GEN\_TRA\_Work Instruction to troubleshoot SWT\_DOWN alarm of cisco CSR

|  |  |  |  |
| --- | --- | --- | --- |
|  | | |  |
| Author  Reviewer | Guna  Leo Mallet |
| Owner | Guna |
| Organization | Nokia Optus |
| Approver |  |
| Document ID | GEN\_TRA\_Work Instruction to troubleshoot SWT\_DOWN alarm of cisco CSR |
| Document location |  |
| |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Change History | | | | | | | | | | | Version | Status | Date | Author | Owner | Reviewed by | Reviewed date | Approver | Approval date | Description of changes | | 0.1 | Draft | 12-09-2023 | Guna | Guna |  |  |  |  |  | | 0.2 | Draft | DD-MM-YYYY | YourNameHere | YourNameHere | YourNameHere | DD-MM-YYYY | YourNameHere | DD-MM-YYYY | TypeYourCommentsHere | | 1.0 | Approved | DD-MM-YYYY | YourNameHere | YourNameHere | YourNameHere | DD-MM-YYYY | YourNameHere | DD-MM-YYYY | TypeYourCommentsHere | | |  |
|  | | |  |

**Disclaimer:** This material, including documentation and any related computer programs, is protected by copyright controlled by Nokia Networks. All rights are reserved. Copying, including reproducing, storing, adapting or translating, any or all of this material requires the prior written consent of Nokia Networks. This material also contains confidential information, which may not be disclosed to others without the prior written consent of Nokia Networks.

Contents

[1 Acronyms 1](#_Toc147330218)

[2 Introduction 1](#_Toc147330219)

[2.1 About the document 1](#_Toc147330220)

[2.1.1 Purpose 1](#_Toc147330221)

[3 Prerequisites/Requirements 1](#_Toc147330222)

[3.1.1 NAC integration with NSM Change module 1](#_Toc147330223)

[3.1.2 NAC integration with NSM IM module 1](#_Toc147330224)

[3.1.3 NAC integration with Helix module 1](#_Toc147330225)

[3.1.4 NAC integration with EPNM 1](#_Toc147330226)

[3.1.5 Network Element access via ?(JUMPHOST|ANSIBLE)? 1](#_Toc147330227)

[4 Flow Diagram 1](#_Toc147330228)

[5 Work Instructions 1](#_Toc147330229)

[5.1 High Level Steps 1](#_Toc147330230)

[5.2 Basic Pre Checks 1](#_Toc147330231)

[5.2.1 Log onto EPNM and check device uptime 1](#_Toc147330232)

[5.2.2 Log onto device 1](#_Toc147330233)

[5.2.3 Check device reporting alarm/upstream device logs for network events 1](#_Toc147330234)

# Acronyms

|  |  |  |
| --- | --- | --- |
| Acronym | Expansion | Description |
| CSR | Cell Site Router | Network device used to transport mobile related data from the edge node towards access aggregators |
| AA | Access Aggregator | Network concentration point for multiple CSR’s and NTU’s to transport traffic to remote endpoints |
| NAC | Network Assurance Centre | Tool to automate event handling/management |
| NSM | Network Service Manager | Incident, problem, change, and knowledge tool with integrated CMDB |
| CMDB | Configuration Management Database | Tool to record and attribute inventory and network components to assist in asset management |
| EPNM | Evolved Programmable Network Manager | Cisco Network management System/Element Management System |
| VTeMIP | Virtualized Telecommunication Management Information Platform | Event management/Event processing tool |
| SSH | Secure Shell | Algorithmically secured TCP session to facilitate a remote shell context |
| NGCE | Next Generation Carrier Ethernet | Used to describe specific network platform deployment within the Optus Transport network |
| CE | Carrier Ethernet | Used to describe specific network platform deployment within the Optus Transport network |
| TRA | Transport |  |
| IPM | IP |  |

# Introduction

## About the document

## Purpose

This document describes the step-by-step procedure to work on SWT\_DOWN alarm of Cisco CSRs

# Prerequisites/Requirements

## NAC integration with NSM Change module

Required to check if SWT\_DOWN alarm is due to planned work

## NAC integration with NSM IM module

Required to check if SWT\_DOWN alarm is due to due to power issue/fiber cut/upstream link or node fault

