Mandiant

UPGRADE SECURITY VALIDATION VIRTUAL APPLIANCES TO ROCKY LINUX 8

Starting with release 4.14.0.0, Mandiant Security Validation (MSV) uses Rocky Linux 8 as the underlying operating system for virtual appliances. The previous virtual appliance operating system was CentOS 7. As of June 30, 2024, CentOS 7 will be End of Life (EOL) and therefore no longer supported as a base operating system.

To ensure that your deployment continues to receive the latest functionality and security updates, use the guidance in this document to upgrade your MSV virtual appliances to the Rocky Linux 8 platform.

If you're unsure of which platform you're on, run the following CLI command while connected to the Director or Actor using SSH:

```
hostnamectl
```

The following output example confirms that Rocky Linux is the underlying platform:

```
   Static hostname: DIRECTOR_OR_ACTOR_HOSTNAME
         Icon name: computer-vm
           Chassis: vm
        Machine ID: xxxxxxxxxx
           Boot ID: xxxxxxxxxx
    Virtualization: vmware
Operating System: Rocky Linux 8.10 (Green Obsidian)
     CPE OS Name: cpe:/o:rocky:rocky:8:GA
          Kernel: Linux 4.18.0-553.22.1.el8_10.x86_64
    Architecture: x86-64
```

DIRECTOR_OR_ACTOR_HOSTNAME refers to the hostname that you previously set for the Director or Actor you're signed into.

Directors

Follow these steps to upgrade to a 4.14.0.0 Director on Rocky Linux 8 while preserving your data and settings. For an existing Director virtual appliance, on version 4.13 or earlier:

1. Optional: If using a static IP, go to **Settings > Director Settings**, click **Network** and note the following network information for the Director (required for Step 5):
   - Director IP address
   - Director gateway
   - Director DNS server (if applicable)
2. Upgrade your existing Director to version 4.14.0.0. After this step, you will have a 4.14.0.0 Director that is still running on CentOS 7.
   - See **Update Security Validation Components** **(https://docs.mandiant.com/home/msv-system-updates)** for steps to upgrade your Director.
3. After the 4.14.0.0 upgrade, take a backup of the Director virtual appliance. This step preserves your existing settings.
   - See **Backup and Restore Security Validation** **(https://docs.mandiant.com/home/msv-backing-up-and-restoring-the-platform)** for steps to back up your existing Director.
4. Take the existing Director machine offline, then replace it with the Rocky Linux 8 4.14.0.0 Director virtual appliance,

using the same IP address or DNS name.

- See **Director Downloads** (https://docs.mandiant.com/home/msv-director-installers) to obtain a copy of the latest 4.14.0.0 Director virtual appliance.
- See **Director Installation** (https://docs.mandiant.com/home/msv-director-installation) for steps to follow to install the Director virtual appliance.

5. Once the new Director is online, connect to the Director using SSH and then run the following commands:

```
vsetnet
```

There is a known issue where `vsetnet` doesn't correctly apply the static IP to the Director. As a workaround, after running `vsetnet`, run the following:

```
nmcli con show
```

You'll see output that looks like the following:

```
NAME                UUID                  TYPE      DEVICE
Wired connection 1  UUID_VALUE            ethernet  enp1s0
```

Take note of the name `NAME` and `DEVICE` values in the preceding command output (in this case, `Wired connection 1` and `enp1s0`) and then run the following commands, where *DIRECTOR_STATIC_IP_VALUE*, *GATEWAY_IP_VALUE*, and *DNS_SERVER_VALUE* are the network values that you obtained from Step 1:

```
nmcli con mod "Wired connection 1" ipv4.method manual ipv4.addresses DIRECTOR_STATIC_IP_VALUE
ipv4.gateway GATEWAY_IP_VALUE ipv4.dns DNS_SERVER_VALUE
```

```
nmcli device reapply enp1s0
```

As long as you have the netmask, such as `/24`, at the end of the IP Address, the IP address should update properly and be maintained across reboots.

```
vrestart
```

If your CentOS 7 Director had its disk expanded at any point to allow for larger databases or content libraries, you likely need to do this step for your Rocky 8 Director prior to starting the restore step. See **Expand the Director Storage** (https://docs.mandiant.com/home/msv-expanding-the-director-storage) for guidance.

