Mandiant

RESOLVE PROBLEMS DURING ACTOR REGISTRATION

If you are having issues registering an Actor, there are several tools available to help identify and resolve the issue. These include:

- **Monitor Registration Communication**
- **Address Communication Issues during Registration**
- **Restart Services**
- **Make Additional Interfaces visible**

Monitor Registration Communication

You can monitor the registration process by verifying network information (interface IP addresses, route tables, and so on) as it gets updated in the Director. The file you monitor depends on where you are monitoring.

> When available, log samples are provided. IP addresses may have been scrubbed, using xxx to replace private values. Long lines may have been truncated, with ... added to the end of a line to show that there was additional data.

- Director: `/opt/apps/verodin/planner/log/verodin_node_log`

```
2018-05-14 13:25:36 +0000 : NODES FOR CONNECT CHECKING: []
-------
2018-05-14 13:25:36 +0000 : CONNECT - PROXYOBJ: nil
-------
2018-05-14 13:25:36 +0000 : STARTING GET HTTP OBJ: nil
-------
2018-05-14 13:25:36 +0000 : CONNECT - POSTING: #<URI::HTTPS https://xxx.20.0.47/planner_register>
-------
2018-05-14 13:25:37 +0000 : CONNECT - POSTED: #<Net::HTTPOK 200 OK readbody=true>
-------
2018-05-14 13:25:37 +0000 : CONNECT - RESPONSE HASH: {"ipaddr"=>"xxx.20.0.47", "ipmask"=>"255.255.255.0", "node_version"=>"3.3.3.1", "ssh_pub_key"=> ...
```

- All Actors: When an unexpected response is received, a message will be displayed and a `response.txt` file is created.
- Network Actor, Protected Theater - Pull communication: `/opt/apps/verodin/node/log/verodin_registration`

```
DEBUG:10/07/2018 06:27:58 PM information.py:98: /var/run/dhclient-eth0.pid does not exist DHCP is false for eth0
DEBUG:10/07/2018 06:28:06 PM information.py:98: /var/run/dhclient-eth1.pid does not exist DHCP is false for eth1
DEBUG:10/09/2018 09:40:27 PM __init__.py:118: netifaces: eth0 does exist
DEBUG:10/09/2018 09:40:27 PM __init__.py:118: netifaces: eth1 does exist
DEBUG:10/09/2018 09:40:40 PM networking_centos.py:20: netifaces: eth0 does exist
DEBUG:10/09/2018 09:40:40 PM information.py:98: /var/run/dhclient-eth0.pid does not exist DHCP is false for eth0
DEBUG:10/09/2018 09:40:40 PM networking_centos.py:20: netifaces: eth1 does exist
DEBUG:10/09/2018 09:40:40 PM information.py:98: /var/run/dhclient-eth1.pid does not exist DHCP is false for eth1 INFO:10/09/2018 09:40:40 PM _system.py:207: Checking -backend.service for actor user INFO:10/09/2018 09:40:40 PM _system.py:230: Actor user: nodeone INFO:10/09/2018 09:40:40 PM _system.py:207: Checking -backend.service for actor user INFO:10/09/2018 09:40:40 PM _system.py:230: Actor user: nodeone
DEBUG:10/09/2018 09:40:40 PM information.py:150: routing table is Kernel IP routing table Destination Gateway Genmask Flags Metric Ref Use Iface 0.0.0.0 10.10.20.1 0.0.0.0 UG 0 0 0 eth0 10.10.20.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0 10.10.20.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1 ...
```

