Hardened Repository ISO “Community Preview”

Contents

Community Preview disclaimer

This community preview is provided to gather direct customer feedback, but it comes without any support. We plan to release a "beta 1" later that will have "experimental support" and update capabilities.

All communication / feedback is handled via the R&D forums and not via support!

The text below mentions "support" multiple times. That is a preview for what customers can expect for later builds.

Overview

The Hardened Repository ISO simplifies the installation of a DISA STIG hardened Rocky Linux as a Veeam Hardened Repository. Veeam also supports the Rocky Linux operating system itself with the Hardened Repository ISO.

To get support for the operating system, customers must use the unmodified Hardened Repository ISO and meet the system requirements. Any unauthorized modification to the configuration of the operating system / software or installation of 3rd party software will result in the operating system no longer being supported on that installation.

Security

The Hardened Repository ISO applies the DISA STIG security profile. That implies strict password settings, application whitelisting, UEFI secure boot, etc. There are no network services listening after the installation (not even SSH).

There are two users on the system:

1) The user "veeamsvc" which runs Veeam Backup & Replication services (implemented directly in the ISO, no configuration). Password is generated on demand with the Hardened Repository Configurator.
2) The "vhradmin" user. (implemented directly in the ISO, no configuration).

The user "veeamsvc" has sudo permissions to install the Veeam Backup & Replication software & services. The user "vhradmin" has no sudo permissions and can only run the Hardened Repository Configurator to do configuration and maintenance tasks. The default password of "vhradmin" is "vhradmin" and password change is enforced during first login.

Everyone with access to the hardware (whether physically or via remote connection via base management controller, BMC) can bypass all operating system security. Customers are responsible to ensure physical security.

Security and operating system updates

Security and operating system updates are installed automatically and provided by Veeam. The Hardened Repository installs them from repository.veeam.com and must have access to that server to obtain security and operating system updates (HTTP / HTTPS proxies are supported).

If access to Veeam update servers is blocked, then GPG keys will expire at some point in time. If the GPG keys expired, then updates won't be possible anymore and re-installation of the system is needed.

The ISO installs updates automatically at 8am of the configured time zone but does not do automatic reboots. There is also no notification about required reboot (that is a limitation of the beta that will be improved in future versions)

Hardware

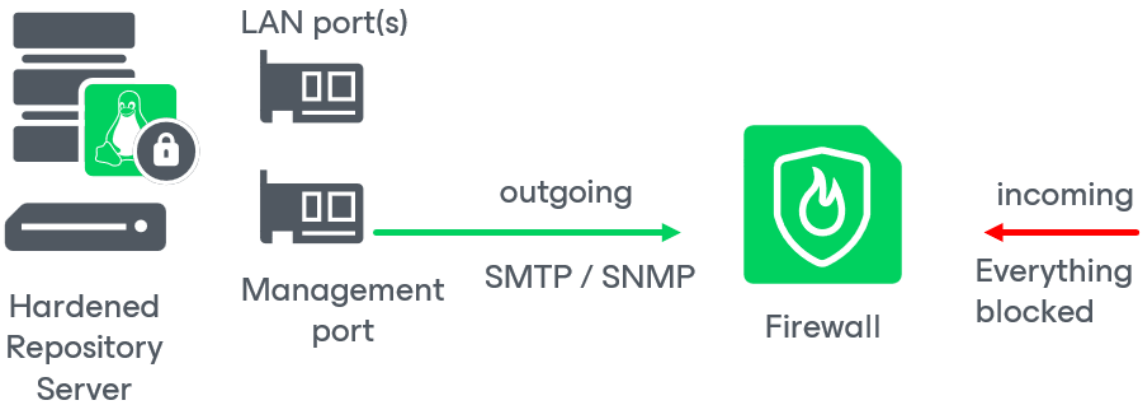
It is recommended to only use physical machines for Hardened Repository in general. Virtual machines have a higher security risk because an attacker could get access to the virtualization platform and delete the entire Hardened Repository machine.

Hardware Monitoring

Hardware monitoring is the responsibility of the customer. The Hardened Repository ISO and Veeam Backup & Replication itself has no built-in hardware monitoring as of now.

Modern servers have base management controllers (BMCs) that can notify via email or an SNMP trap about failed hardware (power supplies, disks, high temperature etc.). Please check the options with the hardware vendor.

For security reasons, the BMC ports should be firewalled because everyone with full access to the BMC can delete the entire server.



Planning & Preparation

System Requirements

- Veeam Backup & Replication must be at least version 12.2.
- Hardware must be on Red Hat compatibility list:
  - https://catalog.redhat.com/hardware
- Same CPU & RAM resources as Linux Repositories:
  - https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=120#backup-repository
- Storage: Must be at least two volumes (disks)
  - Minimum 100GB for operating system
  - Larger disk(s) for data
- Only hardware RAID controllers are supported (software RAID / FakeRAID controllers are unsupported)
- Only internal storage / direct attached storage with hardware RAID controller with write-back cache are supported.
- UEFI secure boot must be enabled in the server UEFI (BIOS) settings.
- Network:
  - 1 Gbit/s minimum
  - 10Gbit/s and faster recommended.
  - Redundant network connection recommended.
  - WIFI is unsupported.
- Internet connection to repository.veeam.com for security updates (direct or via HTTP / HTTPS proxy)

Storage

All storage configurations must be done before installing the Hardened Repository ISO. Direct attached drives are supported (these are drives internal to the server). Hard disk drives or flash drives can be used. iSCSI or Fibre Channel LUNs provisioned to the server are not supported.

Hardware RAID controllers with write-back cache are required. Only the configured RAIDs must be visible to the operating system. The disks itself must not be visible to the operating system (software RAID controllers/ FakeRAID are unsupported).

