IP Maestro®

Version 3.0

Installation Guide

February 2025

IP Infusion Inc.

3979 Freedom Circle

Suite 900

Santa Clara, California 95054

http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:

support@ipinfusion.com

Contents

Preface

This guide describes the steps for installing, configuring and logging in to IP Maestro. This preface includes the following sections:

Supported OcNOS Version

IP Maestro Release 3.0 software is designed to monitor devices running OcNOS-6.3.4-70 and above.

Intended audience

The intended audience for this guide is the end-user with access/role/permission to IP Maestro with valid roles that include Network Administrators, Engineers, Operators, and Users.

Product version

This document applies to the IP Maestro 3.0 release.

Overview

IP Maestro streamlines Element Management processes, enhances visibility, and strengthens security. It features a user-friendly Graphical User Interface (GUI) based Element Management System (EMS) that provides an intuitive display of network topology, faults, performance metrics, and inventory.

Key features include:

- **Centralized Log Repository**: The system gathers and stores logs centrally, simplifying log management and analysis.
- **Mass Device Configuration and Software Updates**: The system facilitates efficient and simultaneous configuration of multiple devices and allows seamless software updates.
- **Role-Based User Management and Auditing Logs**: The system implements a role-based access control system for user management and maintains comprehensive auditing logs for accountability.
- **Fault Management:** Capture and display alarms from network devices, links, and services. IP Maestro's Fault Management module efficiently processes NETCONF alarms and integrates with syslog for centralized management and alerts. IP Maestro also has the ability to send out email notification to users on occurrences of critical alarms.
- **Performance Monitoring:** Monitor network performance effortlessly with metrics (KPI) and calculated/ complex metrics (KQI). Define measurement points, groups, collection intervals, and aggregations intervals for precise and periodic data analysis.

Hardware and Software Requirements

Following are the software/hardware requirements to run the IP Maestro application efficiently.

Software/Hardware	Required/Version
Memory	32 GB 500GB disk space
Cores	4 CPUs
CPU Type	Support SSE 2.4 (Example: Westmere CPU Type)
Supported browsers • Google Chrome • Mozilla Firefox • Microsoft Edge • Opera • Safari • iOS • Android • Windows Mobile	 • 102.0.5005.63 (64 bit) • 99.0.1 (64 bit) • 103.0.1264.62 (64 bit) • 89.0.4447.51 • 15.5 (latest) • 9+ (or latest) • 4.4+ (or latest) • IE 11+ (or latest)
Operating System	Ubuntu 20.04.2 LTS
Docker	23.0.0 and above
Docker Compose	2.20.2 and above

Date and Time

As a requirement, the Date and Time on OcNOS devices, IP Maestro host, and the Local License Server host must be in sync.

OcNOS Devices

- Ensure the OcNOS device date and time is in sync with IP Maestro and with the devices being monitored.
- Ensure the OcNOS device date and time is updated to the current date and time to get the license installed on the device.
- Execute `clock` command to set the device date and time on OcNOS.

Local License Server

The licenses in IP Maestro are encoded with a start date after which they are effective, and some trial licenses also have an expiration date. The Local License Server (LLS) validates the license and also checks for any inconsistencies in the host system time.

To ensure that licenses can be obtained by IP Maestro, it is necessary that the host on which IP Maestro is installed and the host on which LLS container is deployed, have valid system time set.

Note: LLS can also be deployed on the same host as IP Maestro.

Maximize Subscribe Paths for Streaming Telemetry

Streaming Telemetry capability enables IP Maestro to monitor network health efficiently with real-time data from devices. Note that, this capability is available on devices running OcNOS Version 6.6 and above.

For effective utilization of this feature, the maximum subscribe paths in OcNOS must be a minimum of 150, so that all the information required for chassis and interfaces can be collected.

- To check the existing value of the sensor path, use the command:

  ```
  # en
  # show streaming-telemetry
  ```

  Verify the maximum sensor-path information in the output.

- To increase the value, use the following command:

  ```
  # en
  # config term
  # maximum-subscribe-paths [value]
  # commit
  ```

  Verify the current value of the Maximum sensor-paths using the Show command.