- Network Actor, Protected Theater - Push communication: `/opt/apps/verodin/node/log/verodin_node_web`

```
DEBUG:05/14/2018 01:25:36 PM web_helpers.py:43: Received request for planner_register
DEBUG:05/14/2018 01:25:36 PM node_web.py:498: planner register
DEBUG:05/14/2018 01:25:36 PM infrastructure.py:704: registering with planner
DEBUG:05/14/2018 01:25:36 PM networking_centos.py:87: netifaces: ens32 does exist
DEBUG:05/14/2018 01:25:36 PM web_helpers.py:51: planner_register returning result: {"ipaddr": "xxx.20.0.47", "ipmask": "255.255.255.0", "node_version": "3.3.3.1", "ssh_pub_key": "ssh-rsa ABGTR3NzaC1yc2EAAAADAQABAAACAQC1Xl+npYaXXunoiyqhj5NO5BkD4WtnzULiBXUifM4kYm4xjVpFkkLRA/6t8sJof/tvLl3uleAiAm85Dmq+S6xRyzfOs/q+uKS0NbLKb/TJvDBXNRFjLnklMoxTAU78A6bYWSdvD53WWyMrqvf5UFUelM7BOhYsJUWcuHTVBsM0pQo6eM0XtNLL4E8FHgTjHaoieXnptfj4hGCNWPK5ZLClXLVmA3uvcwCdYNab8GRh1QGLlSqnzJ0oYPGkuqnKbBdGUhLKMvF0Os5gNa/vCarsun7bBlPZyOzSf1ljuqGc5vTB/2k7zLGDs7QrTDNkijZC/gfrbR0DALGE2roouFMGL5J5K6kMu2w2E3UhqoXTy3iqMtYUkn/RrKlx1kPyu30DCG3Ls3nsVs35tK7/NJ883dPnS/ou58P3k9j5hMv0jbcIqqxUh24pIx6K9JeSx2D3SeB7pijgMyV8WYTPY/9VefFDI3E4bd0Xi4N1MXyNA4HY77YGsQ2yrVaRWQ7aCS46qwKk4ICzbVPtq4yGVjAvgNhBh3SB4fQtNW5fjoSazGlhmTUggh8ZymQYeDNT61v62pEBZ4WdLKPAj5Q9iikKE8KSKJeyr3rzOuFQfyVK5YdLshjRy0zKF9zaT13O/At6dzOHD0BSQagWNBVwhGlF1LLsD03dG2eXyxNQmgwQsw== support@.com\n", "gateway": "172.20.0.1", "result": "success", "network_info": "{\"interfaces\": \"ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500\\nine
```

- Endpoint Actor - Apple(R) Macintosh(R) OS:If you encounter problems during installation, check the following log file: `/var/log/verodin_installer`
- Windows Actor & Protected Actor: `C:\Program Files\Verodin\node\log\verodin_registration`

```
DEBUG:04/16/2018 06:22:50 PM vregister:332: calling discover_products with config sent from director
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:71: Starting discover_products function with 13 config en
tries
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:72: List of programs: {'updateassistant 1.12.0.0', 'updat
e for windows 10 for x64-based systems (kb4023057) 2.13.0.0', 'microsoft visual c++ 2008 redistributable - x8
6 9.0.30729.4148 9.0.30729.4148', 'windows 10 update and privacy settings 1.0.14.0', ' endpoint 3.3.3.2', 'micr
osoft visual c++ 2008 redistributable - x64 9.0.30729.6161 9.0.30729.6161', 'vmware tools 10.0.9.3917699'}
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:73: List of services: {'winmgmt windows management in
strumentation', 'timebrokersvc time broker', ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: {'technology': {'tech_ty
pe': 'Antivirus', 'vendor': 'McAfee', 'product': 'McAfee Antivirus', 'description': 'Allows you to ingest McAfee EPO d
ata for use in CIM compliant Splunk apps'}, 'logs': [{'value': 'Application', 'type': 'event_log'}], 'type': 'endpoint',
'discovery': {'splunk': [{'value': 'mcafee:ids', 'type': 'field', 'field': '_sourcetype'}], 'alien_vault': [{'value': 'McAfe
e Antivirus', 'type': 'field', 'field': 'device_description'}], 'arcsight': [{'value': 'McAfee Antivirus', 'type': 'field', 'fiel
d': 'Device Product'}], 'endpoint': [{'service': 'McAfee VirusScan Announcer', 'type': 'service_exists'}]}}
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:77: Checking entry in config file: ...
DEBUG:04/16/2018 06:22:55 PM product_discovery.py:113: Returning 0 found products: []
DEBUG:04/16/2018 06:22:55 PM vregister:338: making request to discovered_products with data: {'discovered_
products': '[]', 'token': 'UAasZdMtUMd6rqj2xtiQc2Esxcq8Uj8NTEjzntPD4FKy71o1zdAumCk3UVGgH5gwbLStbT0xL
bz0DrzRdJn2pf25wD37ao0xv0ukJJJn7b2iVygNLYK02bhdprGaAJw5'}
DEBUG:04/16/2018 06:22:55 PM vregister:364: response from discovered_products: 200
```