There are different ways how storage can be presented to the Hardened Repository ISO. Here some examples:

1. Two drives for the operating system in RAID 1 and all other drives in a dual-parity or better RAID (RAID6, RAID60, RAID10 etc.)
2. All drives are managed as one RAID-set by the RAID controller and the RAID controller creates LUNs (logical units) from the RAID-set (not every RAID controller can do this). For example, one may use a 200 GB LUN for the operating system and 500 TB LUN for the data; the Hardened Repository ISO Installer will then see two volumes available: one with 200 GB, and one with 500 TB

It is strongly recommended to use at least dual parity so that two drives can fail. Rebuild-times with large drives can be long and the risk of a second drive failing during rebuild is significant.

The server must have at least two volumes (disks). The smallest (minimum 100GB) is used for the operating system. All other disks are added to a logical volume group with LVM (Logical Volume Manager).

Other hardware components

- Redundant power supplies are recommended.
- Redundant network connection is recommended.

Ports

- same as Hardened Repository from main user guide.
- additionally: HTTPS (HTTP also works) connection to repository.veeam.com (TBD) for operating system updates

Known limitations

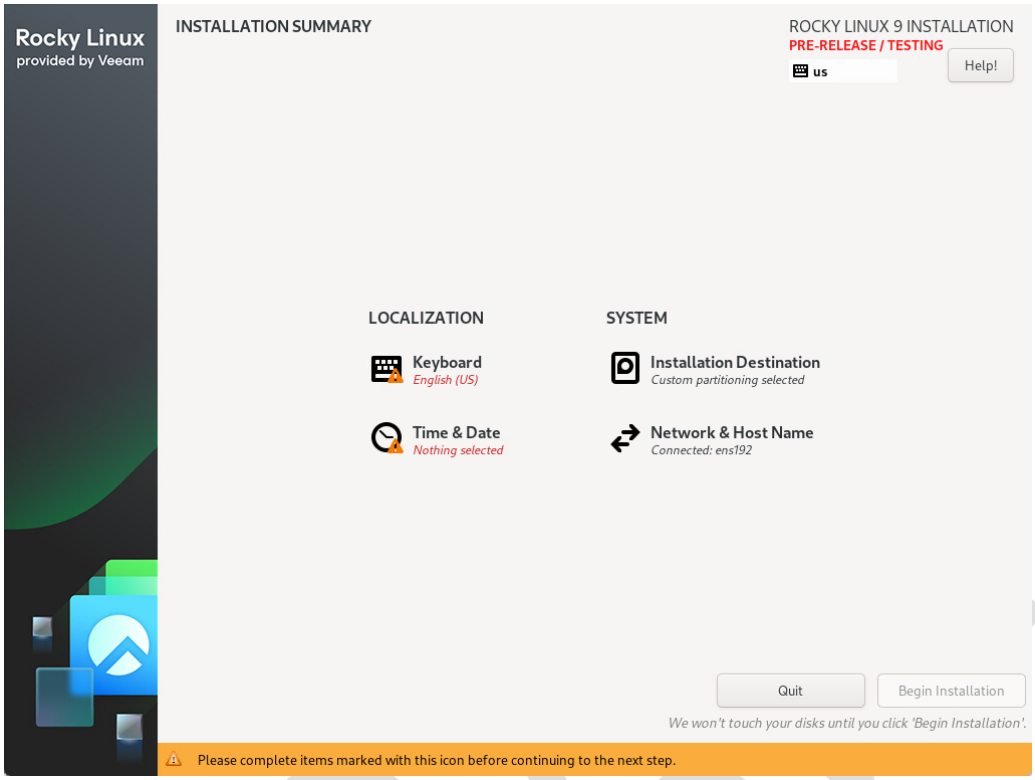
- There is no notification if a reboot is needed due to security updates
- Beta 1 does not have a “repair mode”. That means if the operating system disk is lost (e.g. RAID failure), then there is no option to only re-install the operating system and keep all data.

Installation

The Veeam Hardened Repository ISO is delivered as bootable ISO. The ISO needs to be connected to the physical machine to install. That can be done via remote consoles (virtual CD-ROM, remote images etc.) or by creating a bootable USB stick from the ISO.

When the ISO booted, select “Install Hardened Repository (deletes all data). It’s the only option in beta 1.

After a few minutes (depending on the performance of the remote media), the installer shows a screen like this. It is required to configure Keyboard and Time & Date. Network & Host Name configuration is recommended, but not enforced by the installer in beta 1.