Configure Host for IP Maestro

To prepare the host for IP Maestro deployment, you must have Docker and Docker Compose installed on it. The following sections describe the Docker verification and installation.

Docker Verification or Installation

To install or update Docker to the latest version on the deployment machine refer to Install Docker.

Prerequisites

- Ensure that Docker, Docker Compose plugin and Wget are installed.

Note: If Wget & Unzip are not installed, install using the command `sudo apt-get install wget unzip -y`.

- Ensure that only one docker installation is running on the host.

Procedure

Ensure Docker Compose version is at least v2.20.2.

1. Install the latest version of Docker on the deployment machine. Refer to Install Docker.
2. Execute the following command to verify the docker version:

   ```
   docker version
   ```

   or

   ```
   docker -v
   ```

3. If the Docker compose version is not 2.20.2 or above, install the Docker Compose plugin. Refer to Uninstall Old Versions.

   Follow the instructions:

   - Setup Docker's apt repository (Ensure to copy and run all commands specified.)
   - Install the Docker packages.

   Note: It is recommended to add the host user to the docker group in a post-installation step.

4. Execute the `sudo usermod -aG docker $USER` command to eliminate the requirement to use `sudo` when executing docker commands and to add your user to the docker group.
5. Execute the following command to validate Docker and Docker Compose version:

   ```
   docker version
   ```

   ```
   docker compose version
   ```

Customize Docker IP Subnet and Bridge Network Settings

Docker Compose creates networks in the range `172.17.0.0/16` by default. However, there is a possibility of picking some other IP blocks, often in the `192.168.0.0/16` range. To avoid conflicts with the local environment, it is advised to specify a suitable IP block.

Follow the steps mentioned below before deploying IP Maestro:

Customize the IP subnet and bridge network settings for Docker Compose by modifying the `daemon.json` file as follows:

1. Open the `daemon.json` file

   ```
   sudo nano /etc/docker/daemon.json
   ```

2. Add the configuration (if the file is empty)

   ```
   "bip": "172.20.0.1/16",
    "default-address-pools": [
      {
        "base": "172.21.0.0/16",
        "size": 24
      }
    ]
   }
   ```

   Here is the description of the commands used to add the configuration:

Command	Description
`bip`	Sets the IP address of the Docker bridge network interface (docker0).
`default-address-pools`	Defines the IP address pools for automatic network creation.
`base`	The starting IP address of the pool.
`size`	The subnet size (for example: 24 for a /24 subnet).

3. Restart Docker

   ```
   sudo systemctl restart docker
   ```

Important considerations:

- **Deployment:** The above steps must be done before IP Maestro deployment. If any deployment is already present, it must be shut down and brought up again.
- **Subnet**: The subnet you choose must be non-conflicting and not overlap with any other networks in your environment.
- **IP Range**: The size parameter in `default-address-pools` determines the size of the subnet. A smaller size (/24) provides more subnets with fewer addresses per subnet, while a larger size (/16) provides fewer subnets with more addresses per subnet.

To troubleshoot Docker installation related issues, refer to Remove Old Docker Installation, Remove Docker Snap Installation.

Get Started with Local License Server

Local License Server (LLS) ensures a secure method to provide licensing capabilities for IP Maestro. Here is the procedure to get started with Local License Server.

Hardware Requirements

IMPORTANT: Local License Server (LLS) needs a unique physical MAC address for ensuring IP Maestro licensing. LLS is a Docker container that must be deployed on the physical host which contains this MAC address for validation. This is either the host where IP Maestro VM is deployed or any other remote host with network connectivity from IP Maestro.