Address Communication Issues during Registration

If you find logs are not updated as expected, the issue is generally related to communication. The following is a list of commands and their purpose.

- `vstatus` : Make sure all necessary services are running.

  > - The `vstatus` command is not available for network Actors installed on macOS.
  > - If you are connecting to an Actor virtual machine using SSH from a macOS client (for example, through the Terminal app), you may see runtime errors when you run `vstatus` . To fix this issue, run `export LC_ALL=en_US.UTF-8` in the Terminal app, then try running `vstatus` again.

- `tcpdump` : Use `tcpdump -nei mgmt_interface` on both the Actor and Director, and then attempt registration (it helps to have 2 terminal windows open); in Push mode, there should be packets leaving the Director, destined for the Actor; in Pull mode, there should be packets leaving the Actor, destined for the Director.
- `ifconfig -a` : Make sure interface assignments are accurate; check interface names, MAC addresses, and netmasks.
- `netstat -nr` : Make sure routing tables are accurate; check interface names, default routes, and netmasks.
- `netstat -natup` : Check that TCP port 443 is listening on both Director and Actor.

The `netstat -natup` command is not available for network Actors installed on MacOS.

- `traceroute` : To see the routes and interfaces being used for communication, you can use the traceroute command.
  - Traceroute is included in the virtual-appliance installers.
  - You need to install traceroute, as it is not included in the installation.
- `curl` : Depending on Push or Pull communication method, you should be able to get from Director to Actor (`curl -k https://actor ip/`), or Actor to Director (`curl -k https://director ip/`), using curl and targeting the management interface.

Ping is not a good tool to use in this instance. The Validation Platform drops ICMP on the management interfaces, so pinging them will result in no response. If you want to use ping, pair it with tcpdump so you see the traffic hitting the interface, but be aware you still won't get an ICMP ECHO response.

Restart Services

If the Actor services are down, you can restart them.

Restart the services from the command line

Run `vrestart` .

The process varies based on Actor form factor and operating system.

- Linux: Log into the Actor and run the following:
  - PATH updated: `$ sudo vrestart`
  - PATH not updated: `$ sudo /opt/apps/verodin/node/node/scripts/vrestart`
- Mac: Log into the Operating System and run the following:
  - `Users\Shared\Verodin\node\node\scripts\vrestart`
- Windows: Log into the Operating System and run the following
  - `C:\Program Files\Verodin\node\node\scripts\vrestart`

Restart the services from the Director

This can only be completed if you are a user with power user or administrative privileges.

1. Select **Environment** > **Actors**.
2. Locate the Actor you want to configure, open its Action menu, and click **Edit** .
3. Click **Restart Services**.

Make Additional Interfaces visible

If you are unable to register because you can't see the interfaces you need, such as when you're using a VPN, you need to use a special argument when running vregister. This means you'll need to register the Actor from the command line. The argument you would add is `--include-tap-adapters` . Examples are included as follows:

- Linux, PATH updated:

```
$ sudo vregister --include-tap-adapters
```

- Linux, PATH not updated:

```
$ sudo /opt/apps/verodin/node/node/scripts/vregister --include-tap-adapters
```

- Mac:

```
Users\Shared\Verodin\node\node\scripts\vregister --include-tap-adapters
```

- Windows:

```
C:\Program Files\Verodin\node\node\scripts\vregister --include-tap-adapters
```