DELL Technologies

Best Practices Guide

Run iDRAC Service Module as Podman image file

Abstract

This Best Practices Guide provides information about running iDRAC Service Module (iSM) as a Podman image file. The Best Practices Guide also describes the security related features, dependent entities, and recommendations while running iSM as the Podman image file.

February 2023

Revisions

Date	Description
February 2023	Initial release

Acknowledgments

Authors: Bharath Koushik, Faizal SN, Rose Verma

Support: Navya V, Sheshadri Rao

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third party content is updated by the relevant third parties, this document will be revised accordingly.

Contents

Acronyms

Acronym	Expansion
iDRAC	Integrated Dell Remote Access Controller
iSM	iDRAC Service Module
IPMI	Intelligent Platform Management Interface
KCS	Keyboard Controller Style
OS	Operating System
SNMP	Simple Network Management Protocol
ASLR	Address Space Layout Randomization
DEP	Data Execution Prevention
GPG	GNU Privacy Guard
BMC	Baseboard Management Controller
SLES	SUSE Linux Enterprise Server
RHEL	Red Hat Enterprise Linux

Executive summary

This Best Practices Guide enables you to understand the configuration and deployment of iDRAC Service Module (iSM) as a Podman image file. An iSM image file can be created and deployed in a container environment using the Podman container management technology. The container deployment minimizes setup and configuration tasks. A Dockerfile runs in the Podman container management environment to create iSM application container. Commands in the Dockerfile builds the deployable iSM application container image file. This Best Practices Guide is aimed at administrators who have prior knowledge about iSM and the functionality of container environment.

1 iDRAC Service Module as Podman image file

The iDRAC service Module (iSM) 4.3.0.0 and newer versions provide the ability to deploy and run iSM service as a Podman image file. iSM contains the Podman file that carries clear and minimal instructions to prepare user specific Podman image file for iSM. The iSM Podman image file isolates iSM process from rest of the host operating system ecosystem. For more information and resources about the Podman image file, see https://linux.dell.com/repo/hardware/ism/.

iSM image file is based on SUSE Linux Enterprise Server (SLES) operating system. The created image file can be run on SLES and Red Hat Enterprise Linux (RHEL) operating systems. You can build the image file using either the Docker or Podman container technologies. By default, the Podman service is chosen for the creation of the image file.

1.1 Prerequisites

Before running iSM as the Podman image file, ensure that you have the following:

- Linux package repository—https://registry.suse.com/suse/sle15/
- iSM software repository—https://linux.dell.com/repo/hardware/ism/
- Target server with a supported Linux distribution

1.2 Target operating systems

iSM can be run as the Podman image file on the following target operating systems:

- Red Hat Enterprise Linux 8.x
- Red Hat Enterprise Linux 9.x
- SUSE Linux Enterprise Server 15 SPx

1.3 Host operating system components

To run iSM service as the Podman image file, the host operating system must have the following components:

- Syslog
- Host filesystems
- USB NIC network interface
- Relevant device driver interfaces such as Intelligent Platform Management Interface (IPMI) over Keyboard Controller Style (KCS)

1.4 Runtime prerequisites

The following are the runtime prerequisites to run iSM as the Podman image file:

- Ensure that the `root` privileges (Privileged mode) are enabled for the iSM Podman image file. The command option `--privileged` is necessary to access device driver interfaces. The `root` privileges are necessary to invoke and run iSM as the Podman image file.
- Expose relevant host components such as `syslog` to iSM Podman for audit messaging.
- Ensure that the components listed in the following table are available in the Podman image file:

Component name	Description
`/etc/os-release`	To bind mount os-release file for the OS Information feature.
`/etc/hostname`	To bind mount hostname file for the OS Information feature.
`/etc/snmp/snmpd.conf`	To bind mount snmpd.conf file for SNMP Traps and SNMP Get features.
`/lib/modules`	To bind mount modules directory. Load lib/modules for iDRAC Hard Reset and FullPowerCycle features.
`/dev/ipmi0`	To add host IPMI device to the container.
`/dev/log`	To bind mount log file for iSM system logs.
`–network`	To connect the container to the host network.

- Before deploying the iSM Podman image file, ensure that no instance of iSM is running on the host operating system.