The following are the minimum hardware requirements for LLS:

Hardware	Required/Version
Disk	2 GB
RAM	8 GB
CPU Architecture	X86-64
Operating System	Linux
Operating System Versions	Ubuntu 22.04.5 LTS Debian 12 (bookworm)
Docker Tool Chain	Docker Version Tested 27.3.1 Build ce12230

Deploy and Start Local License Server

Procedure

1. Login to Flexnet Operations with the user credentials.
2. Download the License Installation file `ipi-license-server-prod_2024.08.tar.gz`.
3. Start the Local License Server for the first time (one time only)

```
tar xzf ipi-license-server-prod_2024.08.tar.gz
cd deploy
/deploy-lls.bash
```

Licensing Service is deployed. A quick check can be done with an endpoint URL in the browser:
`http://< LICENSE_SERVER_IP_ADDRESS>:7077/api/1.0/instances/~`

Maintain Local License Server

After the initial setup, you can stop or restart the licensing service using the following commands:

```
cd deploy
docker compose down (stop the license server container)
docker compose up -d (start the license server container)
```

Activate License File

To activate the license file, use the following steps:

1. Copy the license file to `/ipiws/` directory on the system which has the license server deployed.

   For example: `cp myLicenseFile.bin /ipiws/`

2. Run the following command:

```
docker run --rm -v /ipiws:/ipiws ipi-license-server-prod:2024.08 ./
flexnetlsadmin.sh -server http://< LICENSE_SERVER_IP_ADDRESS >:7077/api/1.0/
instances/~ -activate -load /ipiws/myLicenseFile.bin
```

Deploy IP Maestro

If IP Maestro is currently running on your host and you want a fresh installation, you must shutdown the current deployment before installing the new version. For more information, refer to the chapter Shutdown IP Maestro.

If you want an upgrade of IP Maestro, refer to the chapter Upgrade IP Maestro.

Procedure

For a new installation, perform the following to deploy IP Maestro:

1. Login to Flexnet Operations with the user credentials.
2. Download the *.zip* file `IPMA-<VERSION>-<BUILD>.zip`
3. Copy the downloaded *.zip* file to the `/home/user` directory of your Linux server host, where you deploy IP Maestro.
4. Execute the following command to unpack the IP Maestro.zip file:

   ```
   unzip IPMA-<VERSION>-<BUILD>.zip
   ```
5. Execute the following command to navigate into the nsmo folder:

   ```
   cd nsmo
   ```
6. Execute the following command nsmo-init.sh script:

   ```
   ./nsmo-init.sh
   ```
7. Execute the following command to check if images are loaded:

   ```
   docker images
   ```

Example:

```
REPOSITORY                                    TAG              IMAGE ID       CREATED      SIZE
nsmo-sdn                                 3.0.0-227-ipma      bf6339389d12    45 hours ago 834MB
nsmo-portal-server                       3.0.0-9-ipma        618825cabfcd    45 hours ago 1.49GB
nsmo-portal-client                       3.0.0-6-ipma        da053085e090    3 days ago   1.38GB
nsmo-network-monitoring                  3.0.0-2-ipma        122bc186f0aa    7 days ago   223MB
nsmo-logstash                            3.0.0-1-ipma        f711a9786a8f    8 days ago   1.4GB
nsmo-proxy                               3.0.0-1-ipma        51007bd18014    8 days ago   427MB
nsmo-auth                                3.0.0-1-ipma        db37ec7dc27c    8 days ago   522MB
nsmo-dhcp                                1.1.2-29            f9d274f9f472    3 weeks ago  220MB
nsmo-rabbitmq                            3.10-management     5795b4b18b1f    7 weeks ago  246MB
ghcr.io/openconfig/gnmic                 0.38.0              e2cec9ced8bf    6 months ago 118MB
docker.elastic.co/elasticsearch/elasticsearch 8.4.2 2 f8a9577a31d  2 years ago 1.26GB
docker.elastic.co/beats/metricbeat 8.4.2             f36073ca8cbc    2 years ago  496MB
postgres                                 14.4                e09e90144645    2 years ago   376MB
```

At this stage, IP Maestro is deployed with Docker images loaded into a local Docker repository.

Start IP Maestro

This section outlines the steps to initiate the IP Maestro deployment.

