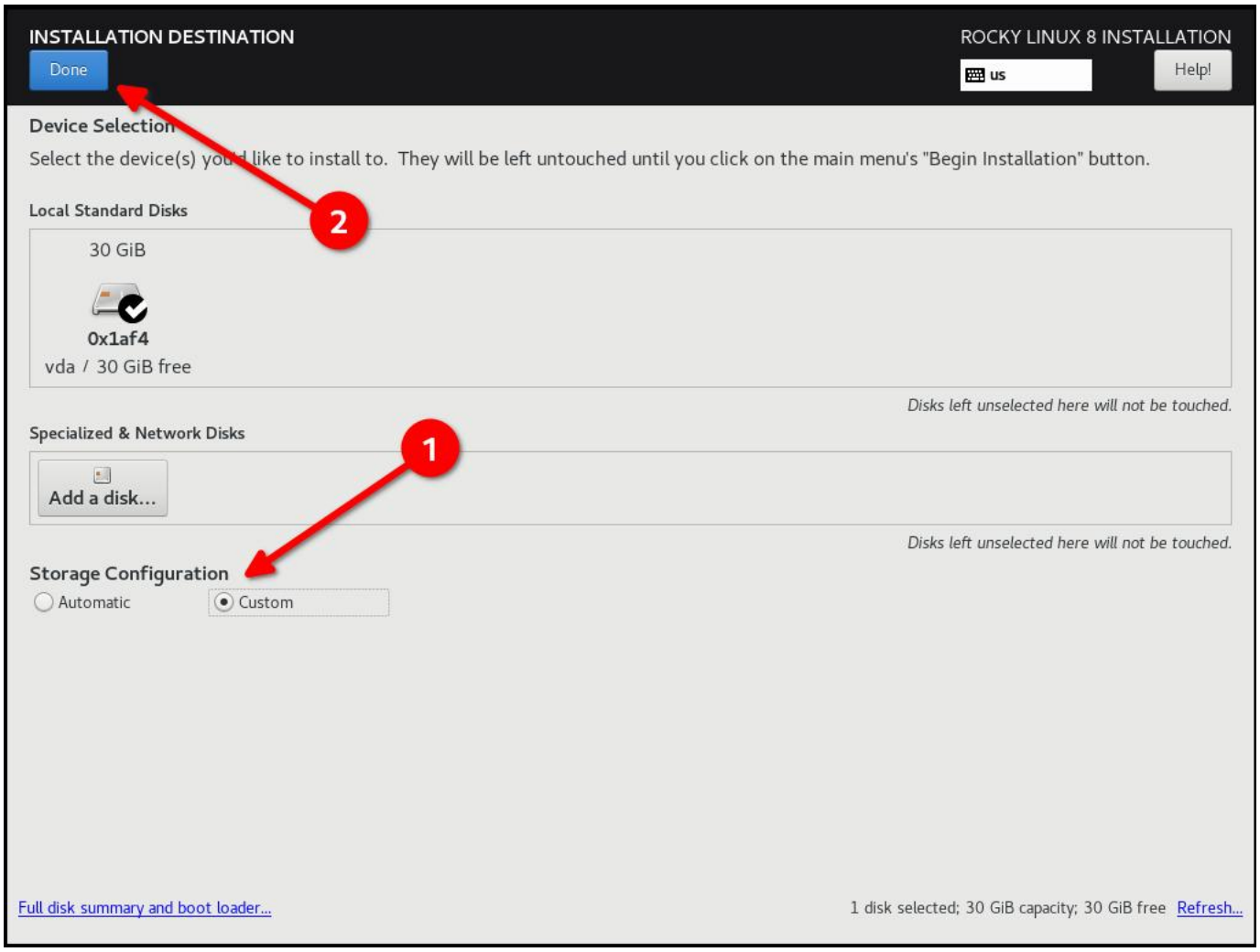
2.2.4 Step 4: Select Partitioning FIRST

This is probably the most complicated step in the installation, and a requirement to be compliant with the STIG. You will need to partition the operating system's filesystem in a way that will probably create new problems. In other words: You're going to need to know exactly what your storage requirements are.

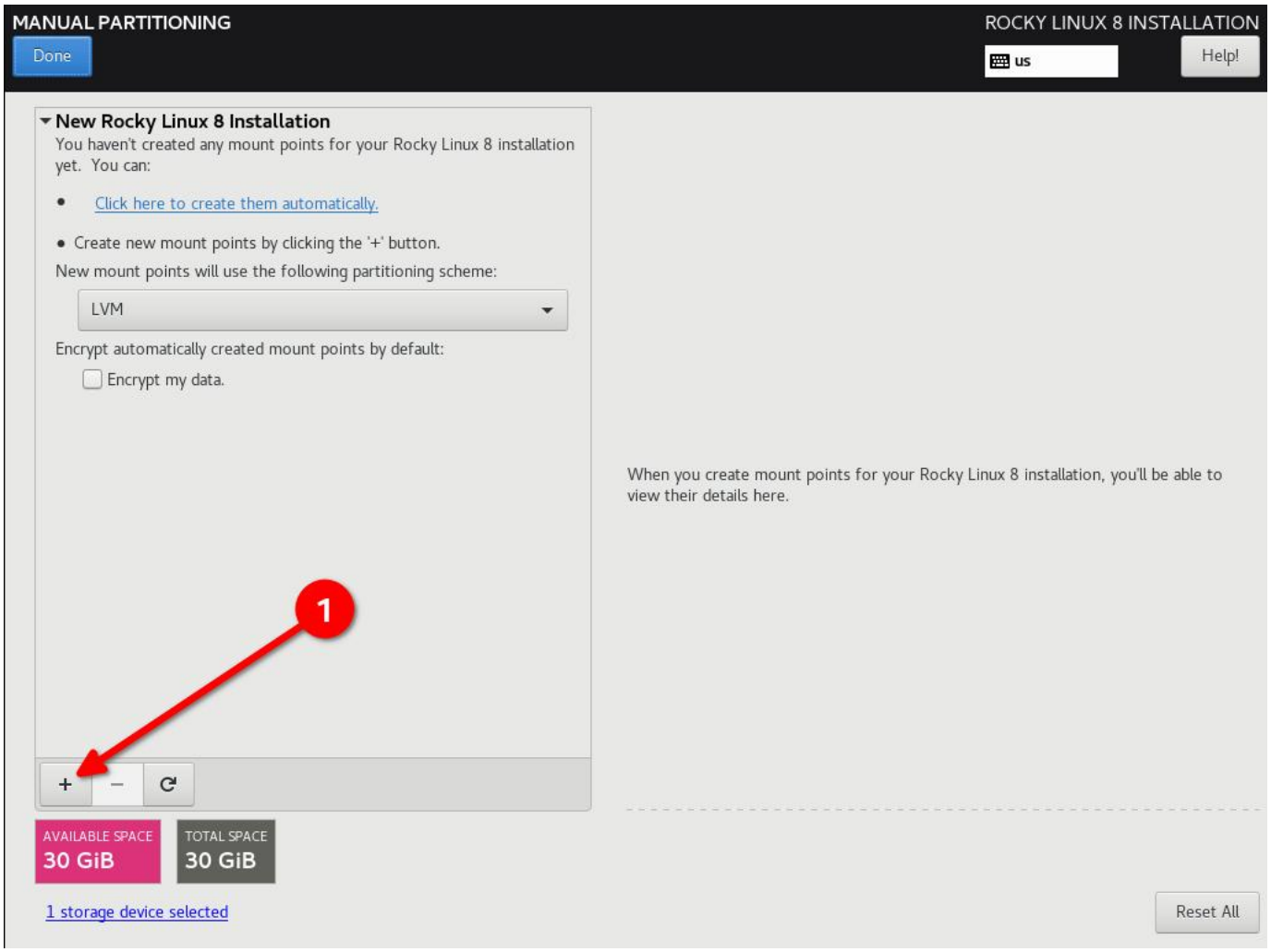
> **Pro-Tip**
>
> Linux lets you resize filesystems, which we'll cover in another article. Suffice to say, this is one of the bigger issues applying the DISA STIG on bare iron, frequently requiring full re-installs to solve, so over spec the size you need here.



- Select "Custom" and then "Done"



- Start Adding Partitions

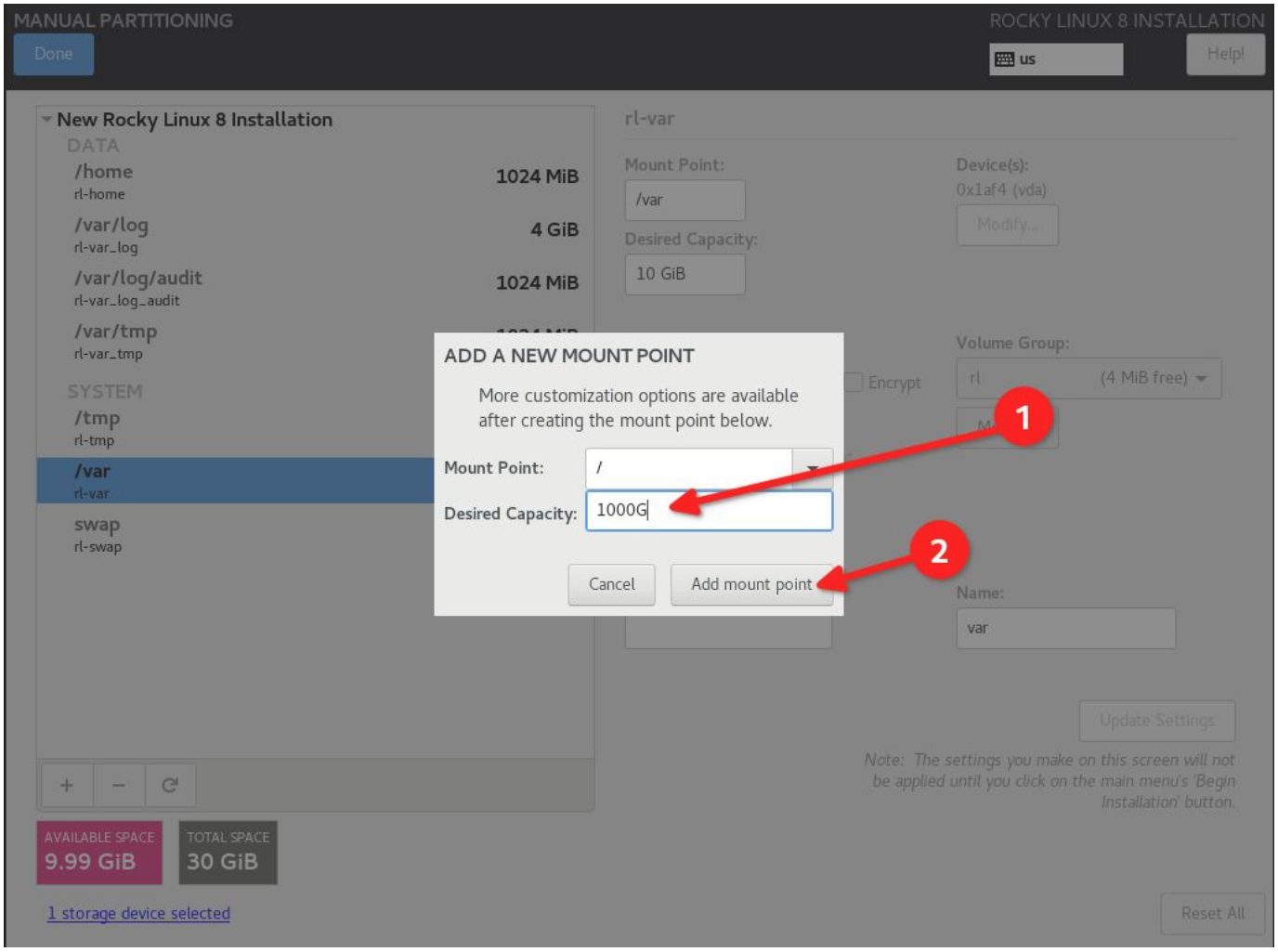


DISA STIG partitioning scheme for a 30G disk. My use case is as a simple web server:

- / (10G)
- /boot (500m)
- /var (10G)
- /var/log (4G)
- /var/log/audit (1G)
- /home (1G)
- /tmp (1G)
- /var/tmp (1G)
- Swap (2G)

Pro-Tip

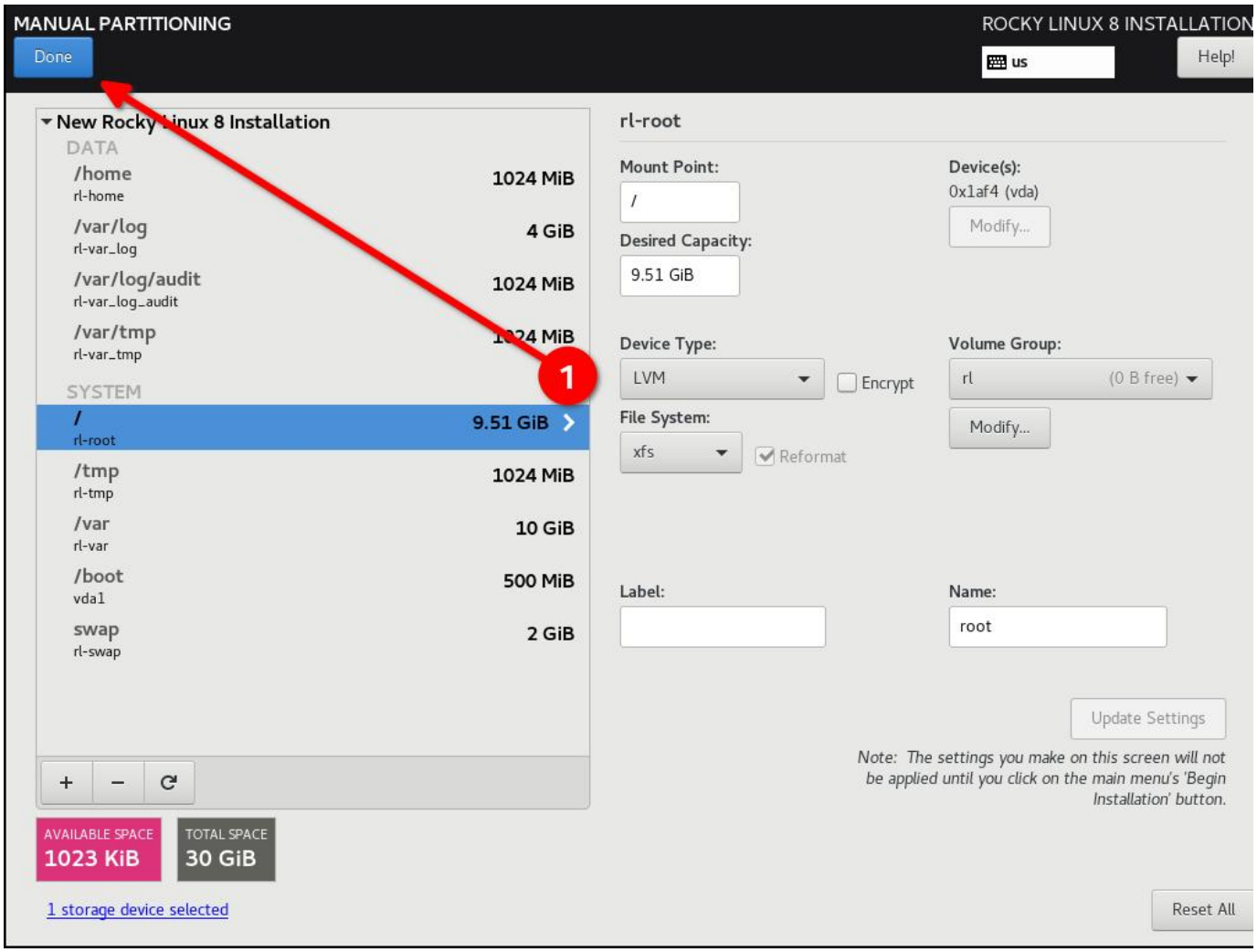
Configure / last and give it a really high number, this will put all the slack disk space left on / and you will not have to do any math.

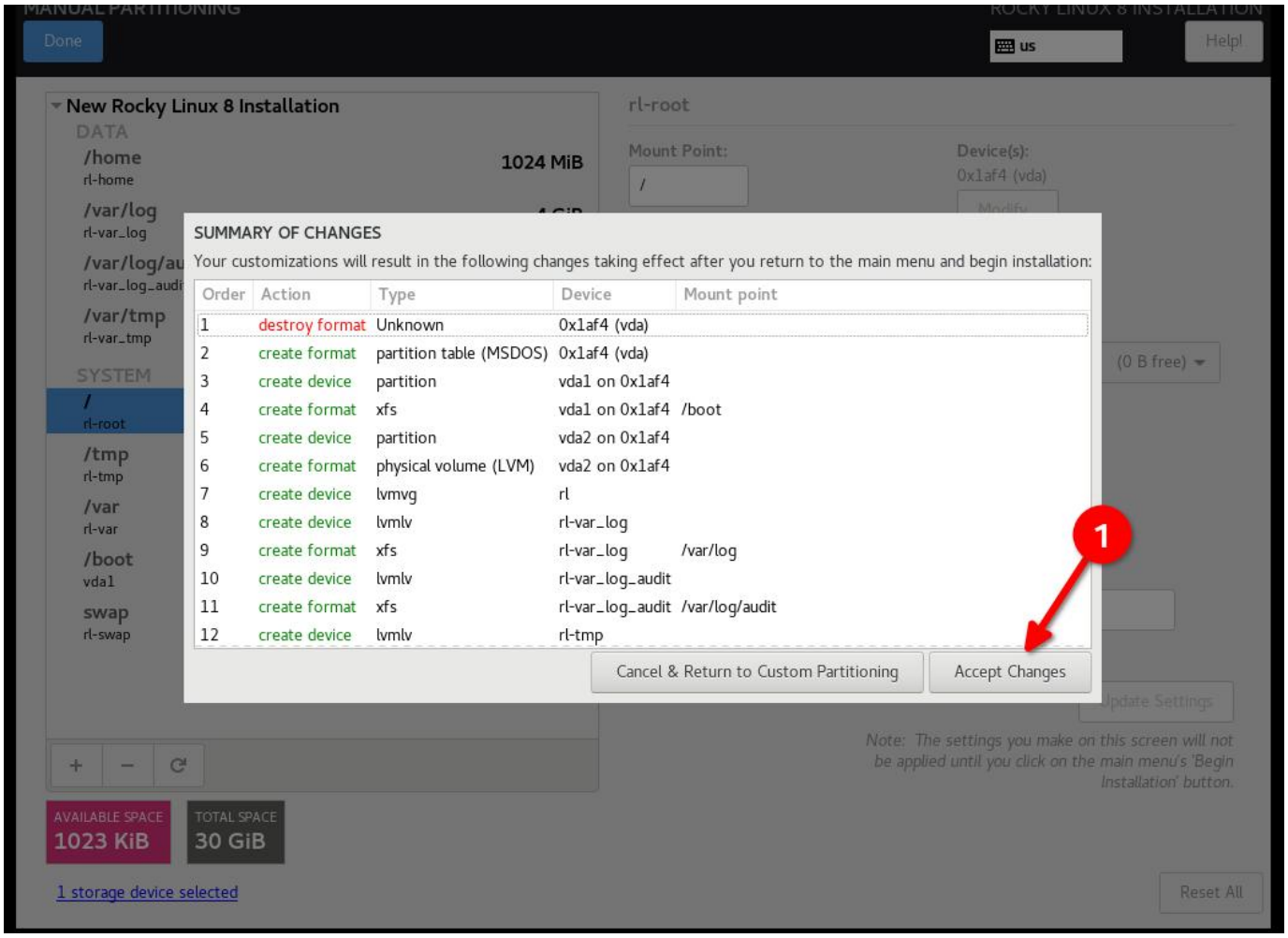


Pro-Tip

Re-iterating from the previous Pro-Tip: OVER SPEC your filesystems, even if you have to grow them again later.

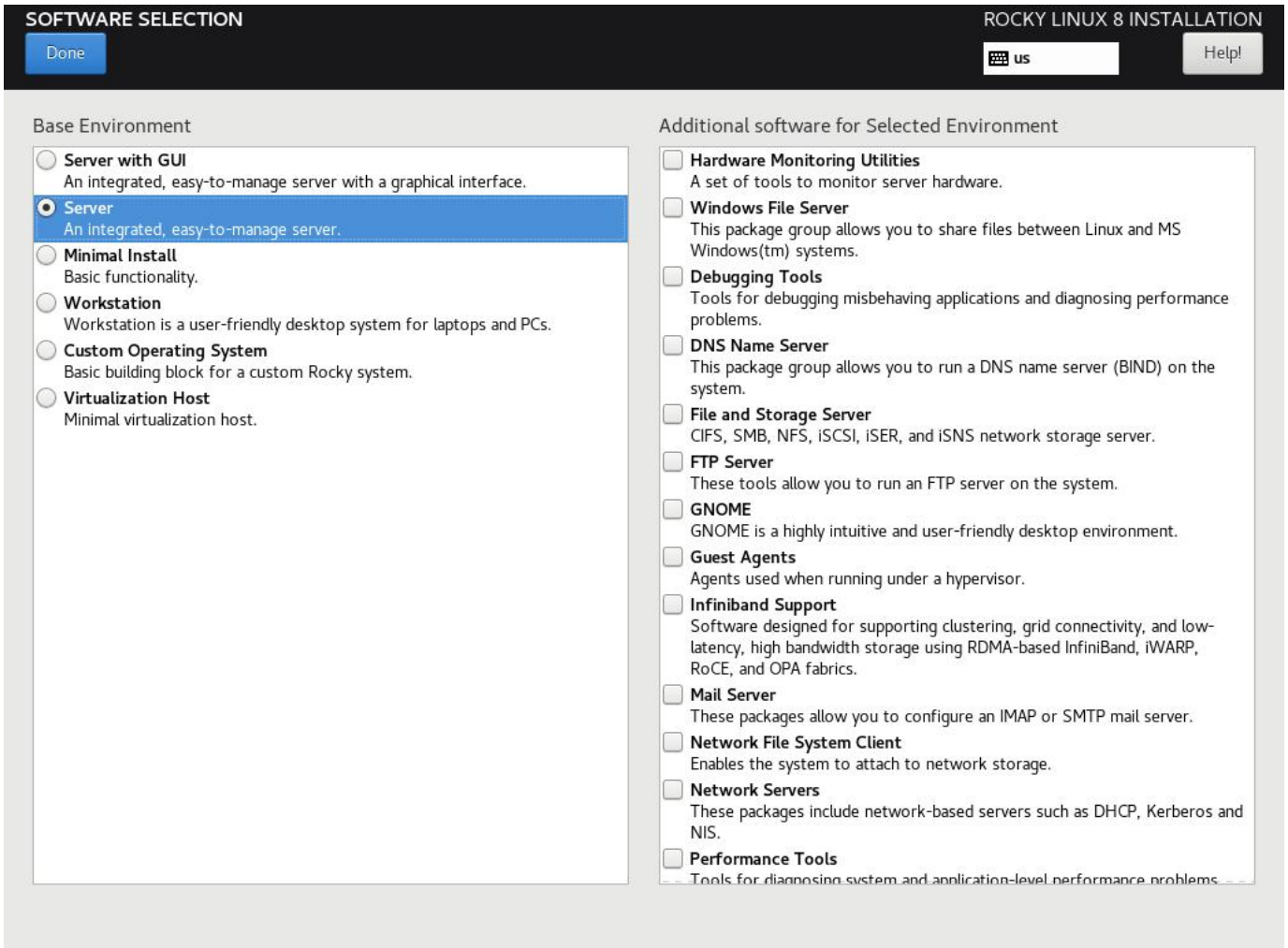
- Click "Done", and "Accept Changes"