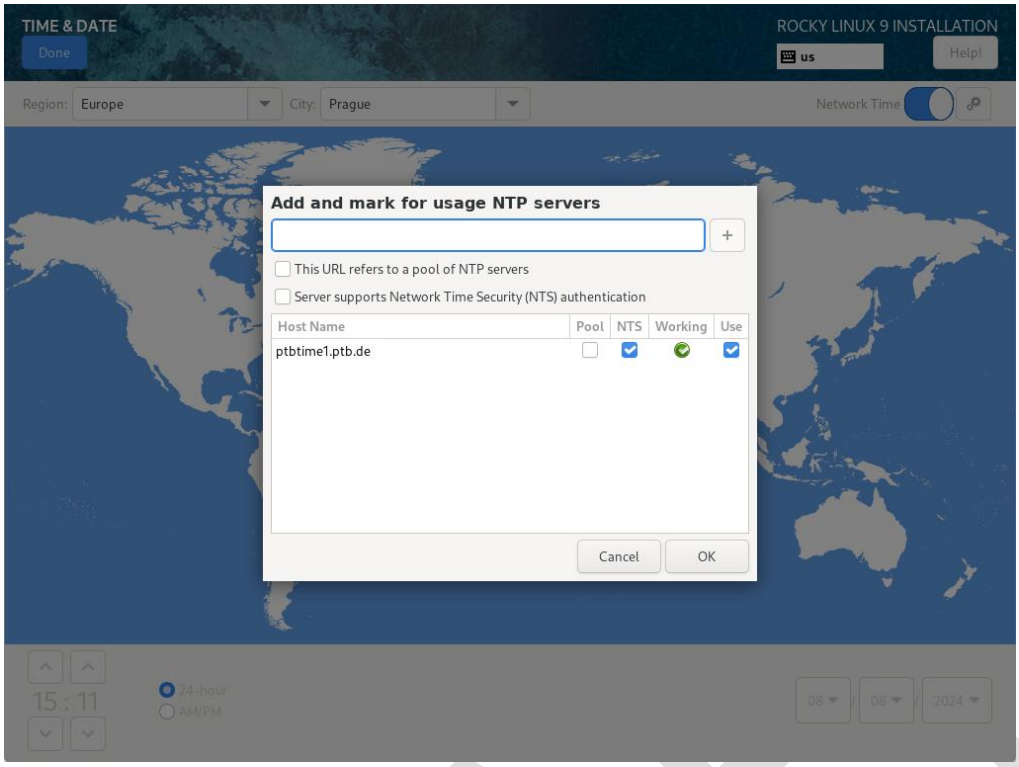


Keyboard

Select your preferred keyboard. This is important because DISA STIG password compliance is enforced.

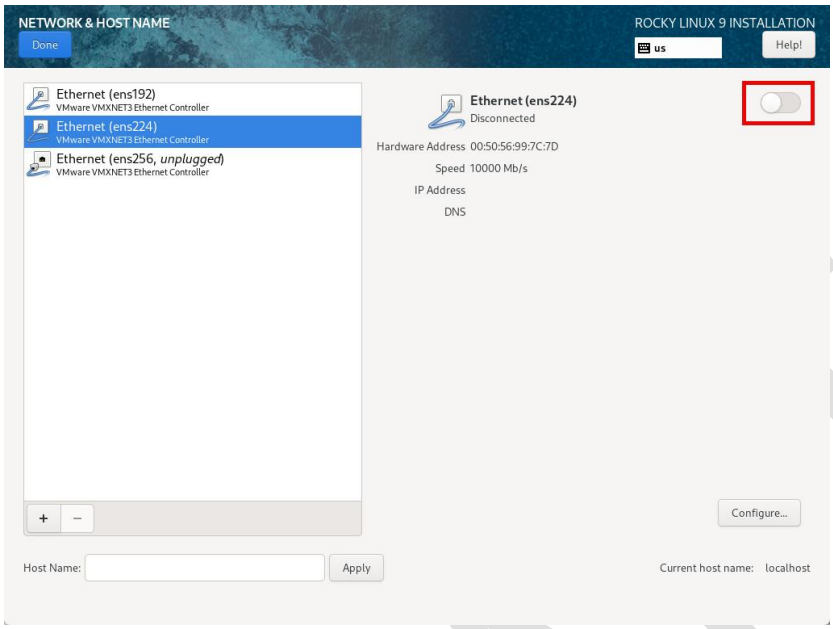
Time and date settings

If you use NTS time servers, then they must be configured during setup. The Hardened Repository Configurator only supports NTP time server configuration as of today.


TIME & DATE
Done
ROCKY LINUX 9 INSTALLATION
us
Help!
Region: Europe
City: Prague
Network Time
Add and mark for usage NTP servers
This URL refers to a pool of NTP servers
Server supports Network Time Security (NTS) authentication
Host Name
Pool
NTS
Working
Use
ptbtime1.ptb.de
Cancel
OK
15 : 11
24-hour
AM/PM
08
08
2024

Network

Static IP addresses are recommended to avoid problems if the DHCP server fails. Only the first network card is enabled per default. If multiple network cards are available, enable the ones that should be used.

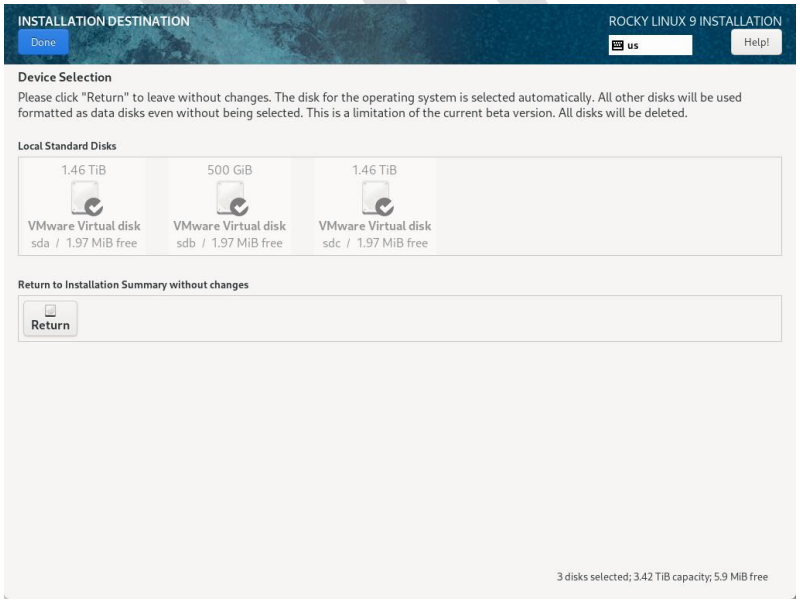


Installation destination (partitioning)

You can click into “Installation Destination”, but you cannot change anything here. The only option is to exit the wizard with “Return”.