Prerequisites

- IP Maestro deployment is installed and Docker images are loaded into the local Docker repository. Refer to the section Deploy IP Maestro.
- IP Maestro deployment requires certificates to guarantee SSL communication between OcNOS devices and IP Maestro stack (Shipping of OcNOS device logs to IP Maestro), and to expose the deployment through `https` protocol. The certificates should be placed/installed in the `nsmo/certs` folder. As part of the IP Maestro startup process, self-signed certificates will be generated and placed inside the `nsmo/certs` folder. This particular step will only be executed during the initial startup call.
- Signed certificates by a Trusted CA Authority, can be used in the deployment instead of self-signed ones. The certificates needs to be placed at `nsmo/certs` folder, and during the first start call, the user must type `false` at the following question: `Use self-signed certificate/key for Portal SSL settings`. The name of the certificate and key will be requested and checked from `nsmo/certs` folder.

Procedure

During startup, questions are presented and default values are preset. To continue with default values, you can hit `<CR>`. The explanations on the options are given below. The user inputs are required only in the first `nsmo-start.sh` call.

Perform the following steps to start IP Maestro:

1. Set up and start IP Maestro containers

   ```
   ./nsmo_start.sh
   ```

   Note: This process creates the deployment, manages dependencies, and starts up containers (takes approximately 15 minutes).

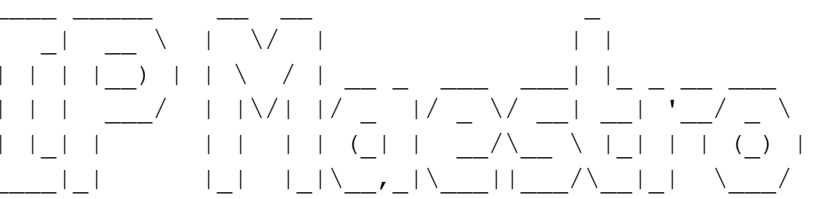
   On running the `nsmo_start.sh` script, user inputs are prompted.

2. Press Enter to select default values for most inputs.

   Note: At this stage, IP Maestro is deployed and Docker image is loaded.