- If you have a large database, expand the `/var` partition.
- If you have a large content library, expand the `/opt` partition.

6. After the new Director reboots, restore the backup that you created in Step 2 onto the new 4.14 Director virtual appliance. After this step, you will have a 4.14.0.0 Director running on Rocky Linux 8 with your existing settings.
   - See **Backup and Restore Security Validation** (https://docs.mandiant.com/home/msv-backing-up-and-restoring-the-platform) for steps to restore the Director backup.

Actors

- Windows Actors, macOS Actors, and installable Linux Actors can be upgraded to 4.14.0.0 through the standard upgrade procedures for Actors: upgrade the Director to 4.14.0.0, and then upgrade Actors through the Director web

interface.
    - See **Update Security Validation Components** (https://docs.mandiant.com/home/msv-system-updates) for steps to upgrade your Actors.

- Appliance Actors on releases prior to 4.14.0.0 should be removed and replaced with equivalent 4.14.0.0 Actor Appliances. These replacement Actors can either be registered as a new Actor with the Director (and the pre-4.14.0.0 Actor removed from the Director), or the Actor can be reattached in the Director.
    - See **Register your Network Actor using the Director** (https://docs.mandiant.com/home/msv-registering-your-actor-using-the-director) for steps to register a 4.14.0.0 Actor.
    - See **Reattach an Actor** (https://docs.mandiant.com/home/msv-reattaching-an-actor) for steps to reattach Actors to the Director.

Protected Theaters and Protected Actors

- You must recreate Protected Theaters and Protected Actors because there is no current procedure for migration.
- Detaching a non-Rocky Linux Protected Theater and reattaching a Rocky Linux Protected Theater is not supported.
- If you encounter issues with importing a QCOW2 image, see **Troubleshoot a Protected Theater Image Import Error** (https://docs.mandiant.com/home/msv-pt-image-import-error).

Workarounds

Workaround: Network settings revert back to DHCP

Azure instances may need the additional `systemctl` commands to disable `cloud-init`.

```
systemctl disable --now cloud-init.service
systemctl mask cloud-init.service
```

If your Director and Actor networking settings revert back to DHCP on reboot, use the following steps as a workaround:

1. Use SSH to sign in to the affected component.
2. Run the following command on the affected images:

```
sudo touch /etc/cloud/cloud-init.disabled
```

3. Run the following command to ensure network settings are configured properly:

```
vsetnet
```

Workaround: Nginx vulnerability

There is a vulnerability in the version of Nginx that's installed on Actors and Protected Theater with MSV 4.14.0.0. To fix this issue, you can manually update the Nginx version:

1. Use SSH to sign into the Actor machine.
2. Run the following command:

```
sudo yum module switch-to nginx:1.20
```

- A fresh installation of MSV 4.14.0.1 also fixes this issue.
- An upgrade to 4.14.0.1 does not fix this issue.

Workaround: Remote Integrations fail to report events

After migration, Remote Integrations may fail on 4.14 Actors running Rocky Linux 8. As a workaround, issue the following commands to update systemd with the correct arguments:

1. Use SSH to sign into the Network Actor.
2. Switch to the root user:
   ```
   sudo -i
   ```
3. Navigate to the following folder:
   ```
   cd /usr/lib/systemd/system/
   ```
4. Open the `verodin-msi-service.service` file:
   ```
   vi verodin-msi-service.service
   ```
5. Modify the `/usr/lib/systemd/system/verodin-msi-service.service` file, adding `--network=host` as an argument to the `/bin/docker run` command.
   After editing, the `ExecStart` should look like the following:
   ```
   ExecStart=/bin/sh -c "/bin/docker run \
      --rm \
      --name msi-service \
      --log-driver=none \
      --network=host \
      -p 8000:8000 \
      -e MSVI_DEV_MODE=1 \
      -e IS_GCP=0 \
      -e MSI_IS_OPENFAAS=0 \
      -e MSI_CLUSTER_ENV=DEV \
      msi-service:latest &>> /opt/apps/verodin/node/log/verodin_msi_service"
   ```
6. Type `:wq` to save changes and quit the editor.
7. Run the following to reload the service:
   ```
   systemctl daemon-reload
   ```
8. Run the following to restart the service so changes take effect:
   ```
   systemctl restart verodin-msi-service
   ```