The automatic partitioning does the following:

- The smallest disk (volume) is used for the operating system
- All other disks (volumes) are put together in one logical volume and mounted to /mnt/veeam-repository01 (LVM is used in the background)



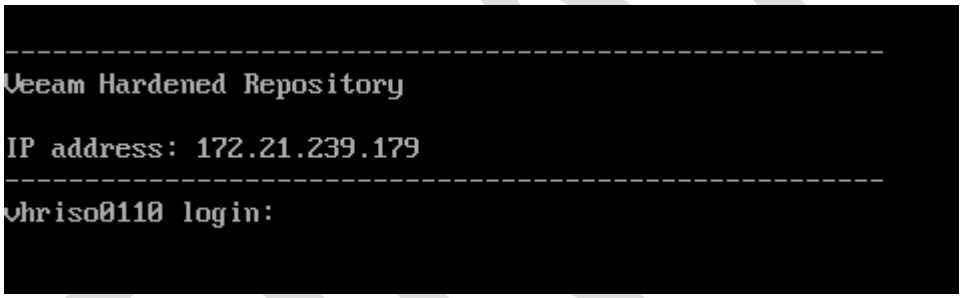
Repairing the system – not in community preview / beta 1

~~In the unlikely case, that the operating system fails and is not boot able anymore (e.g., both operating system disks failed) one can repair the system by re-installing only the operating system and keeping the data. Select the "Repair…" option in the boot menu.~~

First login

Log into the system with vhradmin / vhradmin. During first login, a password change is enforced. The new password must meet DISA STIG complexity requirements. DISA STIG password requirements are the following:

- 1 numeric character
- 1 lower case
- 15 characters
- 1 special character
- Maximum 4 characters of the same character class in a row (e.g. 4 lower case, 4 numbers etc.)
- 24h minimum lifetime of password (that means you can change a password only once per day)

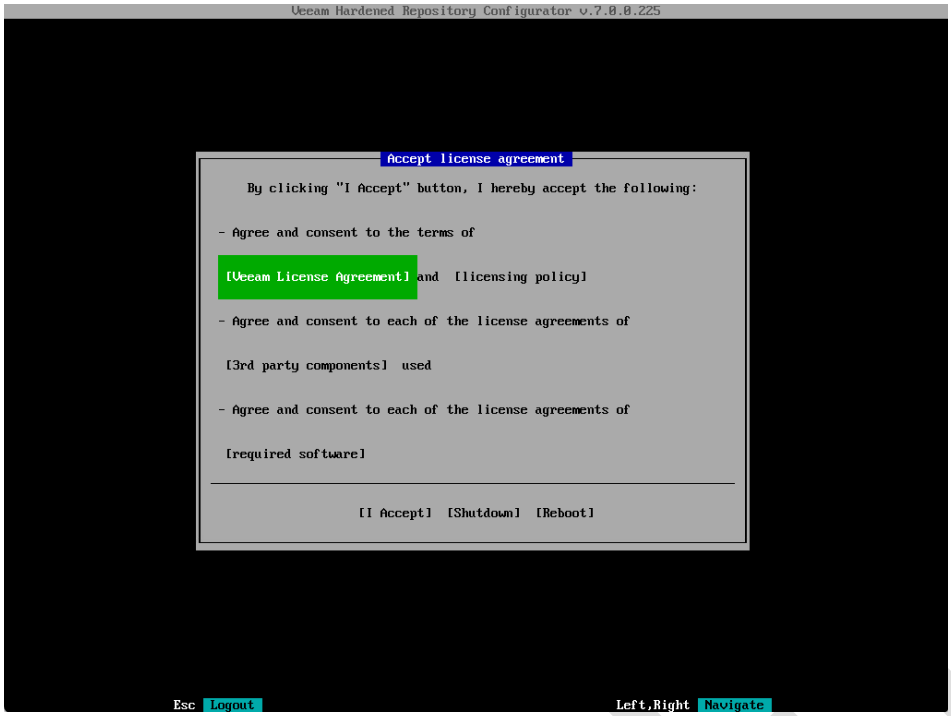


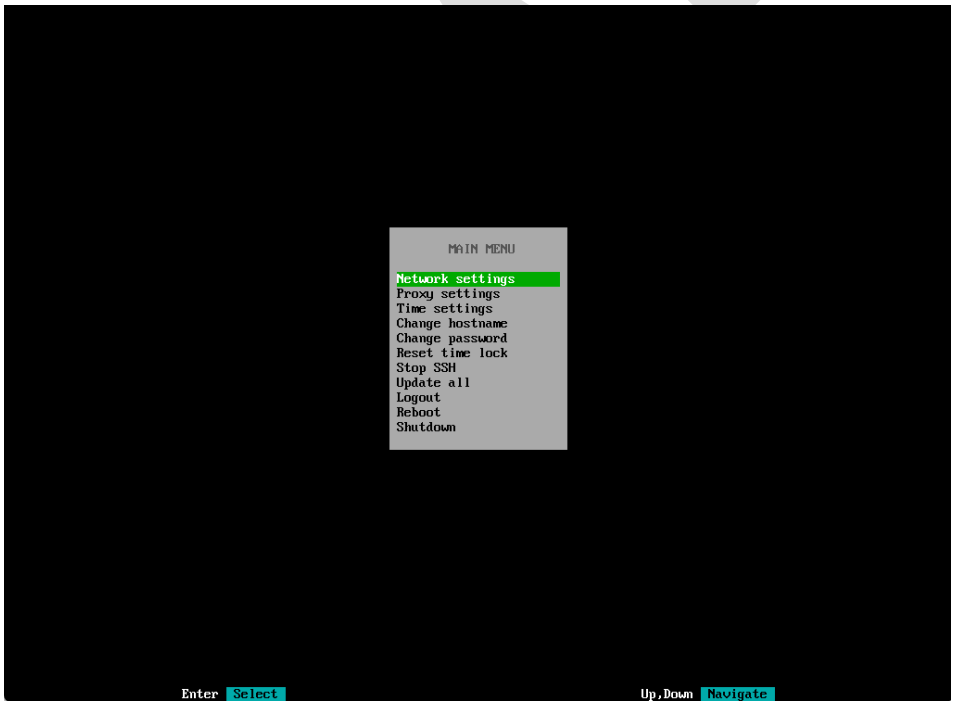
Configuration

To configure the Hardened Repository server, log in with the vhradmin credentials (default password is "vhradmin"). Automatic logout from the Hardened Repository Configurator happens after 10min if there is no user input.