Here is an example of a sample run:

```
# ./nsmo-start.sh
```



```
:: Version 3.0.0-ipma ::

[2025-01-28T20:04:54,789][INFO][host-validation] ----------- Executing Host Validation
[2025-01-28T20:04:54,931][INFO][validate-docker] Docker version: 24.0.5
[2025-01-28T20:04:55,464][INFO][validate-docker-compose] Docker Compose version: 2.25.0
[2025-01-28T20:04:55,528][WARN][validate-host-disk] Total Disk Space: 125GB
```

```
[2025-01-28T20:04:55,532][WARN][validate-host-disk] Host disk space 500GB or higher is
the minimum recommended, but found 125GB
[2025-01-28T20:04:55,536][INFO][validate-host-disk] Available Disk Space: 52GB
[2025-01-28T20:04:55,541][INFO][validate-host-disk] Used Disk Space: 57%
[2025-01-28T20:04:55,579][INFO][validate-host-memory] Total memory: 32GB

[2025-01-28T20:04:55,585][INFO][nsmo-start] ----------- Collecting Host Information
[2025-01-28T20:04:55,589][INFO][nsmo-start] Host IP:           10.14.103.230
[2025-01-28T20:04:55,593][INFO][nsmo-start] Hostname (--fqdn): meg-nsmo-3

[2025-01-28T20:04:55,629][INFO][load-properties] ----------- Checking IP Maestro global
configuration
[2025-01-28T20:04:55,633][INFO][load-properties] Global configuration not present.
Creating ipi-global.cfg and setting required properties

IP Maestro license server IP address []: 10.2.100.20
Push configuration for ALARMS <true/false> [true]:
Push configuration for LLDP <true/false> [true]:
Push configuration for SYSLOG <true/false> [true]:
DHCP interface []:
OcNOS device image repository path []:
OcNOS device license repository path []:
OcNOS login [ocnos]:
OcNOS password [ocnos]:
OcNOS port [830]:

[2025-01-28T20:05:20,685][INFO][config-tls] ----------- Loading IP Maestro TLS/SSL
config
[2025-01-28T20:05:20,691][INFO][config-tls] Creating self-signed certificate/key. Files
will be available for ssl configuration

=======================================================
======== Generating IP MAESTRO Certificate(s) =======
=======================================================

Generating Certificate for host meg-nsmo-3 and ip 10.14.103.230 ...
Using instances.yml file to create certificates...

######### START OF IP Infusion LICENSE BLOCK ###################################
#
# Copyright (C) 2023-2025 IP Infusion, Inc.
# All rights reserved.
#
# This software is the confidential and proprietary information of
# IP Infusion, Inc. ("Confidential Information"). You shall not
# disclose such Confidential Information and shall use it only in
# accordance with the terms of the license agreement you entered into
# with IP Infusion, Inc.
#
######### END OF IP Infusion LICENSE BLOCK #####################################
```

```
# This file is used by elasticsearch-certutil to generate X.509 certificates
# for the Elasticsearch transport networking layer.
# see https://www.elastic.co/guide/en/elasticsearch/reference/current/certutil.html
#
# NOTE Remote connections based on IP is not a good aproach as IPs can change. DNS
should be prefered instead.
instances:
  - name: "CN=Self-Signed,C=US,ST=California,L=Santa Clara,O=IP Infusion,OU=NSMO"
    filename: "selfsigned"
    dns:
      - meg-nsmo-3
    ip:
      - 10.14.103.230


Unzipping Certificates...
Deleting /certs/certs.zip - If it exists...
Creating self-signed PKCS8 key for filebeat from /certs/selfsigned.key
ODL Keystore not found. Creating ODL PKCS12 keystore using self-signed cert and key...
Importing keystore /certs/selfsigned.p12 to /odl/etc/keystore/keystore.jks...
Entry for alias karaf successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or
cancelled
Applying Permissions...

=======================================================
Self-signed Certificate/Key generated successfully.
=======================================================

Use self-signed certificate/key for Portal SSL settings? [true]:
[2025-01-28T20:05:29,801][INFO][config-tls] Use self-signed cert/key settings: true...
[2025-01-28T20:05:29,805][INFO][config-tls] Setting up MY_SSL_CERTIFICATE and
MY_SSL_KEY with self-signed certificate/key from nsmo/certs ...
[2025-01-28T20:05:29,838][INFO][config-tls] Verifying if certificates are present at
nsmo/certs ...

[2025-01-28T20:05:29,898][INFO][config-admin-user] ----------- Defining settings for
User: admin

First Name [IPMA]:
Last Name [Administrator]:
Email [admin@ipinfusion.com]:

[2025-01-28T20:05:32,357][INFO][config-admin-user] First Name: IPMA
[2025-01-28T20:05:32,361][INFO][config-admin-user] Last Name:  Administrator
[2025-01-28T20:05:32,365][INFO][config-admin-user] Email:      admin@ipinfusion.com

Confirm admin settings [y]:

[2025-01-28T20:05:33,913][INFO][config-admin-user] Admin user settings completed...
[2025-01-28T20:05:33,917][INFO][config-admin-user] Changes can be done later in Portal
> System Management > User Management
```

```
[2025-01-28T20:05:33,976][INFO][config-smtp] ----------- Defining settings for SMTP

Host [10.14.103.230]: 10.1.14.102
Port [25]:
From [maestro@ipinfusion.com]:
From Display Name [IP Maestro]:
Reply to Display Name [IP Maestro]:
[2025-01-28T20:05:37,427][INFO][config-smtp] Host:                  10.1.14.102
[2025-01-28T20:05:37,433][INFO][config-smtp] Port:                  25
[2025-01-28T20:05:37,439][INFO][config-smtp] From:
maestro@ipinfusion.com
[2025-01-28T20:05:37,443][INFO][config-smtp] From Display Name:     IP Maestro
[2025-01-28T20:05:37,447][INFO][config-smtp] Reply to Display Name: IP Maestro

Confirm SMTP settings [y]:


[2025-01-28T20:05:38,795][INFO][config-smtp] SMTP settings completed...
[2025-01-28T20:05:38,799][INFO][config-smtp] Changes can be done later in Portal >
System Management > Preferences > SMTP

[2025-01-28T20:05:38,880][INFO][nsmo-start] ----------- Starting IP Maestro Deployment
.
.
.

[2025-01-28T20:13:07,438][INFO][nsmo-start] ----------- IP Maestro Successfully started

[2025-01-28T20:13:07,441][INFO][nsmo-start] IP Maestro Portal Access: https://
10.14.103.230
```

3. Execute the following command to check the status of the containers:

   ```
   watch docker ps
   ```

   Note: Ensure that containers that contain a health check have a `healthy` status.

