Troubleshooting Cisco MSX Issues

Revised: June 30, 2021

Order Fails During Provisioning

Problem

When you place an order and the order goes into provisioning but fails during provisioning. MSX service interface indicates that the order provisioning has failed.

Solution

1. Review the tenant event logs web interface to confirm the error occurred during provisioning and not initial validation.
2. The tenant user needs to escalate this issue to the service provider operator.

Note The system will not self-recover even if the unplugged devices are plugged back in.

3. The service provider operator has to login to NSO directly and fix the problem.
   - Ensure that the malfunctioning devices are taken offline.
   - Retry the provisioning operation.

When the NSO provisioning operation completes successfully, it sends the correct notification to the northbound interface, and resets the MSX service interface to the provisioned state.

Order Failed Error Message

Problem

When you place an order and get an order failed message right away (due to first-level call to NSO failing), it means that the order has failed.

Solution

1. Review the tenant Event logs and confirm the error is caused due to first-level call to NSO failing.
2. Deletes the order from the MSX service interface.
3. Place a new order.

Service Ordering Fails

Problem

When you try to order a service, the service ordering fails.

Solution

- Verify if all microservices are running
- Verify orchestration microservice is sending the appropriate provider name to NSO. Confirm that the "Provider Name" is populated correctly by navigating to **Settings** as an Admin.
- Check NSO netconf-north.log. If not, check connectivity between the MSX Portal and the NSO.

Device Registration Fails Due to Incorrect Serial Number

Problem

The device does not get registered with the PnP server and does not return any error if the tenant user enters an incorrect serial number during registration.

NSO PnP server zero touch provisioning works as:

- Tenant users register a device serial number against a device, which associates a device with a tenant, a site and a device, so Cisco MSX knows what type of configurations to push to this device.
- The connected devices call home to the PnP server, register themselves, and wait for the PnP server to push the configuration.

These events happen in any order and if the tenant user registers a device with a serial number that has not called home to the PnP server, the server waits for the device to call the PnP server. If this device never calls (because the serial number is invalid), the PnP server continues to wait.

Solution

Tenant user needs to register the device with the correct serial number. For more information, see the service pack guides on cisco.com.

Obtaining a CPE Password

If a CPE is in True/True/True state, then it should be possible to SSH from the NSO to the CPE. Required information (CPE Management IP Address, username, password) can be obtained from NSO by executing the `show pnp-state device` command as shown below.

```
admin@vms-ncs-sm> show pnp-state device XXX194326WW
pnp-state device XXX194326WW
udi PID:C881-K9,VID:V01,SN:XXX194326WW
device-info 15.5(3)M1
ip-address 11.156.141.167
mgmt-ip 10.254.0.29
port 22
name cpe-XXX194326WW
username admin
password cpe_password
sec-password cpe_password
salt ABCD
remote-node vms-ncs-dm
wan-interface FastEthernet4
lan-interface FastEthernet0
configured true
request backoff
```

```
 added true
 synced true
 is-netsim false
 need-clean false
 pending-exec ""
 last-contact 2015-12-09 01:53:33
 last-clean 0
 [ok][2015-12-09 01:54:14]
```

From NSO, establish an SSH session to the CPE.

```
 admin@vms-ncs-sm> ssh 10.254.0.29
 Password:cpe_password
 router line 11
 router#
```

Physical or Virtual CPE Status

If you want to check the CPE status, execute the following command:

```
admin@ncs-sm> show pnp list
SERIAL        IP ADDRESS       CONFIGURED  ADDED  SYNCED  LAST CONTACT
-------------------------------------------------------------------------------
FJC2012A29P   11.255.255.35    false       false  false   2016-06-08 16:16:28
FJC2013L1SZ   11.255.255.42    false       false  false   2016-06-08 16:17:13
FJC2020L11L   11.255.255.25    false       false  false   2016-06-06 16:27:12


CONFIGURED: Day-0 config. Pushed onto CPE device
ADDED: CPE device is added into NCS
SYNCED: Service configs pushed into device
```

