Mandiant

CUSTOM IPTABLES RULES

To enable ports that are required on the host system for non-Security Validation activities, such as `ping` and `snmp`, you need to add custom iptables rules. The rules are retained across Job Actions once they are added.

- The custom iptables rules are supported for OVA and software-based installations.
- For information about iptables rules and parameters, see the documentation for your operating system.

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.

You must complete the steps in both the Director and Actor tabs.

Director

1. Open an SSH session to the Director.
2. Using the built-in `vi` text editor, open the iptables file to add custom rules, depending on your Director's platform:
   - For Rocky Linux:

     ```
     sudo vi /etc/sysconfig/iptables
     ```

   - For CentOS:

     ```
     sudo vi /etc/iptables.rules
     ```

3. Enter custom rules in standard iptables formatting. For example, the following command appends two custom rules that accept incoming traffic on ports 22 and 443 over the TCP protocol:

   ```
   -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
   -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
   ```

4. Save your changes by typing `:wq`, then pressing Enter.
5. Reboot the host. The custom iptable rules become active for the Director.

Mandiant

Actor

1. Open an SSH session to the host system where the Actor is installed.
2. Using the built-in `vi` text editor, open the iptables file to add custom rules:

   ```
   sudo vi /opt/apps/verodin/node/settings/iptables.rules
   ```

3. Enter custom rules in standard iptables formatting. For example, the following command appends two custom rules that accept incoming traffic on ports 22 and 443 over the TCP protocol:

   ```
   -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
   -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
   ```

4. Save your changes by typing `:wq`, then pressing `Enter`.
5. Reboot the host. The custom iptable rules become active for the Actor.