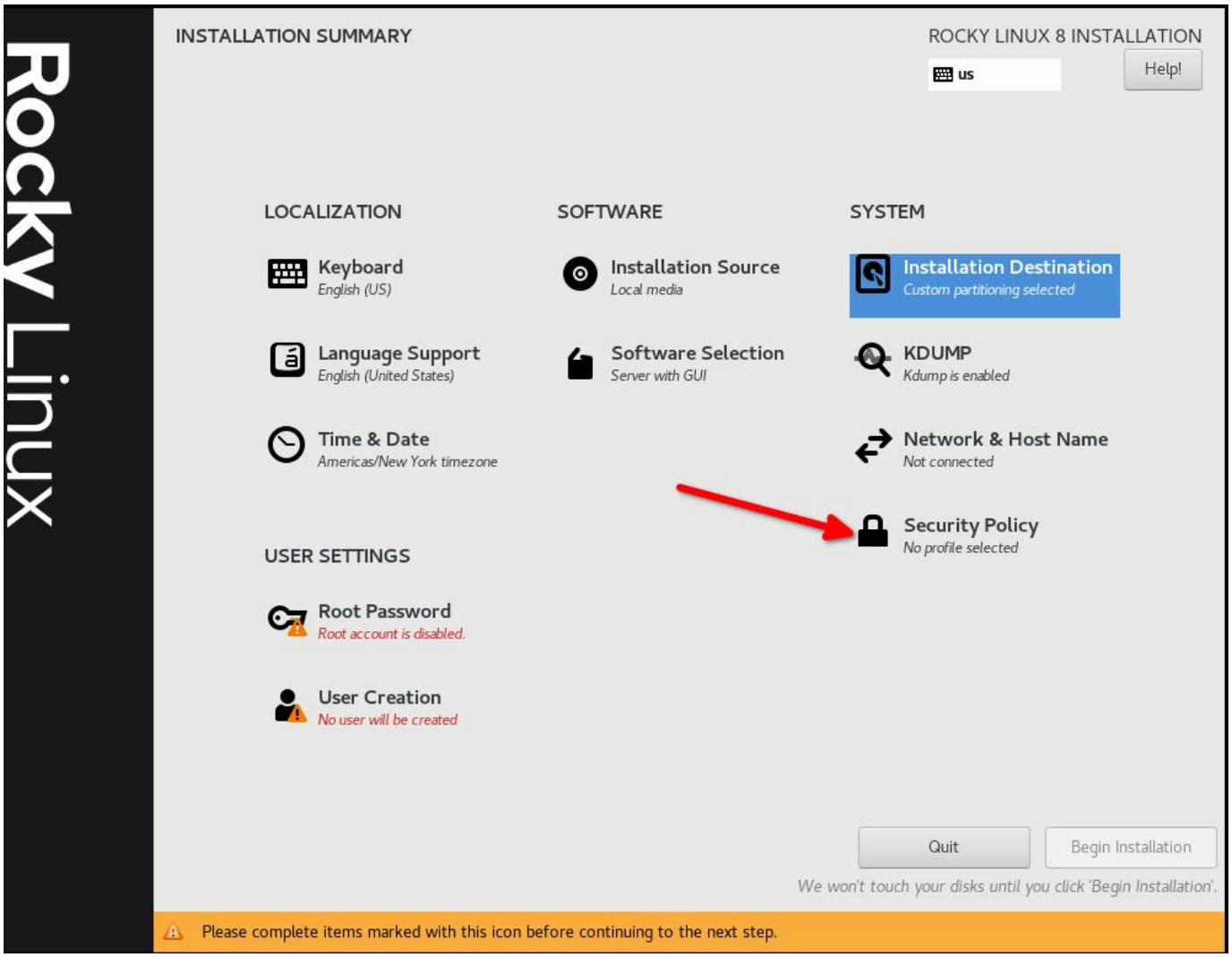
2.2.5 Step 5: Configure software for your environment: Server install without a GUI

This will matter in **Step 6**, so if you are using a UI or a workstation configuration the security profile will be different.

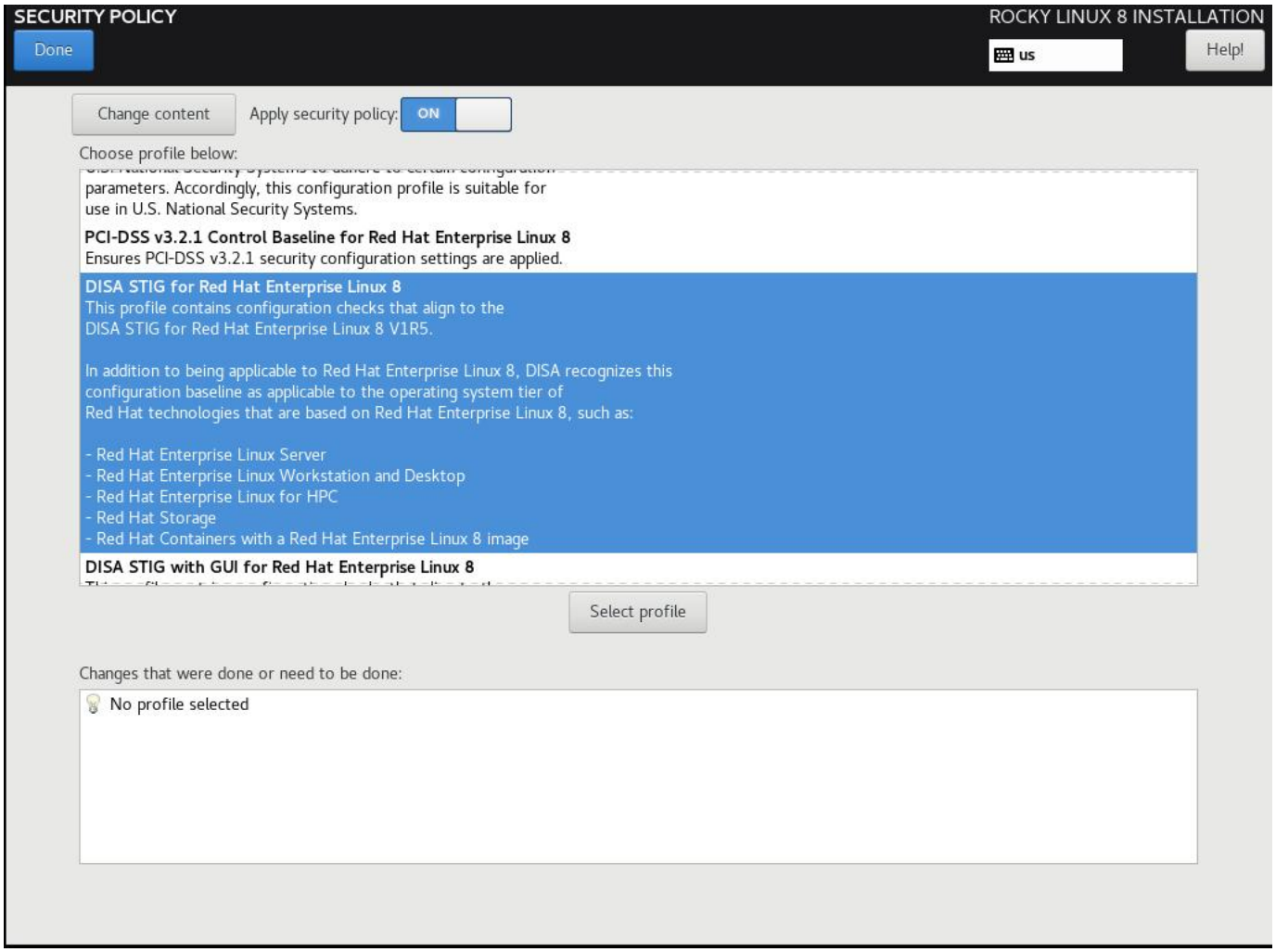


2.2.6 Step 6: Select Security Profile

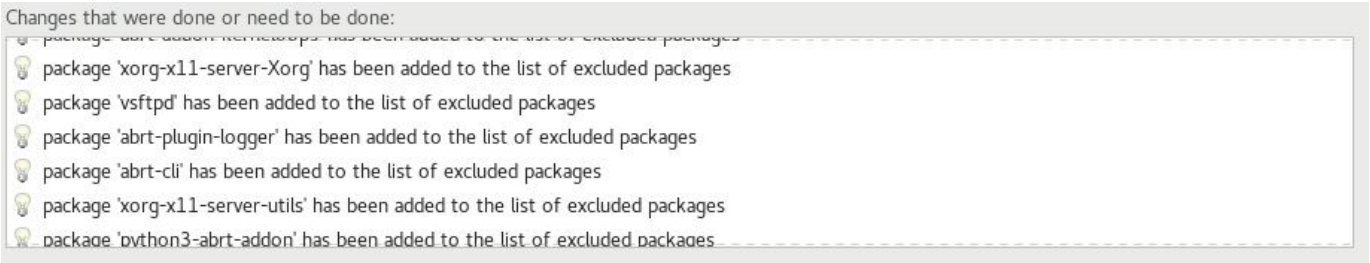
This is going to configure a number of security settings on the system based on the selected policy, leveraging the SCAP framework. It will modify the packages you selected in **Step 5**, adding or removing components needed. If you *did* select a GUI install in **Step 5**, and you use the non-GUI STIG in this step, it will remove the GUI. Adjust accordingly!