   Here is an example of the output:

   ```
   *** The following is a short output to show the "healthy" STATUS expected
   NAMES                   STATUS
   ipi-portal-server       Up 35 hours (healthy)
   ipi-odl                 Up 35 hours (healthy)
   ipi-portal-client       Up 35 hours (healthy)
   ipi-rabbitmq            Up 6 days (healthy)
   ipi-dhcp                Up 6 days (healthy)
   ipi-metricbeat          Up 6 days (healthy)
   ipi-proxy               Up 35 hours (healthy)
   ```

```
ipi-keycloak            Up 35 hours (healthy)
ipi-gnmic               Up 45 hours (healthy)
ipi-logstash            Up 35 hours (healthy)
ipi-network-monitoring  Up 35 hours (healthy)
ipi-elasticsearch       Up 6 days (healthy)
ipi-postgresql          Up 6 days (healthy)
```

Log in to the IP Maestro Portal

For logging in to IP Maestro, you must ping the server as follows:

Prerequisites

- The containers are up and running.
- Login credentials.

Procedure

1. Type the IP Maestro portal URL on any web browser. For Example: https://[HOST_IP] for self-signed and https://[fqdn] for private CA certificate.
2. Enter the Username and Password.

   Note: The default username/password is admin/admin123.
3. Click **Sign In**.

   If the username and password are valid, the user is authenticated and redirected to the Portal home page.

Shutdown IP Maestro

This section describes the steps to shut down IP Maestro.

Prerequisites

- IP Maestro must be up and running. Refer to the section Start IP Maestro for more information.

Procedure

Run the `./nsmo-shutdown.sh` script to shutdown IP Maestro services and to clean volumes/data (optional). When no option is specified, only a standard list of services will be terminated. The volumes are not removed to ensure data preservation.

Execute the following command to shutdown IP Maestro and remove containers and volumes:

```
./nsmo-shutdown.sh --all -v
```

Or

Execute the following command to stop and remove containers from the quick list:

```
./nsmo-shutdown.sh     Stop and remove containers from the quick list
./nsmo-shutdown.sh -v   Stop and remove containers from the quick list and
delete volume
./nsmo-shutdown.sh --all  Stop and remove all containers
```

For more information, execute the `-help` command.

Cleanup IP Maestro Deployment

Cleaning up the IP Maestro process involves systematically shutting down all the IP Maestro components, removing associated directories, and purging any superfluous artifacts.

Prerequisites

- IP Maestro must be up and running.

Procedure

Perform the following to clean the IP Maestro:

1. Clean up all the IP Maestro created resources using the command `nsmo - shutdown.sh -- all -v`

   and

   Execute the command `sudo rm -rf nsmo` to completely clean IP Maestro deployment from the host.

   Note: The `sudo rm -rf` command deletes all directories and its contents, including IP Maestro contents.

2. Execute the command `sudo docker system prune -a` to delete all Docker images from the host local repository.

   Here is an example of the warning message displayed while performing the above steps:

```
WARNING! This will remove:
  - all stopped containers
  - all networks not used by at least one container
  - all images without at least one container associated to them
  - all build cache

Are you sure you want to continue? [y/N]
```

Upgrade IP Maestro

You can upgrade an existing installation of the IP Maestro Application without initiating a shutdown or performing a cleanup of the IP Maestro deployment.

IMPORTANT: It is highly recommended to take a backup of the Database, so there is an option to restore in case of a failure. For more information on Database backup, refer to the *Database Management* section in the *IP Maestro User Manual*.

Prerequisites

- IP Maestro must be up and running.

