Mandiant

CONFIGURATION FOR ACTORS IN THE CLOUD

When your Actors are cloud-based, there may be additional configuration required. This includes:

- **Modifying the IP Address used by the Actor**
- **Setting up Virtual Addresses**
- **Adding Custom iptables Rules**
- **Adding the sub-interface in AWS or Azure**

Modifying the IP Address used by the Actor

When you register cloud Actors, it is important to verify the configuration is correct for both the private and public IP addresses. Required configuration changes depends on where the Actor is in relation to the Director and if it is a Push or Pull communication Actor.

If the Actor is local to the Director (in the same subnet or VPC for example), the Director should be able to communicate directly on the private IP. However, a typical cloud Actor is installed in an isolated network. This means the Director should connect to the Actor via the public IP address. Push Actors will automatically be setup to use the correct management public IP address based on registering from the Director with that IP. However, Actors registered using vregister (Pull communication) will need to be updated with their public IP address.

Verify your Actors are using the proper IP address

1. Capture the Actor's IPv4 Public IP address.
2. Launch the Director and sign in.
3. Select **Environment** > **Actors**.
4. Review the IP addresses listed in the table. If an Actor does not have the correct public IP address, click **Edit** for that Actor.
5. Change the IP in the Test field so it shows the public IP and click **Update Actor**.

   Each interface you are using (Test, Management, Monitor) must have its own public IP
6. Add the appropriate public IP addresses to the Test, Management, and Monitor field and click **Update Actor**.
7. Repeat for any other Actors.

Setting up Virtual Addresses

In certain cases, Actors may need to be addressed using a different IP or FQDN. This would be based on the source location of the traffic, such as an external AWS Actor communicating with an Actor hosted in a DMZ within a network. An Actor can have a private address that all Actors and Directors inside the Network can talk to. However, to test traffic from an external source coming in from outside the network, a different IP address would be required. By configuring a Virtual IP Address in these instances, a single Actor can be addressed in multiple ways depending on the source location.

Add a virtual address

1. Launch the Director and sign in.
2. Go to **Settings** > **Director Settings**. The Systems Settings page opens.
3. Select **Virtual Address**.
4. Click **Add Actor Virtual Address**.
5. Populate the form:
   a. Select *one or more Source Actors* (the external AWS Actor from the preceding example).
   b. Select *the Destination Actor* (the DMZ Actor from the preceding example).

c. Enter *a Test Address, a Monitor Address* , or both (Management Address is not necessary unless the source is the Director).

6. Click **Create Actor Virtual Address**.

Adding Custom iptable 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.

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.

Adding the sub-interface

Security Validation Network Actors support the use of a second network interface for running tests that are separated from the management interface. Using a second network interface lets you add the management IP address to your allowlist without any changes to the security stack when running Actions to the test address. You can also use a third network interface for running monitors.

Security Validation Network Actors on AWS can use multiple interfaces or use sub-interfaces. To create a sub-interface and associate it with the Security Validation Platform instance, use the following procedure.

- Each interface and sub-interface must have a unique Public IP address.
- If your Actor is hosted by Mandiant, contact **Support (https://docs.mandiant.com/home/mandiant-support-cases)** for any interface work and only update files as directed.

Add a sub-interface to an AWS instance

1. In the Amazon EC2 console, select your Validation Platform instance in the list, and then select **Actions** > **Networking** > **Manage IP Addresses**
2. Expand the **eth0** interface.
3. Click **Assign New IP** to create the sub-interface (eth0:2). Both interfaces get internal IP addresses after this step.
4. Create an Elastic IP address for eth0 and for the sub-interface.
5. Associate the Elastic IP addresses with the Validation Platform instance.

Configure your OS to recognize the secondary interface

To add your interfaces, modify your network configuration script. The procedure varies by operating system. In your operating system documentation, search for information about configuring additional network interfaces and secondary IPv4 addresses. You can also search for information about using routing rules to work around asymmetric routing.

An example of how to configure your secondary interface for CentOS is provided.

Example: Adding a secondary network interface in CentOS

1. To configure your interfaces, alter the network configuration script (or run the `vsetnet` command), where *interface_ID* is the unique interface identifier, such as `eth0:2` .. `/etc/sysconfig/network-scripts/ifcfg-`*interface_ID*

2. BOOTPROTO=none

   DEVICE=*interface_ID*

   ONBOOT=yes

   TYPE=Ethernet

   USERCTL=no

   IPADDR=*IP Address*

   NETMASK=*Netmask*

   GATEWAY=*Gateway*

2. Save and close the script file.
3. Edit the following file to specify the interface allocation: `/opt/apps/verodin/node/settings/node_settings.conf`
4. [DEFAULT]

   primary_nic = eth0

   secondary_nic = eth0:2

   tertiary_nic =

   firewall_control = True

   Where:

- `primary_nic` is your management interface.
- `secondary_nic` is your test interface (e.g., eth0:2, etc.).
- `tertiary_nic` can be your Monitor Interface, if a third address is allocated.
- Save and close the `node_settings.conf` file.
- Register the Actor.