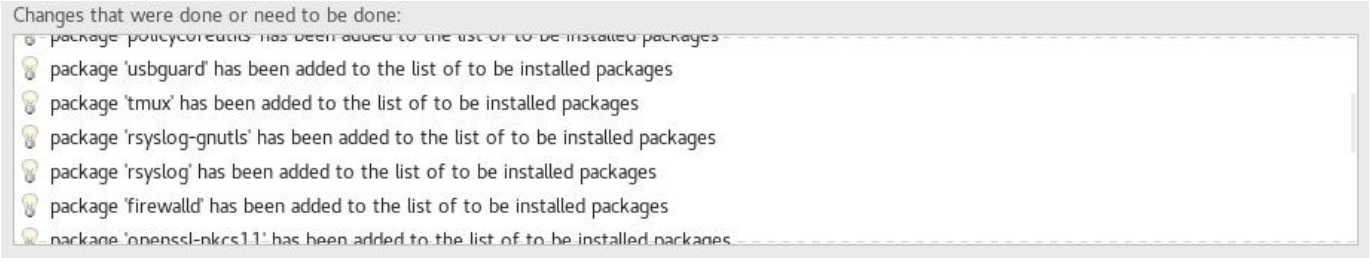


Select the DISA STIG for Red Hat Enterprise Linux 8:

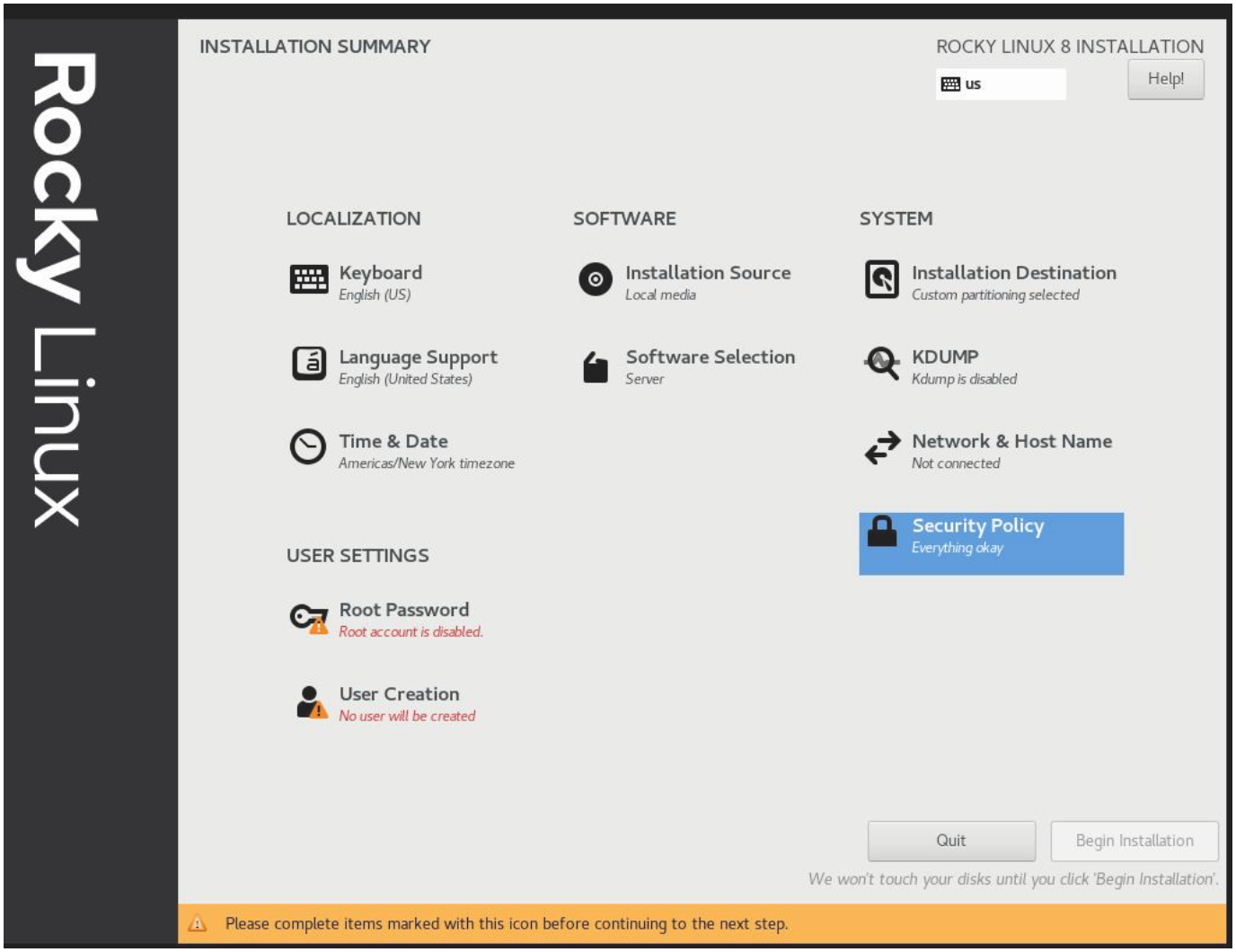


Click "Select Profile", and note the changes it is going to make to the system. This will set options on mount points, add/remove applications, and make other configuration changes:



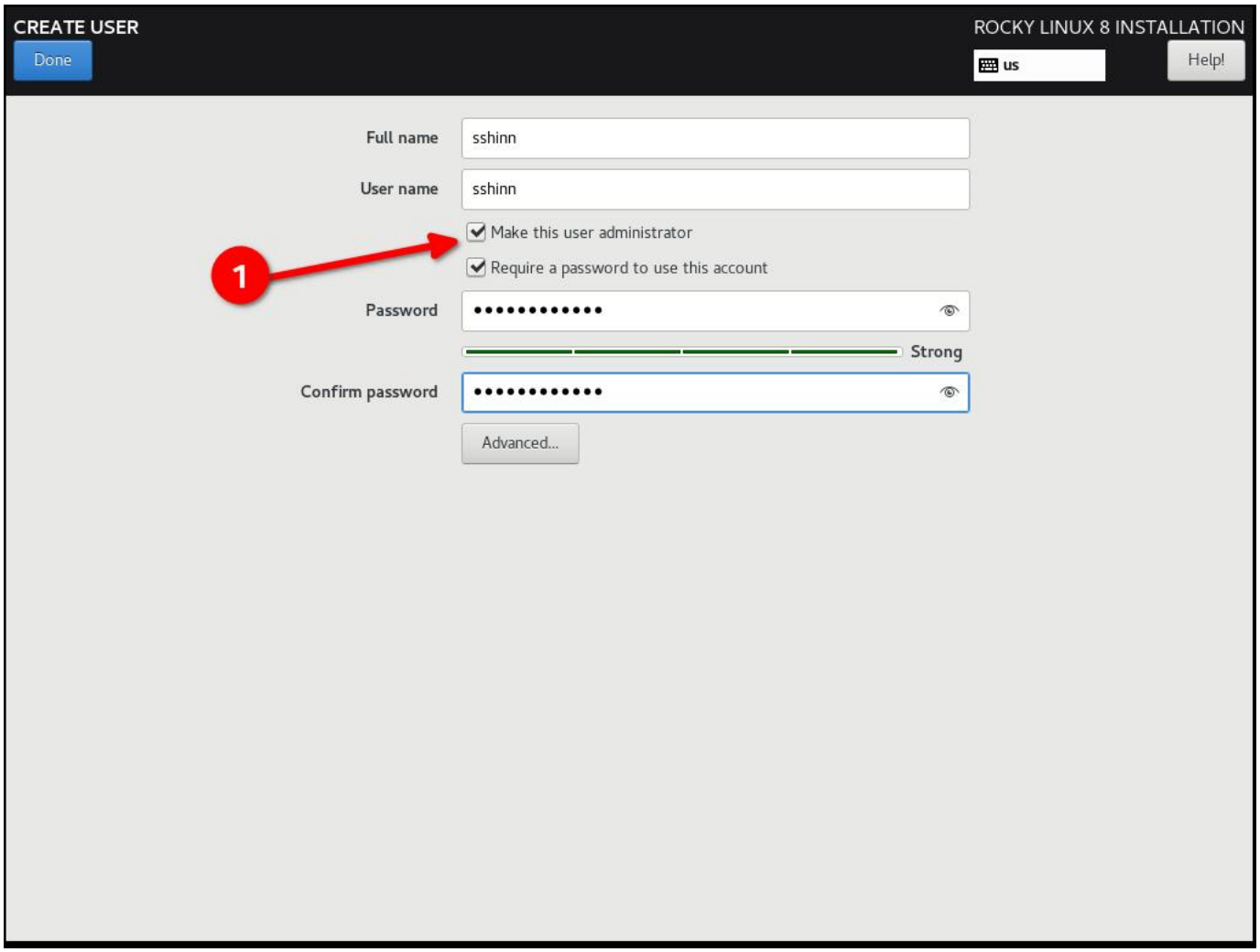


2.2.7 Step 7: Click "Done", and Continue To Final Setup

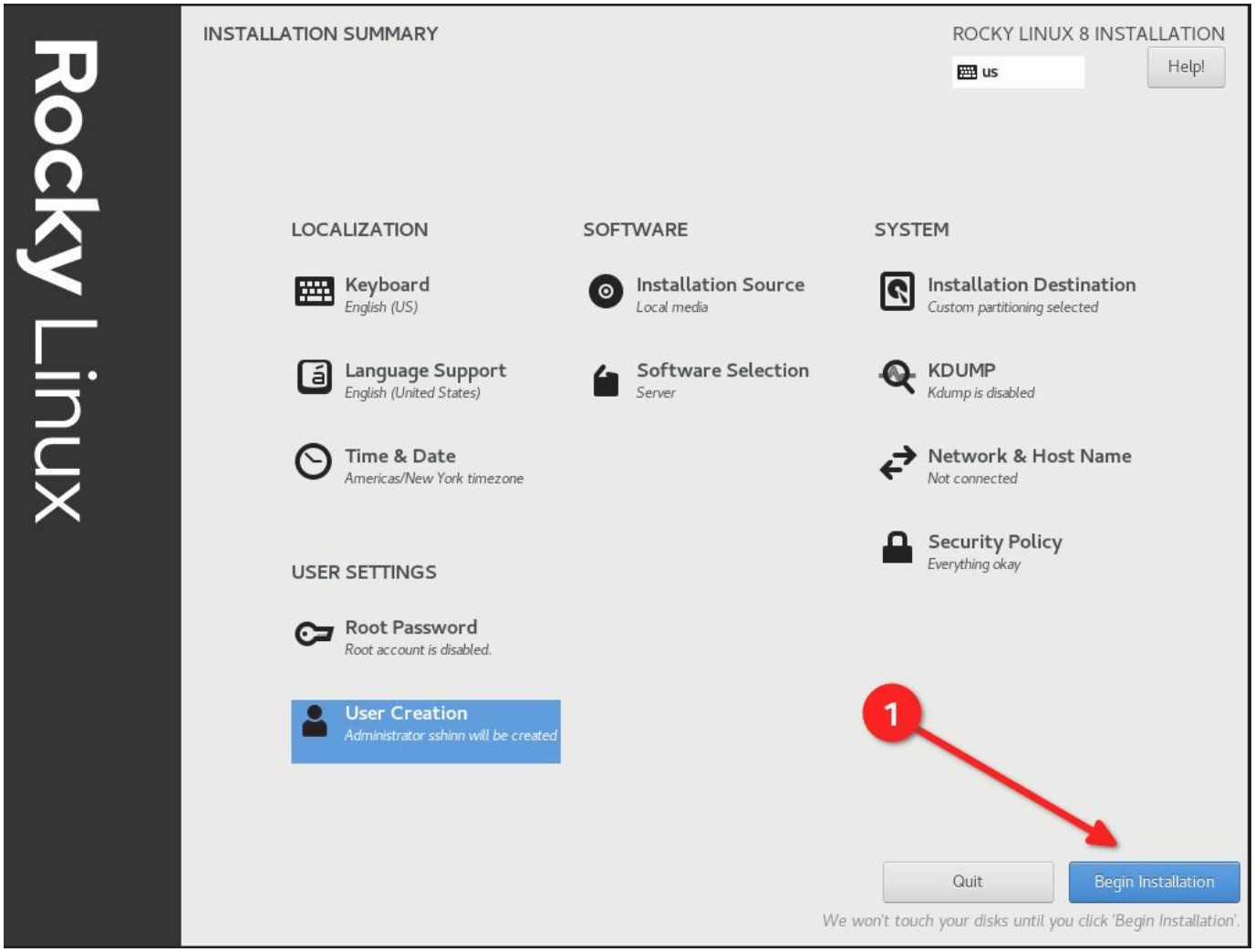


2.2.8 Step 8: Create a user account, and set that user to administrator

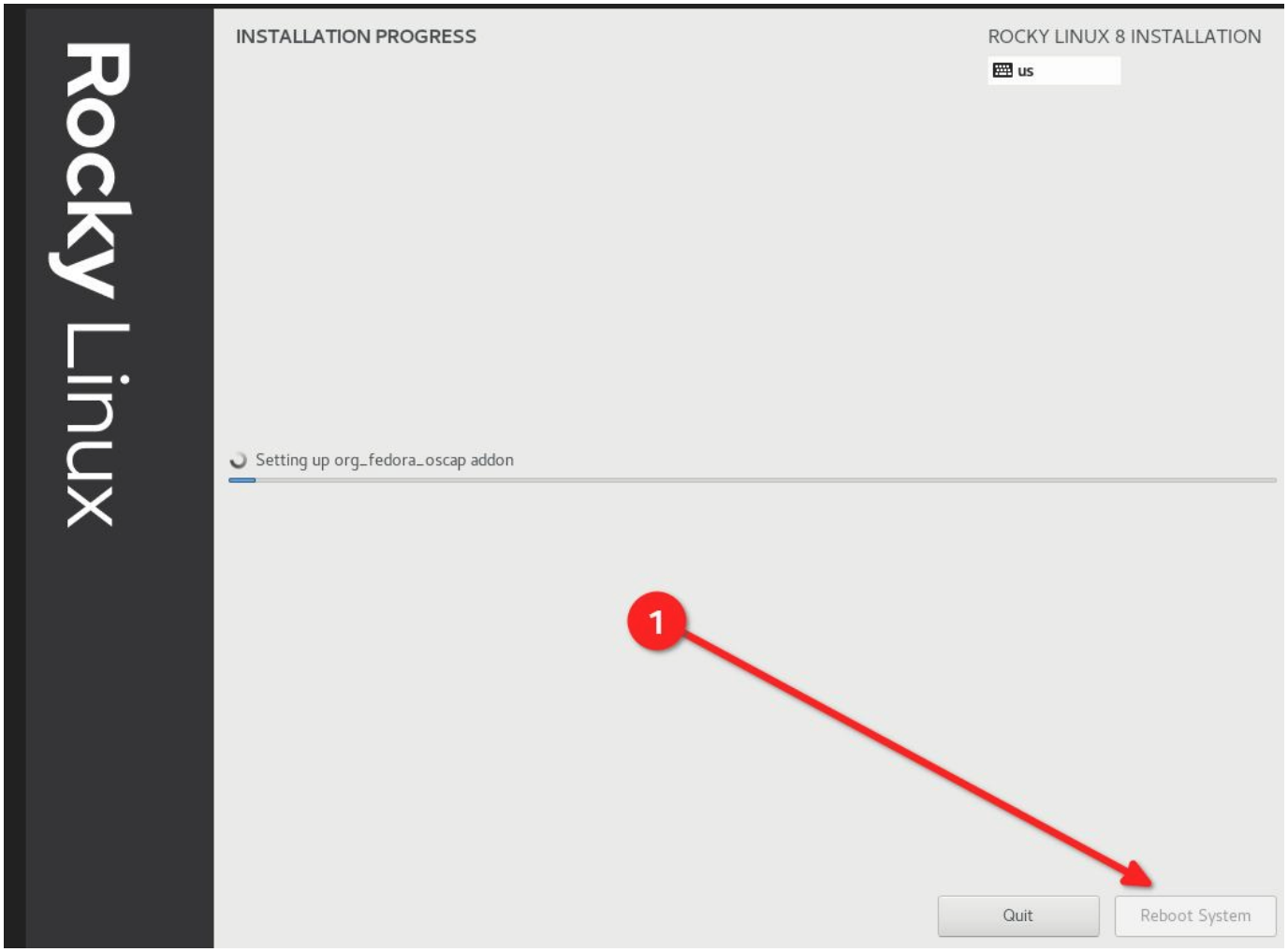
In later tutorials we can get into joining this to a FreeIPA enterprise configuration. For now, we'll treat this as a standalone. Note that I am not setting a root password, rather we give our default user `sudo` access.



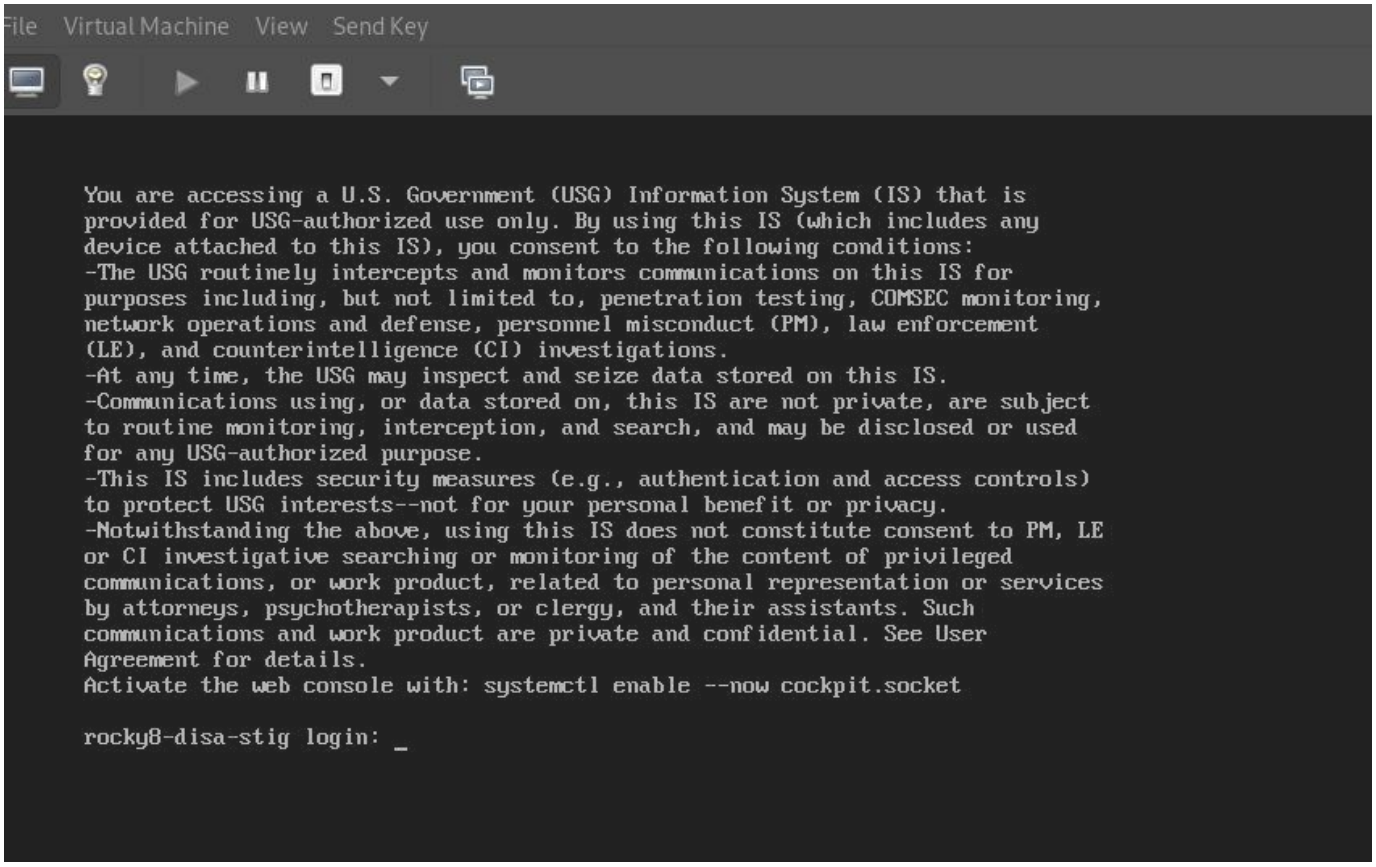
2.2.9 Step 9: Click "Done", and then "Begin Installation"



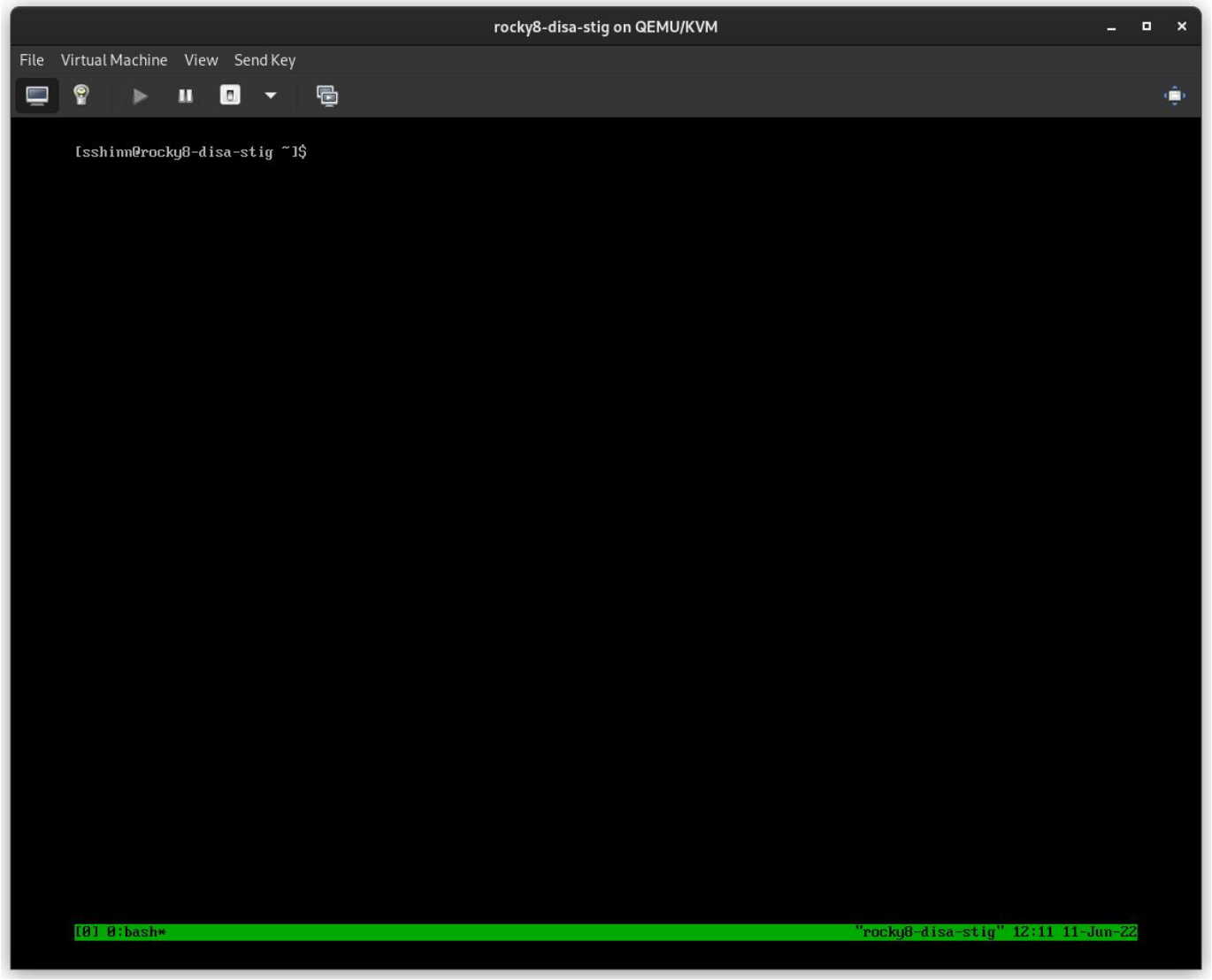
2.2.10 Step 10: Once the installation is completes, click "Reboot System"