NOTE: due to DISA STIG security requirements, the account gets locked permanently after three failed login attempts. KB4663 describes how to unlock a locked account

Once logged in, the Hardened Repository Configurator shows up which allows configuration of the system. At the first start, the license agreements need to be accepted (license agreements & EULA are empty in the Community Preview / Beta 1).





Network settings

Hopefully self-explaining.

Proxy settings

Hopefully self-explaining

Time settings

Hopefully self-explaining

Change hostname

Hopefully self-explaining

Change password

Hopefully self-explaining. Beware that error messages are not perfect yet. You must ensure to meet DISA STIG password complexity compliance. A compliant password is for example: Summ3er!Wint3r

Reset time lock

https://www.veeam.com/kb4482

Start SSH

SSH is required to install the Hardened Repository Role. It generates a password that is shown in the console. Use the credentials to add the Hardened Repository machine to Veeam Backup & Replication

Reboot

Hopefully self-explaining

Shutdown

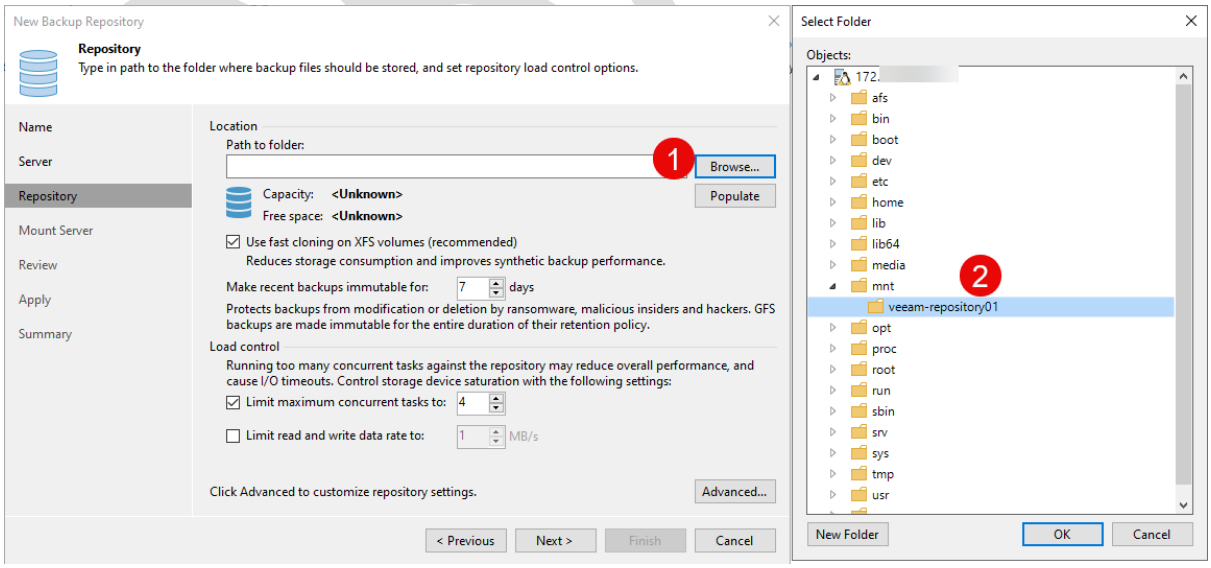
Hopefully self-explaining

Connecting Veeam Backup & Replication

Veeam Backup & Replication must be at least version 12.2. Per default, the SSH service is stopped. Start the SSH service in the Hardened Repository Configurator and follow the regular instructions

Select /mnt/veeam-repository01 for data storage.

After the installation finished, stop the SSH service again.



Known Issues

Known issues installation ISO

- sudo permissions for the veeamsvc user allow to install packages that are signed by trusted key. Improvements are planned.
- The “help” button does not show anything right now.
- Only the first network adapter is connected per default. Additional adapters can be enabled manually.

Known issues Hardened Repository Configurator

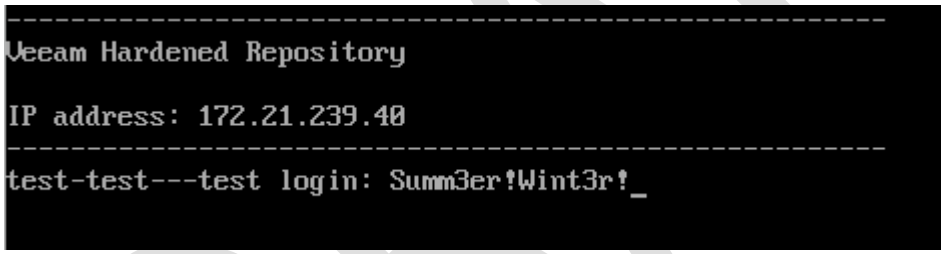
- License Agreement wizard and files are incomplete.
- Text and error messages are not finalized.