Procedure

Perform the following to upgrade IP Maestro:

1. Create a folder named **update** in the **nsmo** folder.
2. Place the new *.zip* file for deployment in the **nsmo/update** folder.
3. From the **nsmo** folder, run:

   ```
   unzip -o -j update/IPMA-<VERSION>-<BUILD>.zip -d . */nsmo-update.sh
   ```

4. From the **nsmo** folder, run:

   ```
   ./nsmo-update.sh -f IPMA-<VERSION>-<BUILD>.zip
   ```

5. Add the License Server details at the prompt as shown below:

   ```
   [2025-01-27T19:12:41,389][INFO][load-properties] ----------- Checking IP
   Maestro global configuration

   [2025-01-27T19:12:41,397][INFO][load-properties] Adding IP Maestro License
   Server configuration:

   IP Maestro license server IP address []: 10.2.100.20

   [2025-01-27T19:14:30,289][INFO][load-properties] Global configuration updated
   with IP Maestro License Server
   ```

The upgrade process will shutdown and remove containers from the old version, and initialize new ones using the new version loaded. Note that the previous configurations are retained.

Note: PostgreSQL and Elasticsearch databases will not be shut down in order to preserve the existing data.

Troubleshoot IP Maestro

IP Maestro Services Fail

When Maestro services are failing:

- Check Service Status: Execute the Docker commands to ensure all services are up and running:
  - `docker images` (Lists all images)
  - `docker ps` (Displays all running containers)

If any service appears inactive (life cycle phase of restart/ unhealthy/ exited), attempt to restart it by invoking the `nsmo-start.sh` script. If the service remains non-operational even after running the script again, then shut down the service and rerun `nsmo-start.sh`. This recreates the service container from scratch in an attempt to start it.

Access Services through a Specified Port

When you are unable to access services through a specified port, i.e., if any IP Maestro service is inaccessible through the assigned port, check the following:

- Ensure all necessary ports are open in the IP tables.
- Check for potential firewall restrictions or blocks.
- Check the logs of the service container which is failing or is unable to reach the service with docker commands:

  `docker logs -f containerid` or `docker logs -f container-name`

Remove Old Docker Installation

In case you have issues while installing Docker or getting Docker version up to the minimum requirement, uninstall all conflicting packages from the old version. Refer to Uninstall Old Versions.

Remove Docker Snap Installation

If Docker was previously installed with snap, it is recommended to remove it and have docker installation with apt only.

1. Execute the following command to check if Docker is installed with snap:

   ```
   snap list
   ```

2. If Docker is present in the snap list, execute the following command to remove:

   ```
   sudo snap remove --purge docker
   ```

Enhance Performance

To boost configuration and enhance the performance, follow the steps mentioned below:

1. Insert an entry into the `/etc/sysctl.conf` file with the required parameter.

```
vm.max_map_count = 262144
```

Note: This helps to make the changes permanent.

2. Run the following command to change the current state of kernel.

```
sysctl -w vm.max_map_count=262144
```

3. Run the following command to restart the docker for the changes to take effect.

```
systemctl restart docker
```

4. Run the following command to verify the changes after reboot.

```
sysctl vm.max_map_count
```

Appendix

Start Options Description

This section describes the user configuration options during IP Maestro Startup:

1. Set up SSL Certificates: Select the SSL certificates model. Currently support self-signed certificates, but users also have the option to provide their own certificates from a Certificate Authority (CA). The default is set to 'true' for self-signed certificates.

   ```
   Use self-signed certificate/key for Portal SSL settings? [true]: <<<<< <CR>
   ```

   If false is provided, make sure external certificates are placed at nsmo/certs folder in advance. The startup will required the certificate and key names and check their existence at nsmo/certs folder.

   ```
   Use self-signed certificate/key for Portal SSL settings? [true]: false
   [2024-01-25T15:19:41,362][INFO][config-tls] Use self-signed cert/key settings: false...
   [2024-01-25T15:19:41,366][INFO][config-tls] Setting up external SSL certificate/key for Portal. Files MUST be located at nsmo/certs ...
   SSL Certificate Name: fullchain.pem     <<<< Type name of certificate
   SSL Certificate Key Name: privkey.key   <<<< Type name of key
   [2024-01-25T15:19:57,354][INFO][config-tls] Verifying if certificates are present at nsmo/certs ...
   ```

2. Provide local Image and License Repository: IP Maestro supports a local Image and License repository for OcNOS. Users can download images and licenses from this hosted repository, which can be located anywhere (not restricted to the IP Maestro server). The following prompts allow users to specify the repository details.