2.2.11 Step 11: Log in to your STIG'd Rocky Linux 8 System



If all went well, you should see the default DoD warning banner here.



2.3 About The Author

Scott Shinn is the CTO for Atomicorp, and part of the Rocky Linux Security team. He has been involved with federal information systems at the White House, Department of Defense, and Intelligence Community since 1995. Part of that was creating STIG's and the requirement that you use them and I am so very sorry about that.

3. Introduction

In the last article we set up a new rocky linux 8 system with the DISA stig applied using OpenSCAP. Now we're going to cover how to test the system using those same tools, and look at what kinds of reports we can generate using the tools oscap, and its UI counterpart SCAP Workbench.

Rocky Linux 8 (and 9!) includes a suite of SCAP content to test, and remediate compliance against various standards. If you built a STIG'd system in part 1, you've already seen this in action. The anaconda installer leveraged this content to modify the rocky 8 configuration to implement various controls, install/remove packages, and change the way the OS level mount points work.

Over time, these things could change and you will want to keep an eye on it. Frequently, I also use these reports to show proof that a particular control has been implemented correctly. Either way, its baked in to Rocky. We will begin with some basics.

3.1 List Security Profiles

To list the security profiles available, we need to use the command `oscap info` provided by the `openscap-scanner` package. This should already be installed in your system if you've been following along since Part 1. To obtain the security profiles available:

```
oscap info /usr/share/xml/scap/ssg/content/ssg-rl8-ds.xml
```

> **Note**
>
> Rocky linux 8 content will use the tag "rl8" in the filename. In Rocky 9, it will be "rl9".

If all goes well, you should receive a screen that looks something like this one:

```
sshinn@winona6:~/src/awp-agent/src/awp-agent/active-response — ssh 192.168.122.174
Document type: Source Data Stream
Imported: 2022-04-29T22:32:36

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-rl8-xccdf-1.2.xml
Generated: (null)
Version: 1.3
Checklists:
        Ref-Id: scap_org.open-scap_cref_ssg-rl8-xccdf-1.2.xml
                Status: draft
                Generated: 2022-04-30
                Resolved: true
                Profiles:
                        Title: ANSSI-BP-028 (enhanced)
                                Id: xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced
                        Title: ANSSI-BP-028 (high)
                                Id: xccdf_org.ssgproject.content_profile_anssi_bp28_high
                        Title: ANSSI-BP-028 (intermediary)
                                Id: xccdf_org.ssgproject.content_profile_anssi_bp28_intermediary
                        Title: ANSSI-BP-028 (minimal)
                                Id: xccdf_org.ssgproject.content_profile_anssi_bp28_minimal
                        Title: CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Server
                                Id: xccdf_org.ssgproject.content_profile_cis
                        Title: CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Server
                                Id: xccdf_org.ssgproject.content_profile_cis_server_l1
                        Title: CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Workstation
                                Id: xccdf_org.ssgproject.content_profile_cis_workstation_l1
                        Title: CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Workstation
                                Id: xccdf_org.ssgproject.content_profile_cis_workstation_l2
                        Title: Unclassified Information in Non-federal Information Systems and Organiz
ations (NIST 800-171)
                                Id: xccdf_org.ssgproject.content_profile_cui
                        Title: Australian Cyber Security Centre (ACSC) Essential Eight
                                Id: xccdf_org.ssgproject.content_profile_e8
                        Title: Health Insurance Portability and Accountability Act (HIPAA)
                                Id: xccdf_org.ssgproject.content_profile_hipaa
                        Title: Australian Cyber Security Centre (ACSC) ISM Official
                                Id: xccdf_org.ssgproject.content_profile_ism_o
                        Title: Protection Profile for General Purpose Operating Systems
                                Id: xccdf_org.ssgproject.content_profile_ospp
                        Title: PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8
                                Id: xccdf_org.ssgproject.content_profile_pci-dss
                        Title: DISA STIG for Red Hat Enterprise Linux 8
                                Id: xccdf_org.ssgproject.content_profile_stig
                        Title: DISA STIG with GUI for Red Hat Enterprise Linux 8
                                Id: xccdf_org.ssgproject.content_profile_stig_gui
                Referenced check files:
                        ssg-rl8-oval.xml
                                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
:
[5] 0:bash*                                                "rocky8-disa-stig" 15:02 11-Jun-22
```

DISA is just one of many Security Profiles supported by the Rocky Linux SCAP definitions. We also have profiles for:

- ANSSI
- CIS
- Australian Cyber Security Center
- NIST-800-171
- HIPAA
- PCI-DSS

3.2 Auditing DISA STIG compliance

There are two types to choose from here:

- stig - Without a GUI
- stig_gui - With a GUI

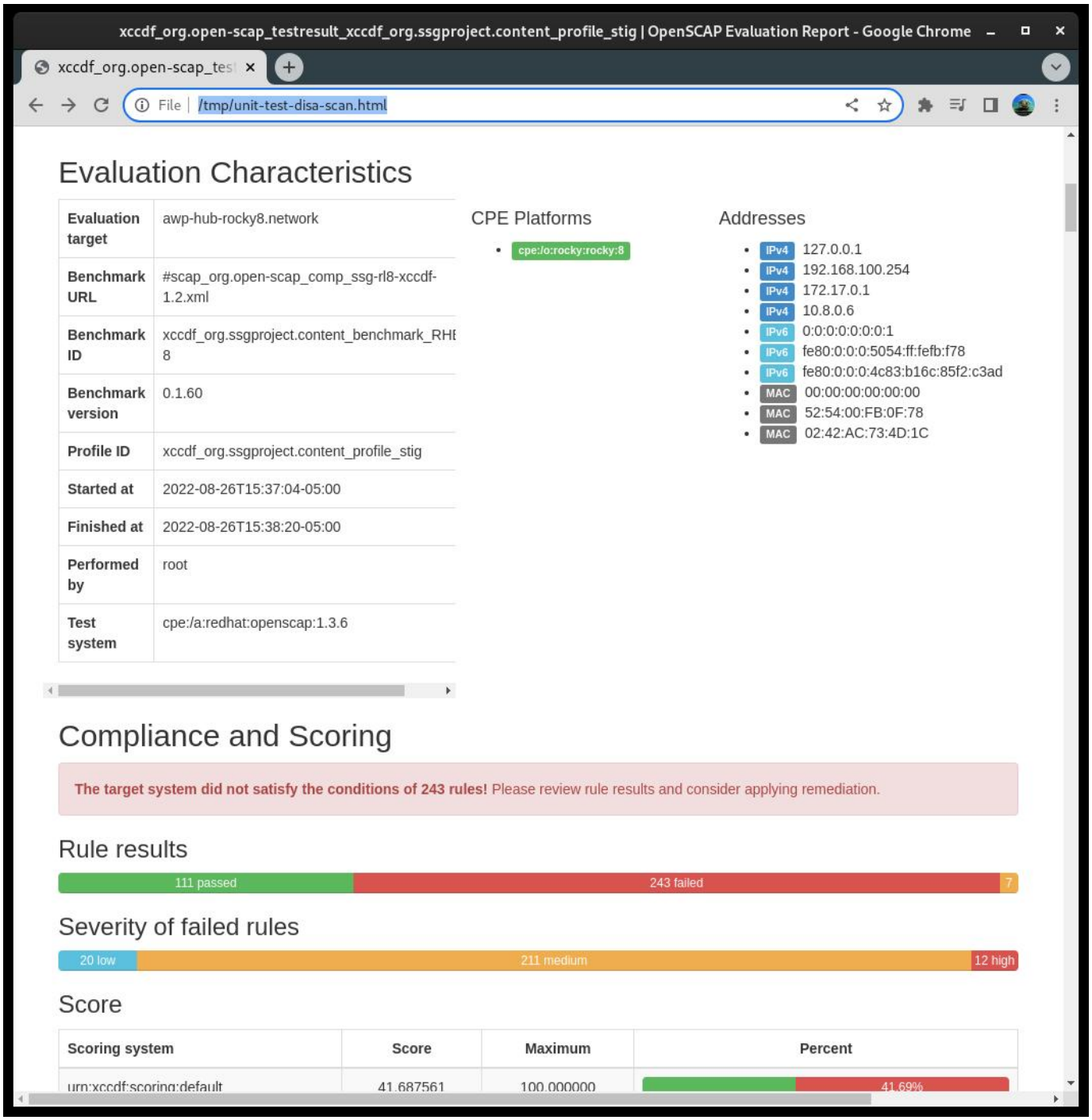
Run a scan and create an HTML report for the DISA STIG:

```
sudo oscap xccdf eval --report unit-test-disa-scan.html --profile stig /usr/
share/xml/scap/ssg/content/ssg-rl8-ds.xml
```

This will result in a report like this:

```
sshinn@winona6:~/src/awp-agent/src/awp-agent/active-response — ssh 192.168.122.174

Result  pass

Title   Verify User Who Owns /var/log Directory
Rule    xccdf_org.ssgproject.content_rule_file_owner_var_log
Result  pass

Title   Verify User Who Owns /var/log/messages File
Rule    xccdf_org.ssgproject.content_rule_file_owner_var_log_messages
Result  pass

Title   Verify Permissions on /var/log Directory
Rule    xccdf_org.ssgproject.content_rule_file_permissions_var_log
Result  pass

Title   Verify Permissions on /var/log/messages File
Rule    xccdf_org.ssgproject.content_rule_file_permissions_var_log_messages
Result  pass

Title   Verify that Shared Library Directories Have Root Group Ownership
Rule    xccdf_org.ssgproject.content_rule_dir_group_ownership_library_dirs
Result  pass

Title   Verify that Shared Library Directories Have Root Ownership
Rule    xccdf_org.ssgproject.content_rule_dir_ownership_library_dirs
Result  pass

Title   Verify that Shared Library Directories Have Restrictive Permissions
Rule    xccdf_org.ssgproject.content_rule_dir_permissions_library_dirs
Result  pass

Title   Verify that system commands files are group owned by root
Rule    xccdf_org.ssgproject.content_rule_file_groupownership_system_commands_dirs
Result  pass

Title   Verify that System Executables Have Root Ownership
Rule    xccdf_org.ssgproject.content_rule_file_ownership_binary_dirs
Result  pass

Title   Verify that Shared Library Files Have Root Ownership
Rule    xccdf_org.ssgproject.content_rule_file_ownership_library_dirs
Result  pass

Title   Verify that System Executables Have Restrictive Permissions
Rule    xccdf_org.ssgproject.content_rule_file_permissions_binary_dirs
Result  pass

Title   Verify that Shared Library Files Have Restrictive Permissions
Rule    xccdf_org.ssgproject.content_rule_file_permissions_library_dirs

[5] 0:sudo*                                    "rocky8-disa-stig" 15:16 11-Jun-22
```

And will output an HTML report:



3.3 Generating Remediation Bash Scripts

Next, we will generate a scan, and then use the results of the scan to generate a bash script to remediate the system based on the DISA stig profile. I do not recommend using automatic remediation, you should always review the changes before actually running them.