Display Core Data

If you want to check if the firewall, router and such Cloud VPN components are provisioned, you can execute the `show core-data` command as follows. The following example is for a Cloud VPN Advanced Service with Web Security offer:

```
 admin@ncs-sm% show core-data eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1
offering      CVPN;
service-type  FULL;
provider      vms-ottpod1;
tenant        eb272672-e0e4-4344-9a52-68cc3c1d1be1;
remote-node   ncs-dm;
geo-redundant false;
nfv cpe-FJC2027L1NQ {
    isProvisioned true;
}
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-ASA-dev1-esc-device {
    type          vFirewall;
    isProvisioned true;
}
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-CSR-dev1-esc-device {
    type          vRouter;
    isProvisioned true;
}
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-WSA-dev1-esc-device {
    type          vWSA;
```

```
    isProvisioned true;
}
allocations eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-CSR-dev1-esc-device {
    pool-name loopback;
}
```

Core data for VCE

```
 admin@ncs-sm% show core-data eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-2
offering     VCE;
service-type converged;
provider     vms-ottpod1;
tenant       eb272672-e0e4-4344-9a52-68cc3c1d1be1;
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-CSR-dev1-esc-device {
    type          vRouter;
    isProvisioned true;
}
```

Device Registration Fails Due to Incorrect CPE Day -1 Configuration

Problem

Problem When you place an order for a service, the service comprises of devices for sites. These devices must be registered with the MSX service interface.

Problem If the device fails to register with the PnP server, you need to verify that the Day -1 configuration on the CPE allows it to call home to the PnP server.

Solution

1. Log in to the device and verify to which PNP server the device is connected to.
2. Run command show run | s pnp to list the current PnP server that this device is talking to, and examine the output:

   ```
   Router#show run | s pnp pnp
   Router#profile zero-touch transport https ipv4 <IP address> port 443 remotecert ncs
   ```

3. To change the IP address of the PNP server, switch to the configuration mode.

   ```
   Router#config terminal
   Router(config)#
   ```

4. Enter text that you received as output in Step 2, replacing the IP address with the new one.

   ```
   Router(config)#pnp profile zero-touchtransport https ipv4 <IP address> port 443 remotecert ncs
   ```

5. Exit out of Router(config-pnp-init) mode and then out of Router(config) mode.
6. Copy the configuration into flash configuration, by running the following command:

   ```
   Router#copy running-config flash:day--1-config
   Destination filename [day--1-config]?
   %Warning:There is a file already existing with this name
   Do you want to over write? [confirm]
   4609 bytes copied in 0.876 secs (5261 bytes/sec)
   ```

PnP Server CLI Command

Solution PnP Server to IP Device

```
show run | s pnp
Router#show run | s pnp pnp profile zero-touch transport https ipv4 203.35.248.89 port 443
remotecert ncs
```

Solution PnP Server configured with HTTPS and SSL

```
admin@ncs-sm-vbranch> show configuration pnp server
port 443;
use-ssl true;
[ok][2016-05-31 19:33:28]
```

Solution List of devices and states in contact with the PnP Server

```
admin@ncs-sm-vbranch> show pnp list
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT
------------------------------------------------------------------------------
FTX1738AJME 173.36.207.85 true true true 2016-05-23 23:44:44
FTX1738AJMG 173.36.207.81 true true true 2016-05-23 23:43:50
FTX1740ALBX 173.36.207.80 true true true 2016-05-23 23:44:21
SSI184904LG 173.36.207.82 true true true 2016-05-23 23:43:56
SSI185104LT 173.36.207.84 true true true 2016-05-23 23:43:57
[ok][2016-05-23 23:44:49]
```

Solution PNP commands to reset the CPE

```
request pnp reset clean serial xxxxxx
request pnp delete serial xxxxxx
```

If the day-1-config file need changing on CPE use the commands to create a new file and overwrite the existing:

```
tclsh
puts [open "flash:day--1-config" w+] {
aaa new-model
aaa authentication login default none
interface GigabitEthernet0
…..
pnp profile zero-touch
transport https ipv4 x.x.x.x port 443 remotecert ncs
}
Tclquit
```

Solution Viewing device-info through PnP-state

```
admin@ncs-sm-vbranch> show pnp-state device FTX1738AJME
pnp-state device FTX1738AJME
udi PID:ISR4451-X/K9,VID:V02,SN:FTX1738AJME
device-info 15.5(3)S2
ip-address 173.36.207.81
mgmt-ip 10.254.0.1
port 22
name FTX1738AJME
username user-site2
password cisco223
sec-password priv-cisco222
snmp-community-ro cisco
salt ABCD
remote-node ""
wan-interface GigabitEthernet0/0/1
lan-interface GigabitEthernet0/0/0
configured true
request config
added false
synced false
is-netsim false
need-clean false
pending-exec ""
last-contact 2016-05-31 19:29:18
```

```
last-clean 0
reload-upon-delete false
[ok][2016-05-31 19:29:23]
```

Troubleshooting Data Platform Issues

Data Platform is used to get the operational status of devices, collect matrix for device and service. They are customizable by service packs.

