Software Assurance Tips

A product of the Software Assurance Tips Team[3]

Jon Hood

Monday 21st March, 2022

1 The Death of CentOS on DoD Networks

Updated Tuesday 22nd March, 2022

When selecting an operating system for a new DoD product, there are several factors that are considered. The top three factors we often see are:

1. Price
2. DoD Compliance
3. Ease of Setup

When CentOS, recently acquired by RedHat, announced that they would no longer support CentOS 8 at the end of 2021,[1] architects began looking for an alternative. The possible alternatives that will be explored are:

- RedHat Enterprise Linux 8
- Oracle Linux 8
- Rocky Linux 8
- AlmaLinux OS 8
- Ubuntu 20.04
- SUSE Linux Enterprise Server 15

Each of these alternatives will be discussed here along with considerations DoD projects must make before they implement one of them. The minimal installation for each of the options is selected, and an install of Tenable Nessus 10.1.1 (commercially known as ACAS) will be used to evaluate compatibility.

1.1 RedHat Enterprise Linux 8

The first competitor is the seasoned veteran of the group: RHEL. One of the benefits of CentOS 8 is that it has been binary compatible with RHEL. Everything works out of the box, including DISA STIG compliance, SCAP Compliance Checker, and Nessus scanning. The downside to this option is the recurring subscription cost. Some organizations have a difficult time funding material and license purchases (i.e. labor-cost-only contracts), It's often difficult to use a subscription-based service contractually, even if the cost is reasonable.

1.2 Oracle Linux 8

Oracle Linux is now the oldest kid on the block when it comes to RHEL-compatible alternatives. A DISA STIG already exists for compliance, and a beta benchmark is available which knocks out the majority of automated checks in the STIG. For a streamlined experience in regards to compliance and compatibility, Oracle Linux 8 should be at the top of the list for consideration. The Nessus 10.1.1 ES8 RPM works with Oracle Linux 8, and the Oracle Linux 8 distribution is expressly supported by Tenable.

1.3 Rocky Linux 8

Rocky Linux is one of the newer RHEL-binary-compatible rebuilds that attempts to recreate the RHEL environment using the same standards that CentOS 8 used before it went EOL.

1.3.1 Installation Issues

When applying the DISA STIG for Red Hat Enterprise Linux 8 security profile during installation, it does not appear that the majority of the checks and configuration options (eg: partition information) are being performed or configured. Additionally, installing with this security profile will require the installation of openscap which will crash the installer with the minimal installation media. Rocky's inability to maintain compatibility with RHEL's security baselines (when both AlmaLinux and Oracle Linux were able to do so) is concerning.

1.3.2 Compliance

Rocky Linux does not currently have DISA risk acceptance or a standard STIG to apply. Instead, the RHEL 8 benchmark can be utilized with a note that the checks against the `CPE_NAME` in `/etc/os-release` should be modified to look for Rocky Linux rather than RHEL. The benchmark file (such as the one installed with SCAP Compliance Checker) can be modified to work with Rocky Linux using the command in Listing 1.

```
# sed -i -e 's|redhat:enterprise_linux|(.*|)</pattern>|rocky:rocky|1*</pattern>|g' |
    /opt/scc/Resources/Content/SCAP12_Content/U_RHEL_8_*_STIG_SCAP_1-2_Benchmark.
        xml
```

Listing 1: Modify RHEL Benchmark for Rocky Linux

If using the RHEL benchmark for evaluating Rocky Linux, the SCAP content will flag on rules relating to using a supported release (it checks /etc/redhat-release for this) and RedHat certificate authorities. The check content for these two CAT I checks should be modified to reflect the Rocky Linux support lifecycle and certificate authorities respectively.

1.3.3 Compatibility

I had no problem installing the RHEL version of Nessus 10.1.1 (though it should be noted that Rocky Linux is not listed as an officially supported distribution by Tenable). All RHEL packages installed and ran without issues, as they did with CentOS 8. FIPS compliance was enabled and tested with the `fips-mode-setup --enable` command.

1.4 AlmaLinux OS 8

AlmaLinux OS 8, like Rocky Linux, is one of the newcomers that is attempting to court CentOS migrators.

1.4.1 Installation Issues

The first thing that should be noted is the presence of a security profile for "DISA STIG for AlmaLinux 8." It should be emphasized that DISA has not released such a STIG, and the implications of there being one is disconcerting from a DoD compliance point of view. A bug has been created with the AlmaLinux team to address this.[2] Additionally, installing with this security profile selected against the minimal installation media will result in a crash due to an inability to install openscap.