1) Generate a scan on the system:

```bash
sudo oscap xccdf eval --results disa-stig-scan.xml --profile stig /usr/share/xml/scap/ssg/content/ssg-rl8-ds.xml
```

2) Use this scan output to generate the script:

```bash
sudo oscap xccdf generate fix --output draft-disa-remediate.sh --profile stig disa-stig-scan.xml
```

The resulting script will include all the changes it would make the system.

> **Warning**
>
> Review this before running it! It will make significant changes to the system.

```
root@awp-hub-rocky8:~/tmp
inactivity_timeout_value='900'


# Check for setting in any of the DConf db directories
# If files contain ibus or distro, ignore them.
# The assignment assumes that individual filenames don't contain :
readarray -t SETTINGSFILES < <(grep -r "\\[org/gnome/desktop/session\\]" "/etc/dconf/db/" | grep -v 'dis
tro\|ibus' | cut -d":" -f1)
DCONFFILE="/etc/dconf/db/local.d/00-security-settings"
DBDIR="/etc/dconf/db/local.d"

mkdir -p "${DBDIR}"

if [ "${#SETTINGSFILES[@]}" -eq 0 ]
then
    [ ! -z ${DCONFFILE} ] || echo "" >> ${DCONFFILE}
    printf '%s\n' "[org/gnome/desktop/session]" >> ${DCONFFILE}
    printf '%s=%s\n' "idle-delay" "uint32 ${inactivity_timeout_value}" >> ${DCONFFILE}
else
    escaped_value="$(sed -e 's/\\/\\\\/g' <<< "uint32 ${inactivity_timeout_value}")"
    if grep -q "^\\s*idle-delay\\s*=" "${SETTINGSFILES[@]}"
    then

        sed -i "s/\\s*idle-delay\\s*=\\s*.*/idle-delay=${escaped_value}/g" "${SETTINGSFILES[@]}"
    else
        sed -i "\\|\\[org/gnome/desktop/session\\]|a\\idle-delay=${escaped_value}" "${SETTINGSFILES[@]}"
    fi
fi

dconf update
# Check for setting in any of the DConf db directories
LOCKFILES=$(grep -r "^/org/gnome/desktop/session/idle-delay$" "/etc/dconf/db/" | grep -v 'distro\|ibus'
| cut -d":" -f1)
LOCKSFOLDER="/etc/dconf/db/local.d/locks"

mkdir -p "${LOCKSFOLDER}"

if [[ -z "${LOCKFILES}" ]]
then
    echo "/org/gnome/desktop/session/idle-delay" >> "/etc/dconf/db/local.d/locks/00-security-settings-lo
ck"
fi

dconf update
                                                                    669,1          1%
```

3.4 Generating Remediation Ansible Playbooks

You can also generate remediation actions in ansible playbook format. Let's repeat the section above, but this time with ansible output:

1) Generate a scan on the system:

```bash
sudo oscap xccdf eval --results disa-stig-scan.xml --profile stig /usr/share/xml/scap/ssg/content/ssg-rl8-ds.xml
```

2) Use this scan output to generate the script:

```bash
sudo oscap xccdf generate fix --fix-type ansible --output draft-disa-remediate.yml --profile stig disa-stig-scan.xml
```

> **Warning**
>
> Again, review this before running it! Do you sense a pattern here? This verification step on all of these procedures is very important!

```
root@awp-hub-rocky8:~/tmp
---
##############################################################################
#
# Ansible Playbook for DISA STIG for Red Hat Enterprise Linux 8
#
# Profile Description:
# This profile contains configuration checks that align to the
# DISA STIG for Red Hat Enterprise Linux 8 V1R5.
# In addition to being applicable to Red Hat Enterprise Linux 8, DISA recognizes this
# configuration baseline as applicable to the operating system tier of
# Red Hat technologies that are based on Red Hat Enterprise Linux 8, 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 8 image
#
# Profile ID:  xccdf_org.ssgproject.content_profile_stig
# Benchmark ID:  xccdf_org.ssgproject.content_benchmark_RHEL-8
# Benchmark Version:  0.1.60
# XCCDF Version:  1.2
#
# This file was generated by OpenSCAP 1.3.6 using:
# $ oscap xccdf generate fix --profile xccdf_org.ssgproject.content_profile_stig --fix-type ansible xccd
f-file.xml
#
# This Ansible Playbook is generated from an OpenSCAP profile without preliminary evaluation.
# It attempts to fix every selected rule, even if the system is already compliant.
#
# How to apply this Ansible Playbook:
# $ ansible-playbook -i "localhost," -c local playbook.yml
# $ ansible-playbook -i "192.168.1.155," playbook.yml
# $ ansible-playbook -i inventory.ini playbook.yml
#
##############################################################################


- hosts: all
  vars:
    var_system_crypto_policy: !!str FIPS
    inactivity_timeout_value: !!str 900
    var_sudo_timestamp_timeout: !!str 0
    login_banner_text: !!str ^(You[\s\n]+are[\s\n]+accessing[\s\n]+a[\s\n]+U\.S\.[\s\n]+Government[\s\n]
@@@
"draft-disa-remediate.yml" 29907L, 1050440C                                    29,1          Top
```

3.5 About The Author

Scott Shinn is the CTO for Atomicorp, and part of the Rocky Linux Security team. He has been involved with federal information systems at the White House, Department of Defense, and Intelligence Community since 1995. Part of that was creating STIG's and the requirement that you use them and I am so very sorry about that.

4. Introduction

In part 1 of this series we covered how to build our web server with the base RHEL8 DISA STIG applied, and in part 2 we learned how to test the STIG compliance with the OpenSCAP tool. Now we're going to actually do something with the system, and build a simple web application and apply the DISA web server STIG: https://www.stigviewer.com/stig/web_server/

First lets compare what we're getting into here, the RHEL 8 DISA STIG is targeted at a very specific platform so the controls are pretty easy to understand in that context, test, and apply. Application STIGs have to be portable across multiple platforms, so the content here is generic in order to work on different linux distributions (RHEL, Ubuntu, SuSE, etc)**. This means that tools like OpenSCAP won't help us audit/remediate the configuration, we're going to have to do this manually. Those STIGs are:

- Apache 2.4 V2R5 - Server; which applies to the web server itself
- Apache 2.4 V2R5 - Site; Which applies to the web application / web site

For our guide, we're going to create a simple web server that does nothing more than serve static content. We can use the changes we make here to make a base image and then use this base image when we build more complex web servers later.

4.1 Apache 2.4 V2R5 Server Quickstart

Before you start, you'll need to refer back to Part 1 and apply the DISA STIG Security profile. Consider this step 0.

1.) Install `apache` and `mod_ssl`

```
dnf install httpd mod_ssl
```

2.) Configuration changes

```
sed -i 's/^\([^#].*\)**/# \1/g' /etc/httpd/conf.d/welcome.conf
dnf -y remove httpd-manual
```

```
dnf -y install mod_session

echo “MaxKeepAliveRequests 100” > /etc/httpd/conf.d/disa-apache-stig.conf
echo “SessionCookieName session path=/; HttpOnly; Secure;” >>  /etc/httpd/
conf.d/disa-apache-stig.conf
echo “Session On” >>  /etc/httpd/conf.d/disa-apache-stig.conf
echo “SessionMaxAge 600” >>  /etc/httpd/conf.d/disa-apache-stig.conf
echo “SessionCryptoCipher aes256” >>  /etc/httpd/conf.d/disa-apache-stig.conf
echo “Timeout 10” >>  /etc/httpd/conf.d/disa-apache-stig.conf
echo “TraceEnable Off” >>  /etc/httpd/conf.d/disa-apache-stig.conf
echo “RequestReadTimeout 120” >> /etc/httpd/conf.d/disa-apache-stig.conf

sed -i “s/^#LoadModule usertrack_module/LoadModule usertrack_module/g” /etc/
httpd/conf.modules.d/00-optional.conf
sed -i "s/proxy_module/#proxy_module/g" /etc/httpd/conf.modules.d/00-proxy.conf
sed -i "s/proxy_ajp_module/#proxy_ajp_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_balancer_module/#proxy_balancer_module/g" /etc/httpd/
conf.modules.d/00-proxy.conf
sed -i "s/proxy_ftp_module/#proxy_ftp_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_http_module/#proxy_http_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_connect_module/#proxy_connect_module/g" /etc/httpd/
conf.modules.d/00-proxy.conf
```

3.) Update Firewall policy and start `httpd`

```
firewall-cmd --zone=public --add-service=https --permanent
firewall-cmd --zone=public --add-service=https
firewall-cmd --reload
systemctl enable httpd
systemctl start httpd
```

4.2 Detail Controls Overview

If you’ve gotten this far, you’re probably interested in knowing more about what the STIG wants us to do. It helps to understand the importance of the control, and then how it applies to the application. Sometimes the control is technical (change X setting to Y) and other times it's operational (how you use it). Generally speaking, a technical control is something you can change with code, and an operational control probably isn’t.

4.2.1 Levels

- Cat I - (HIGH) - 5 Controls
- Cat II - (MEDIUM) - 41 Controls
- Cat III - (LOW) - 1 Controls

4.2.2 Types

- Technical - 24 controls
- Operational - 23 controls

We’re not going to cover the “why” for these changes in this article, just what needs to happen if it is a technical control. If there is nothing we can change like in the case of an Operational control, the **Fix:** field will be none. The good news in a lot of these cases, this is already the default in Rocky Linux 8, so you don’t need to change anything at all.

4.3 Apache 2.4 V2R5 - Server Details

(V-214248) Apache web server application directories, libraries, and configuration files must only be accessible to privileged users.

Severity: Cat I High
Type: Operational
Fix: None, check to make sure only privileged users can access webserver files

(V-214242) The Apache web server must provide install options to exclude the installation of documentation, sample code, example applications, and tutorials.