Troubleshooting

Unable to log in (for the first time)

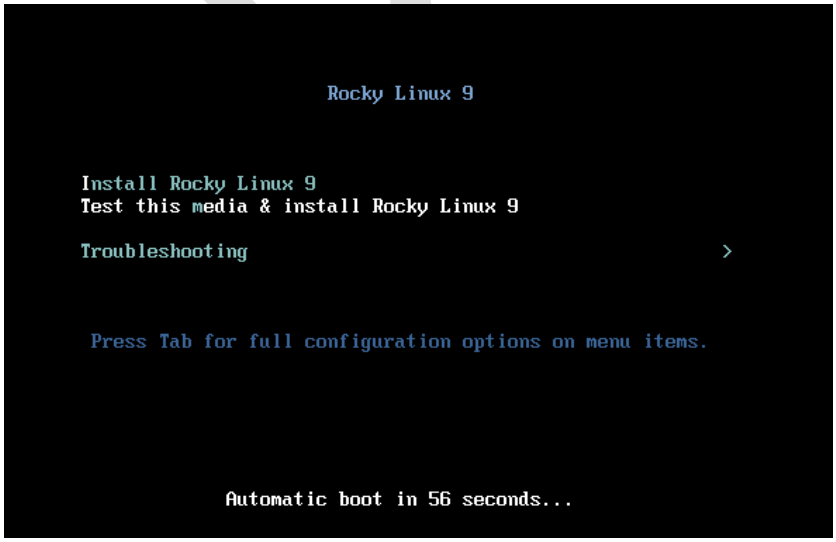
First: please remember that DISA STIG security profile locks an account forever after three failed login attempts

If you are unable to log in, testing the password in the username field helps to detect misconfigured keyboard settings. The screenshot below shows a valid password:



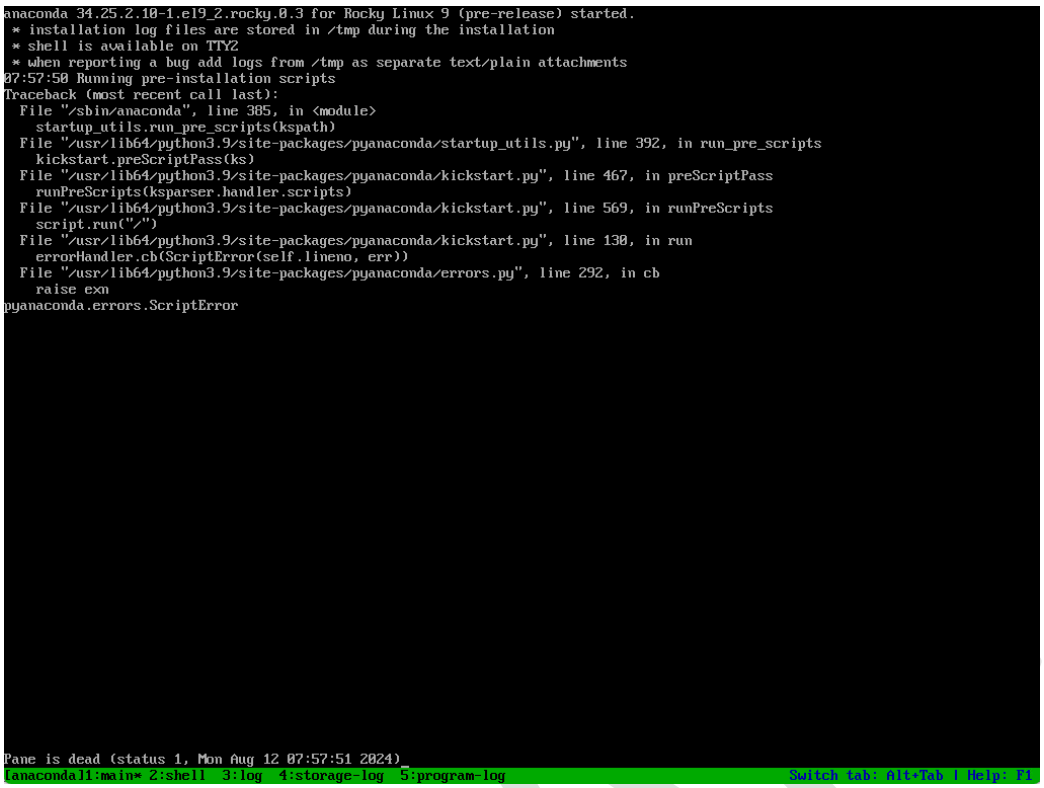
The installer shows the regular Rocky Linux install menu

- Unsupported configuration
- The system was booted with BIOS instead of UEFI

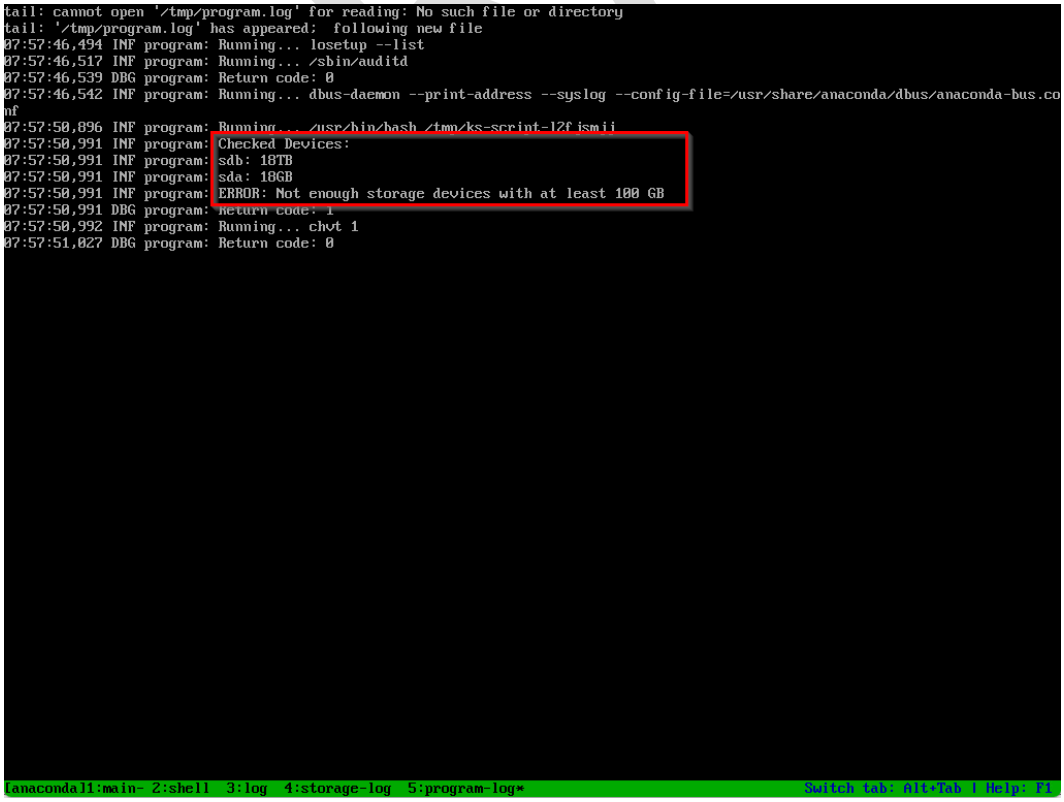


The installer fails before getting into the Installer GUI - Pyanaconda.errors.Scripterror