The following are some of the problems in Data Platform that can be fixed:

- Blocking of data due to low disk space
- Device health status is down
- No device health status is available
- Device metrics are not available

Blocking of data due to low disk space

The table below lists the issues encountered in Read-Only indices.

Table 1: Read-Only Indices Issues

Problem	Solution

Read-Only indices in Elastic Search blocks you pushing any data to it due to the low disk space	Execute the following command in Kibana:
	`PUT .kibana/_settings`
	`{`
	`"index": {`
	`"blocks": {`
	`"read_only_allow_delete": "false"`
	`}`
	`}`
	`}`

Device Health Status is Down

The table below lists the issues due to which the device health status is down.

Table 2: Device Health Status Down Issues

Problem	Solution
Destination (CSRHUB) IP not set properly	Make sure correct CSRHUB IP is set in NSO under “pnp day0-common manageddevice”.
Destination (CSRHUB) is not reachable from the device	Make CSRHUB reachable.
The beat network does not have access to the device management network	Grant access to the device management network. • If devices are behind a firewall, add rules to the firewall to let the traffic.

Problem	Solution
CSRHUB not letting traffic towards the device	Check CSRHUB license and configurations.

No Device Health Status is Available

The table below lists the issues due to which the device health status may not be available.

Table 3: No Device Health Status Available Issues

Problem	Solution
The heartbeat containers are not up	Make sure containers are up and running in Kubernetes.
Deployment issue-check deployment logs for more info	Depends on what you see in the deployment logs.
• Monitor MS failed to push device data to Cassandra • Monitor MS failed to populate "devicemetrics" for the device • Monitor MS failed to populate "deviceofmetrictype" for the device	Trigger the process on Monitor MS to push the device information to the database. • Get device connection info from Manage MS using "*GET /manage /api/v2/devices/connections/{deviceInstanceId}*". • Trigger the process in Monitor MS using "*POST /monitor/api/v2/devicemetrics/notifications /monitorChangelog*" using the device connection information you got from the previous step.
Beats did not receive correct configs from Monitor MS • Heartbeat containers crashed, and so on.	Restart collecting data by calling "*POST /monitor/api/v2 /devicemetrics/{deviceInstanceId}/start*".

Device Metrics are not Available

The table below lists the issues due to which the device metrics may not be available.

Table 4: No Device Metrics Available Issues

Problem	Solution
snmpbeat containers are not up	Make sure containers are up and running in Kubernetes.
Deployment issue-check deployment logs for more info	Depends on what you see in the deployment logs.
• Monitor MS failed to push device data to Cassandra • Monitor MS failed to populate "devicemetrics" for the device • Monitor MS failed to populate "deviceofmetrictype" for the device	Trigger the process on Monitor MS to push the device information to the database. • Get device connection info from Manage MS using "*GET /manage /api/v2/devices/connections/{deviceInstanceId}*". • Trigger the process in Monitor MS using "*POST /monitor/api/v2/devicemetrics/notifications /monitorChangelog*" using the device connection information you got from the previous step.

Problem	Solution
Beats did not receive correct configs from Monitor MS	Restart collecting data by calling "*POST /monitor/api/v2 /devicemetrics/{deviceInstanceId}/start*".
SNMP authentication failure; means that the credentials in beat configs and on the device itself don't match, so Day0 configs might not be pushed to the device properly.	Double check the Day0 configs to be pushed to the device on Kubernetes master under "*/data/vms/custom-templates/manageddevice/cfg*".
No response from the device might mean that the device is not reachable	Double check the connectivity to the device by checking CSRHUB health and configs and device tunnels.
No response from the device might mean that SNMP port on device is not reachable	Make sure the security groups allow traffic on SNMP port (161).

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.