Severity: Cat I High
Type: Technical
Fix:

```
sed -i 's/^\([^#].*\)/# \1/g' /etc/httpd/conf.d/welcome.conf
```

(V-214253) The Apache web server must generate a session ID using as much of the character set as possible to reduce the risk of brute force.

Severity: Cat I High
Type: Technical
Fix: None, Fixed by default in Rocky Linux 8

(V-214273) The Apache web server software must be a vendor-supported version.

Severity: Cat I High
Type: Technical
Fix: None, Fixed by default in Rocky Linux 8

(V-214271) The account used to run the Apache web server must not have a valid login shell and password defined.

Severity: Cat I High
Type: Technical
Fix: None, Fixed by default in Rocky Linux 8

(V-214245) The Apache web server must have Web Distributed Authoring (WebDAV) disabled. **Severity:** Cat II Medium **Type:** Technical **Fix:**

```
sed -i 's/^\([^#].*\)/# \1/g' /etc/httpd/conf.d/welcome.conf
```

(V-214264) The Apache web server must be configured to integrate with an organization's security infrastructure.

Severity: Cat II Medium **Type:** Operational **Fix:** None, forward web server logs to SIEM

(V-214243) The Apache web server must have resource mappings set to disable the serving of certain file types.

Severity: Cat II Medium **Type:** Technical **Fix:** None, Fixed by default in Rocky Linux 8

(V-214240) The Apache web server must only contain services and functions necessary for operation.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
dnf remove httpd-manual
```

(V-214238) Expansion modules must be fully reviewed, tested, and signed before they can exist on a production Apache web server.

Severity: Cat II Medium **Type:** Operational **Fix:** None, disable all modules not required for the application

(V-214268) Cookies exchanged between the Apache web server and the client, such as session cookies, must have cookie properties set to prohibit client-side scripts from reading the cookie data.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
dnf install mod_session
echo “SessionCookieName session path=/; HttpOnly; Secure;” >>  /etc/httpd/
conf.d/disa-apache-stig.conf
```

(V-214269) The Apache web server must remove all export ciphers to protect the confidentiality and integrity of transmitted information.

Severity: Cat II Medium **Type:** Technical **Fix:** None, Fixed by default in Rocky Linux 8 DISA STIG security Profile

(V-214260) The Apache web server must be configured to immediately disconnect or disable remote access to the hosted applications.

Severity: Cat II Medium **Type:** Operational **Fix:** None, this is a procedure to stop the web server

(V-214249) The Apache web server must separate the hosted applications from hosted Apache web server management functionality.

Severity: Cat II Medium **Type:** Operational **Fix:** None, this is related to the web applications rather than the server

(V-214246) The Apache web server must be configured to use a specified IP address and port.

Severity: Cat II Medium **Type:** Operational **Fix:** None, the web server should be configured to only listen on a specific IP / port

(V-214247) Apache web server accounts accessing the directory tree, the shell, or other operating system functions and utilities must only be administrative accounts.

Severity: Cat II Medium **Type:** Operational **Fix:** None, all files, and directories served by the web server need to be owned by administrative users, and not the web server user.

(V-214244) The Apache web server must allow the mappings to unused and vulnerable scripts to be removed.

Severity: Cat II Medium **Type:** Operational **Fix:** None, any cgi-bin or other Script/ScriptAlias mappings that are not used must be removed

(V-214263) The Apache web server must not impede the ability to write specified log record content to an audit log server.

Severity: Cat II Medium **Type:** Operational **Fix:** None, Work with the SIEM administrator to allow the ability to write specified log record content to an audit log server.

(V-214228) The Apache web server must limit the number of allowed simultaneous session requests.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
echo “MaxKeepAliveRequests 100” > /etc/httpd/conf.d/disa-apache-stig.conf
```

(V-214229) The Apache web server must perform server-side session management.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
sed -i “s/^#LoadModule usertrack_module/LoadModule usertrack_module/g” /etc/
httpd/conf.modules.d/00-optional.conf
```

(V-214266) The Apache web server must prohibit or restrict the use of nonsecure or unnecessary ports, protocols, modules, and/or services.

Severity: Cat II Medium **Type:** Operational **Fix:** None, Ensure the website enforces the use of IANA well-known ports for HTTP and HTTPS.

(V-214241) The Apache web server must not be a proxy server.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
sed -i "s/proxy_module/#proxy_module/g" /etc/httpd/conf.modules.d/00-proxy.conf
sed -i "s/proxy_ajp_module/#proxy_ajp_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_balancer_module/#proxy_balancer_module/g" /etc/httpd/
conf.modules.d/00-proxy.conf
sed -i "s/proxy_ftp_module/#proxy_ftp_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_http_module/#proxy_http_module/g" /etc/httpd/conf.modules.d/00-
proxy.conf
sed -i "s/proxy_connect_module/#proxy_connect_module/g" /etc/httpd/
conf.modules.d/00-proxy.conf
```

(V-214265) The Apache web server must generate log records that can be mapped to Coordinated Universal Time (UTC)** or Greenwich Mean Time (GMT) which are stamped at a minimum granularity of one second.

Severity: Cat II Medium **Type:** Technical **Fix:** None, Fixed by default in Rocky Linux 8

(V-214256) Warning and error messages displayed to clients must be modified to minimize the identity of the Apache web server, patches, loaded modules, and directory paths.

Severity: Cat II Medium **Type:** Operational **Fix:** Use the "ErrorDocument" directive to enable custom error pages for 4xx or 5xx HTTP status codes.

(V-214237) The log data and records from the Apache web server must be backed up onto a different system or media.

Severity: Cat II Medium **Type:** Operational **Fix:** None, document the web server backup procedures

(V-214236) The log information from the Apache web server must be protected from unauthorized modification or deletion.

Severity: Cat II Medium **Type:** Operational **Fix:** None, document the web server backup procedures

(V-214261) Non-privileged accounts on the hosting system must only access Apache web server security-relevant information and functions through a distinct administrative account. **Severity:** Cat II Medium **Type:** Operational **Fix:** None, Restrict access to the web administration tool to only the System Administrator, Web Manager, or the Web Manager designees.

(V-214235) The Apache web server log files must only be accessible by privileged users.

Severity: Cat II Medium **Type:** Operational **Fix:** None, To protect the integrity of the data that is being captured in the log files, ensure that only the members of the Auditors group, Administrators, and the user assigned to run the web server software is granted permissions to read the log files.

(V-214234) The Apache web server must use a logging mechanism that is configured to alert the Information System Security Officer (ISSO) and System Administrator (SA) in the event of a processing failure.

Severity: Cat II Medium **Type:** Operational **Fix:** None, Work with the SIEM administrator to configure an alert when no audit data is received from Apache based on the defined schedule of connections.

(V-214233) An Apache web server, behind a load balancer or proxy server, must produce log records containing the client IP information as the source and destination and not the load balancer or proxy IP information with each event.

Severity: Cat II Medium **Type:** Operational **Fix:** None, Access the proxy server through which inbound web traffic is passed and configure settings to pass web traffic to the Apache web server transparently.

Refer to https://httpd.apache.org/docs/2.4/mod/mod_remoteip.html for additional information on logging options based on your proxy/load balancing setup.

(V-214231) The Apache web server must have system logging enabled.

Severity: Cat II Medium **Type:** Technical **Fix:** None, Fixed by default in Rocky Linux 8

(V-214232) The Apache web server must generate, at a minimum, log records for system startup and shutdown, system access, and system authentication events.

Severity: Cat II Medium **Type:** Technical **Fix:** None, Fixed by default in Rocky Linux 8

V-214251 Cookies exchanged between the Apache web server and client, such as session cookies, must have security settings that disallow cookie access outside the originating Apache web server and hosted application.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
echo “Session On” >>  /etc/httpd/conf.d/disa-apache-stig.conf
```

(V-214250) The Apache web server must invalidate session identifiers upon hosted application user logout or other session termination.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
echo “SessionMaxAge 600” >>  /etc/httpd/conf.d/disa-apache-stig.conf
```

(V-214252) The Apache web server must generate a session ID long enough that it cannot be guessed through brute force.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
echo “SessionCryptoCipher aes256” >>  /etc/httpd/conf.d/disa-apache-stig.conf
```

(V-214255) The Apache web server must be tuned to handle the operational requirements of the hosted application.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
echo “Timeout 10” >>  /etc/httpd/conf.d/disa-apache-stig.conf
```

(V-214254) The Apache web server must be built to fail to a known safe state if system initialization fails, shutdown fails, or aborts fail.

Severity: Cat II Medium **Type:** Operational **Fix:** None, Prepare documentation for disaster recovery methods for the Apache 2.4 web server in the event of the necessity for rollback.

(V-214257) Debugging and trace information used to diagnose the Apache web server must be disabled.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
echo “TraceEnable Off” >>  /etc/httpd/conf.d/disa-apache-stig.conf
```

(V-214230) The Apache web server must use cryptography to protect the integrity of remote sessions.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
sed -i "s/^#SSLProtocol.*/SSLProtocol -ALL +TLSv1.2/g" /etc/httpd/conf.d/
ssl.conf
```

(V-214258) The Apache web server must set an inactive timeout for sessions.

Severity: Cat II Medium **Type:** Technical **Fix:**

```
echo “RequestReadTimeout 120” >> /etc/httpd/conf.d/disa-stig-apache.conf
```

(V-214270) The Apache web server must install security-relevant software updates within the configured time period directed by an authoritative source (e.g., IAVM, CTOs, DTMs, and STIGs).

Severity: Cat II Medium **Type:** Operational **Fix:** None, Install the current version of the web server software and maintain appropriate service packs and patches.

(V-214239) The Apache web server must not perform user management for hosted applications.

Severity: Cat II Medium **Type:** Technical **Fix:** None, Fixed by default in Rocky Linux 8

(V-214274) The Apache web server htpasswd files (if present) must reflect proper ownership and permissions.

Severity: Cat II Medium **Type:** Operational **Fix:** None, Ensure the SA or Web Manager account owns the "htpasswd" file. Ensure permissions are set to "550".

(V-214259) The Apache web server must restrict inbound connections from nonsecure zones.

Severity: Cat II Medium **Type:** Operational **Fix:** None, Configure the "http.conf" file to include restrictions. Example:

```
Require not ip 192.168.205
Require not host phishers.example.com
```

(V-214267) The Apache web server must be protected from being stopped by a non-privileged user.

Severity: Cat II Medium **Type:** Technical **Fix:** None, Fixed by Rocky Linux 8 by default

(V-214262) The Apache web server must use a logging mechanism that is configured to allocate log record storage capacity large enough to accommodate the logging requirements of the Apache web server.

Severity: Cat II Medium **Type:** Operational **Fix:** none, Work with the SIEM administrator to determine if the SIEM is configured to allocate log record storage capacity large enough to accommodate the logging requirements of the Apache web server.

(V-214272) The Apache web server must be configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including STIGs, NSA configuration guides, CTOs, and DTMs.

Severity: Cat III Low **Type:** Operational **Fix:** None

4.4 About The Author

Scott Shinn is the CTO for Atomicorp, and part of the Rocky Linux Security team. He has been involved with federal information systems at the White House, Department of Defense, and Intelligence Community since 1995. Part of that was

creating STIG’s and the requirement th at you use them and I am so very sorry about that.

https://docs.rockylinux.org/