   ```
   Image upgrade location []: <<<<< <CR>
   License installation path []: <<<<< <CR>
   ```

3. Push Basic Configuration on Device Mount: When mounting devices, IP Maestro pushes basic configurations for LLDP, Beats monitoring, and enabling FMS for Alarms. Users have the option to disable any subset of these configurations. The default is to enable the push.

   ```
   push.configuration.for.ELK <true/false> [true]: <<<<< <CR>
   push.configuration.for.LLDP <true/false> [true]: <<<<< <CR>
   push.configuration.for.ALARMS <true/false> [true]: <<<<< <CR>
   ```

4. OcNOS credentials for SDN service usage and the Netconf port on the device. Default values are set.

   ```
   OcNOS login [ocnos]:      <<<<< <CR>
   OcNOS password [ocnos]:   <<<<< <CR>
   OcNOS port [830]:         <<<<< <CR>
   ```

Call Home Feature

IP Maestro supports the Call Home protocol defined in IETF RFC 8071. The Call-Home Server listens for incoming TCP connections and assumes that the other side of the connection is a device calling home through a NETCONF connection with SSH for management. The Maestro server uses port 4334 for all Call Home connections.

The following is an example which shows a configuration to enable Call Home on a device;

```
OcNOS(config)#netconf callhome
OcNOS(config)#feature netconf callhome enable
OcNOS(config)#reconnect enable
OcNOS(config)#retry-interval 20
OcNOS(config)#callhome server 10.12.104.25 10.12.104.25 port 4334
```

Configure External Databases (LDAP/AD)

In IP Maestro, you can provide users the access to external databases and directories, such as Lightweight Directory Access Protocol (LDAP) and Active Directory (AD). This is an alternate authentication service to the local user database wherein the user interface of IP Maestro utilizes the User Federation capabilities of authentication manager to integrate LDAP and AD.

This section provides a step-by-step guide on how to configure LDAP/AD provider in IP Maestro. A standard LDAP server typically contains an LDAP Data Interchange Format (LDIF) file that holds all the configurations.

The following configurations are demonstrated using the LDIF file shown below:

- 2 Groups: `ldap-admin` and `ldap-user`
- 2 Users:
  - `jbrown123` - part of '*ldap-admin*' and '*ldap-user*' groups.
  - `bwilson` - part of '*ldap-user*' group.

LDIF file

```
dn: dc=keycloak,dc=org
objectclass: dcObject
objectclass: organization
o: Keycloak
dc: Keycloak

dn: ou=People,dc=keycloak,dc=org
objectclass: top
objectclass: organizationalUnit
ou: People

dn: ou=RealmRoles,dc=keycloak,dc=org
objectclass: top
objectclass: organizationalUnit
ou: RealmRoles

dn: uid=jbrown123,ou=People,dc=keycloak,dc=org
objectclass: top
objectclass: person
objectclass: organizationalPerson
```

```
objectclass: inetOrgPerson
uid: jbrown123
cn: James
sn: Brown
mail: jbrown123@keycloak.org
postalCode: 88441
userPassword: password123

dn: uid=bwilson,ou=People,dc=keycloak,dc=org
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: bwilson
cn: Bruce
sn: Wilson
mail: bwilson@keycloak.org
postalCode: 77332
street: Elm 5
userPassword: password123

dn: cn=ldap-admin,ou=RealmRoles,dc=keycloak,dc=org
objectclass: top
objectclass: groupOfNames
cn: ldap-admin
member: uid=jbrown123,ou=People,dc=keycloak,dc=org

dn: cn=ldap-user,ou=RealmRoles,dc=keycloak,dc=org
objectclass: top
objectclass: groupOfNames
cn: ldap-user
member: uid=jbrown123,ou=People,dc=keycloak,dc=org
member: uid=bwilson,ou=People,dc=keycloak,dc=org
```

For detailed information on adding and mapping providers to IP Maestro users, refer to the *User Management* section in *IP Maestro User Manual*.