2 Deploy iDRAC Service Module as Podman image file

For information about creating and deploying the iDRAC Service Module (iSM) as a Podman image file, see https://linux.dell.com/repo/hardware/ism/.

2.1 Supported features in Podman image file

The following features are supported on an iSM 5.1.0.0 Podman image file:

- OS Information (OS Information + Network Information)
- Replicate Lifecycle Log in the OS log
- Auto System Recovery
- iDRAC Hard Reset
- FullPowerCycle
- SupportAssist
- SNMP Alerts via Host OS
- SNMP Get via Host OS
- SNMP OMSA Alerts via Host OS

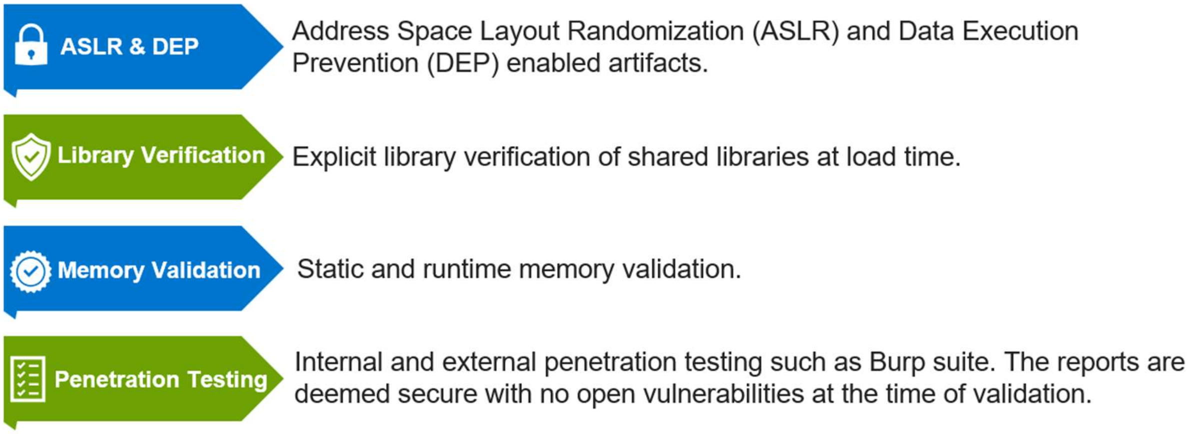
Note: To provide firewall access to the SNMP port of the remote server, run the following command on the host operating system:

```
firewall-cmd --add-port=161/udp
```

For more information about using the SNMP alert features in iSM, see the iDRAC Service Module - In-Band iDRAC SNMP Alerts Technical White Paper.

2.2 iSM Podman security features

The following security features are provided when iSM is running as the Podman image file:



Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) enabled artifacts.

Explicit library verification of shared libraries at load time.

Static and runtime memory validation.

Internal and external penetration testing such as Burp suite. The reports are deemed secure with no open vulnerabilities at the time of validation.

Figure 1 iSM Podman security features

3 Recommendations

The following are the recommended practices for a secure Podman environment:

- Ensure that the SUSE Linux Enterprise Server package repository is up to date.
- Enable trust verification of the repository before consuming any packages.
- Verify the authenticity of the Podman image file and packages using available mechanisms, such as GNU Privacy Guard (GPG) sign verification.
- Ensure no host filesystems are mounted to the Podman image file unless required.
- Recreate the Podman image file when vulnerability is found in the image file version.
- iSM uses designated ports on the host to communicate with Baseboard Management Controller (BMC).
- iSM does not initiate communication with other resident Podman image files. Any paths introduced are documented and audited appropriately.

4 Frequently asked questions

4.1 What action should be taken when vulnerability is reported on OS relevant packages in the package repository?

Update the SUSE Linux Enterprise Server repository with the latest patches released by the Linux community.

4.2 What are the iSM dependent packages when kernel undergoes secure patches?

The following are the dependent packages for iSM on the operating system driver modules:

- Keyboard Controller Style (KCS) device driver
- Network device driver

4.3 Unable to create the Podman image file

Ensure that the SUSE Linux Enterprise Server repository is reachable from the server where the iSM Podman image file will be created.