- The error looks like in this screenshot:

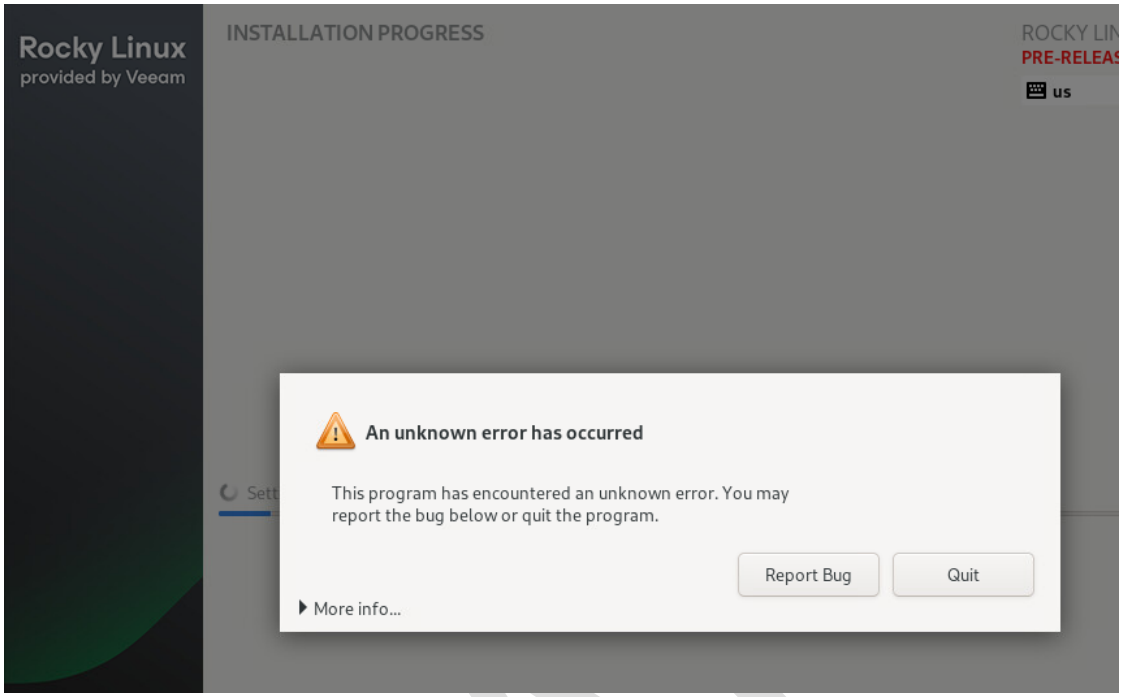


- Press “CTRL+b 5” and check the “program-log”
- Here one can see that the system requirements for disk size are not met.

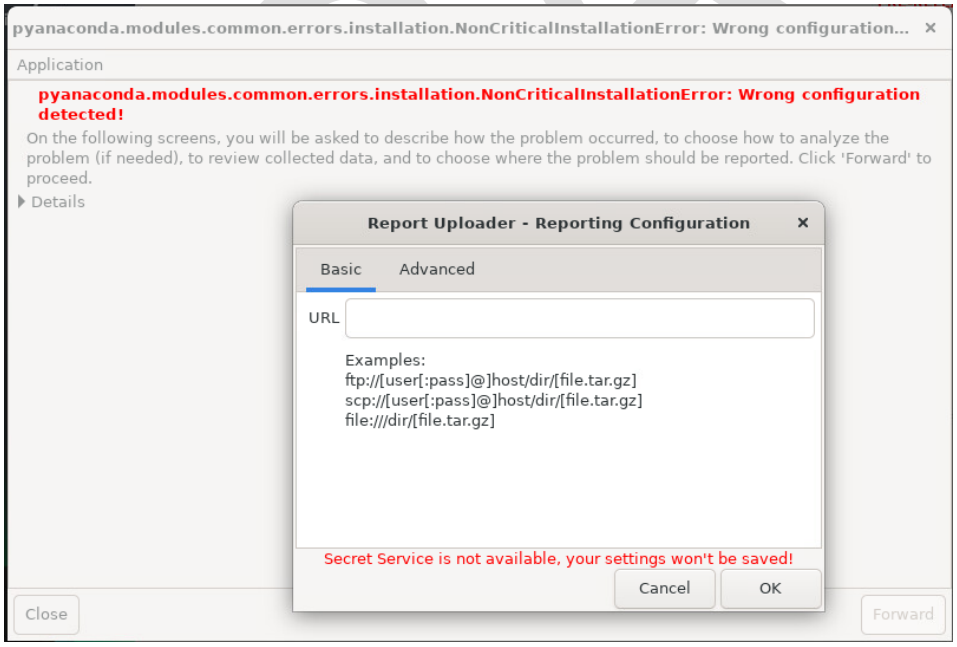


Error in the installer

If a “report bug” message appears, then you can upload logs via that wizard to an SCP (SSH) / FTP server. You need to have this server on your own. No data is sent to Veeam directly.