1.4.2 Compliance

AlmaLinux does not currently have DISA risk acceptance or a standard STIG to apply. Instead, the RHEL 8 benchmark can be utilized with a note that the checks against the `CPE_NAME` in `/etc/os-release` should be modified to look for AlmaLinux rather than RHEL. The benchmark file (such as the one installed with SCAP Compliance Checker) can be modified to work with AlmaLinux using the command in Listing 2.

```
# sed -i -e 's|redhat:enterprise_linux|(.*|) </pattern>|almalinux:almalinux|1*</pattern
    >|g' |
        /opt/scc/Resources/Content/SCAP12_Content/U_RHEL_8_*_STIG_SCAP_1-2_Benchmark.
            xml
```

Listing 2: Modify RHEL Benchmark for AlmaLinux

If using the RHEL baseline for evaluating AlmaLinux, the SCAP content will flag for rules relating to using a supported release (it checks /etc/redhat-release for this) and RedHat certificate authorities. The check content for these two CAT I checks should be modified to reflect the AlmaLinux support lifecycle and certificate authorities respectively.

1.4.3 Compatibility

I had no problem installing the RHEL version of Nessus 10.1.1 (though it should be noted that AlmaLinux is not listed as an officially supported distribution by Tenable). All RHEL packages installed and ran without issues, as they did with CentOS 8. FIPS compliance was enabled and tested with the `fips-mode-setup --enable` command.

1.5 Ubuntu 20.04

For workstation use, Ubuntu is one of my go-to distributions. Nevertheless, a switch from CentOS to Ubuntu involves an architectural change that must be designed in up front rather than providing a drop-in replacement for end-of-life CentOS software. Installation of Nessus on Ubuntu 20.04 resulted in some manual modifications before it was able to work, and it should be noted that upgrading from Ubuntu 20.04 to the development branch of 22.04 (Jammy Jellyfish) resulted in a non-functioning Nessus installation. Nessus doesn't support Debian 11 or Ubuntu 22.04 at this time.

1.6 SUSE Enterprise Linux 15

The final option is SLES 15. Like RHEL, it provides enterprise-level subscription-based support. SLES 15 includes STIG content, SCAP benchmarks, and a seamless installation for products such as Nessus. SCAP content has lagged behind its RHEL counterparts; however, the support lifecycle for SLES 15 allows DoD project planners to have the security of knowing that their underlying operating system will be supported through July 31, 2031. It should also be noted that the STIG and SCAP content are for the enterprise server product, while the RHEL and Oracle products include their workstation derivatives.

1.7 Concluding Remarks

If you are a DoD product designer and needing to switch from CentOS 8, you have a lot of options. The most painless (compliance-wise) is to switch to Oracle Linux or RHEL. With either of these options, you have a robust STIG compliance framework in place to justify the decisions and a support network that can be used if needed. Nevertheless, Oracle Linux isn't the only free option to consider: strong contenders from AlmaLinux and Rocky Linux provide compatibility with very minor compliance caveats. Instead of the General Purpose OS STIG, the RHEL STIG can be modified to record compliance status of these operating systems; however, the AO should be informed of the risks involving using software managed by the Rocky and Alma organizations. These organizations are new and don't have the prodigy of RedHat, Oracle, SUSE, or Canonical in working with DoD projects.

Can the Authorizing Official (AO) accept the risk of allowing the AlmaLinux OS Foundation or Rocky Enterprise Software Foundation having write/update permissions to their package repositories? Both organizations already have the backing of Amazon, Microsoft, and Google platforms; such big names are members of these foundations to help their governance and future direction. The current lack of DoD-level risk acceptance should be acknowledged by the AO, but such an acceptance should not be seen as a high risk.

Finally, AlmaLinux supports the ELevate project which allows users to move to AlmaLinux, Rocky Linux, and Oracle Linux from CentOS 7 (`https://wiki.almalinux.org/elevate/`), and there are a few other tools available for migrating from CentOS 8 to one of the supported RHEL variants.

References

[1] CentOS. CentOS Linux EOL. CentOS. Dec. 31, 2021. URL: https://www.centos.org/centos-linux-eol/.

[2] Jon Hood. AlmaLinux Bug Tracker. AlmaLinux. Mar. 21, 2022. URL: https://bugs.almalinux.org/view.php?id=202.

[3] Jon Hood, ed. SwATips. https://www.SwATips.com/.