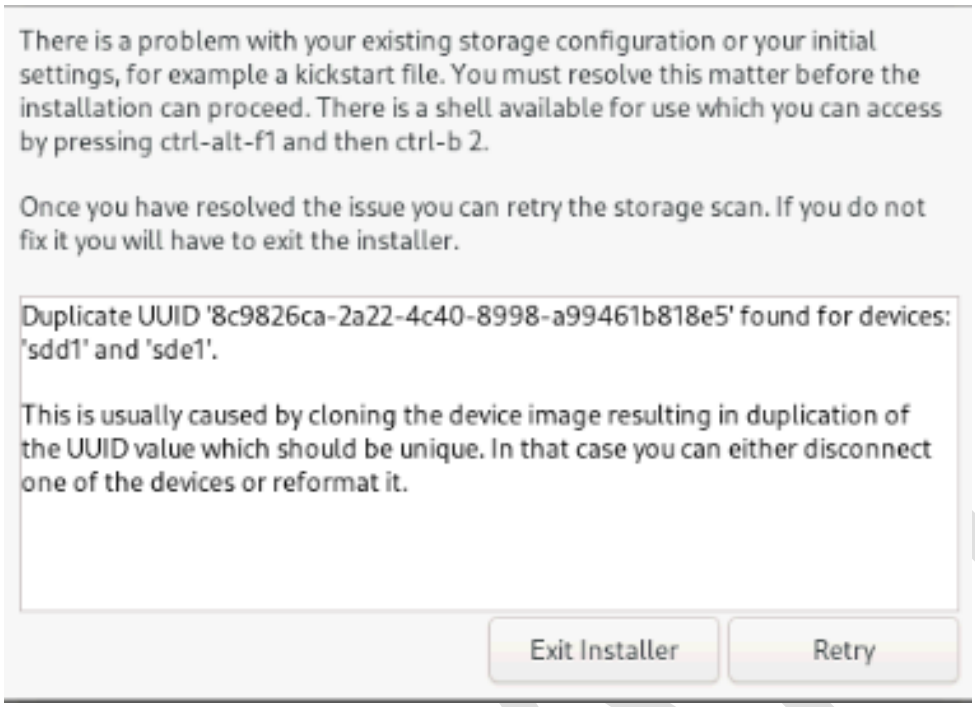


Follow the instructions on the screen. Please remember that a working network configuration is required.



Unsupported RAID controller error message

If you have a software RAID controller in RAID 1, then you very likely will see a “duplicate UUID” error. It’s expected and only hardware RAID controllers are supported. This message is from an HPE B140i controller. Solution: use a hardware RAID controller.



It’s impossible to log in although I’m sure I typed in the correct password

Very likely the credentials were mistyped 3x. Then the account is locked permanently. This is a DISA STIG requirement.

Re-installation is probably the easiest way. KB4663 describes how to unlock accounts manually.

General troubleshooting of the installer / getting logs

If the installer fails, there are different ways to handle that if the sections above do not help. If you are in the graphical mode, then CTRL+ALT+F1 brings you to the console. The console is “tmux”. Here are some shortcuts.

TMUX Key Combinations For Console

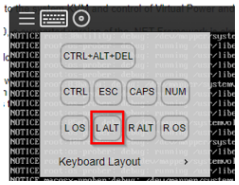
ALT+ TAB (switches windows on Windows)

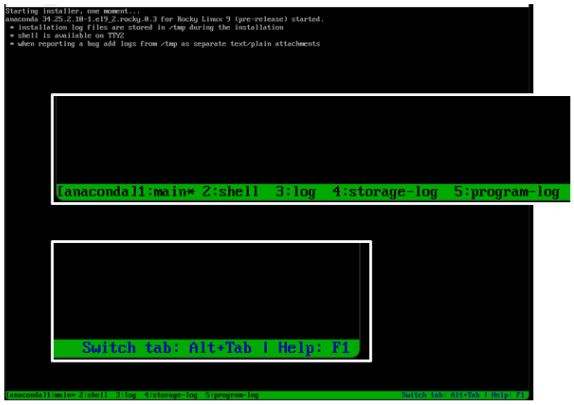
CTRL+b <number> - seems to be safest

CRTL+b <page up / page down> to scroll

ALT+F6 is GUI

Remote consoles have keyboard options. HPE example:





You can watch the program log and storage log by pressing:

- CTRL+b 4
- CTRL+b 5

Export logs

The relevant logs are in /tmp. If you are in the graphical installer, then press CTRL+ALT+F2 to get to the console. In TMUX this would be “CTRL+b 2”. Then you can use regular Linux commands to tar everything in /tmp and then upload with SSH.

Example:

```
cd /root
tar czf logs.tar.gz /tmp
scp logs.tar.gz user@your-ssh-server:
```

Then find the logs on your-ssh-server in the home directory of the user.

Planned features for upcoming (beta) versions

- Limit password complexity for generated passwords for veeamsvc
- “Repair mode” to re-install the operating system while keeping the data
- “live boot” for troubleshooting
- More options for “Hardened Repository Configurator” for troubleshooting
    - Things like “ping”, “fio”, “iperf” etc.

Providing feedback

To improve the ISO, we like to get feedback from testers on the Veeam R&D forums. The following information is important for us.

1) Thinks you liked.
2) Things you don't like.
3) Things you miss from a features perspective.
4) Hardware where you installed it:
    a. Vendor
    b. Model & Generation
    c. RAID controller
    d. Network card model & speed
    e. Disk configuration (e.g. 2x 200GB RAID 1 for OS and 12x10TB RAID 60 for data)
5) If installation failed, please provide logfiles via a file sharing service of your convenience.

Getting support

Please use the Veeam R&D forums to provide feedback via Veeam R&D forums. No official Veeam support will be provided for the community preview. You can also reach out to pm.beta@veeam.com

When reporting issues, please ensure to provide the following information:

- Hardware details (see "Providing feedback" section)
- Logs (see "troubleshooting" section)