## NAC integration with Helix module

Required to check if SWT\_DOWN alarm is due to ongoing commissioning/decommissioning work

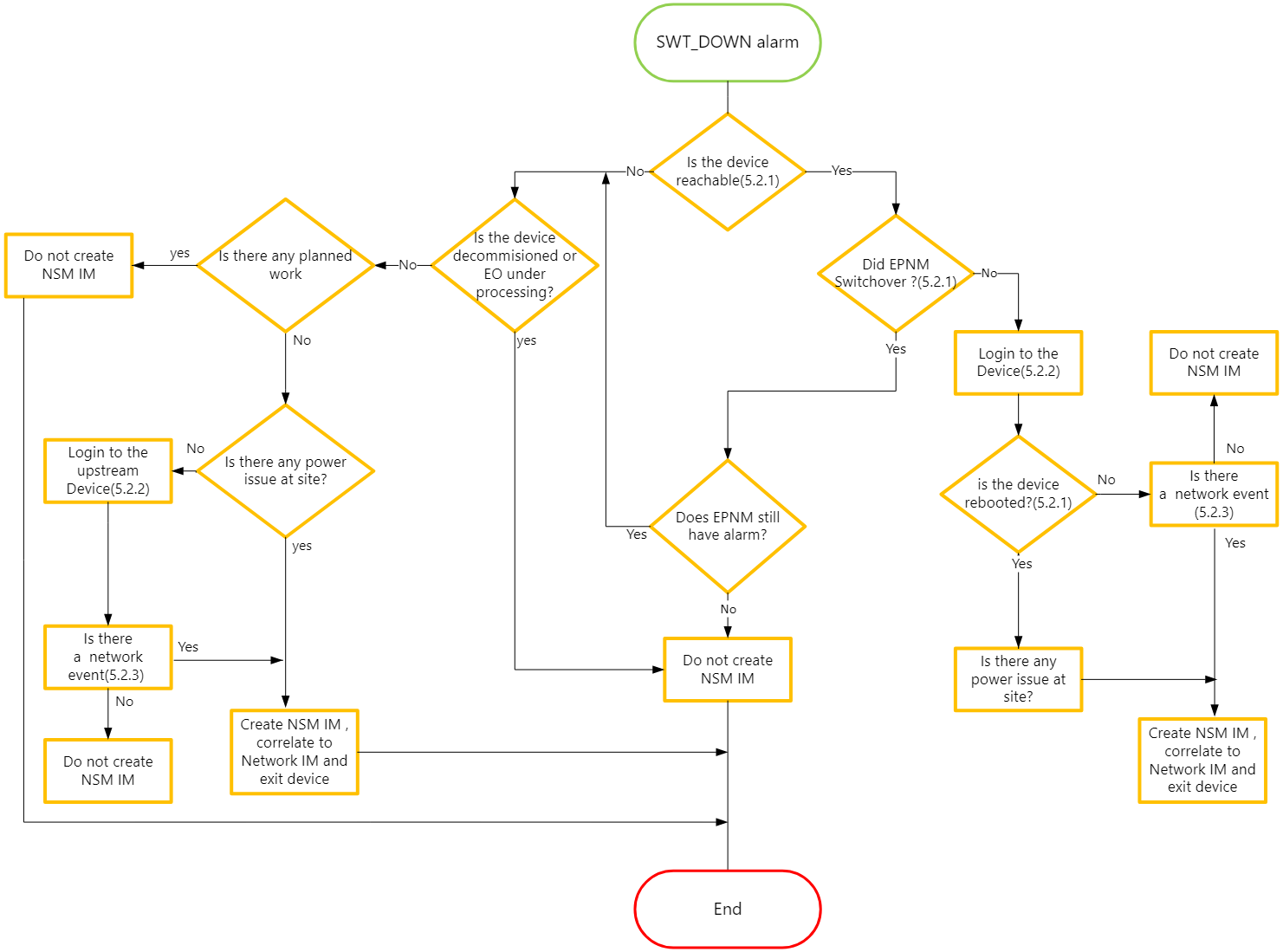
## NAC integration with EPNM

Required to check if it is a genuine or false alarm.

## Network Element access via ?(JUMPHOST|ANSIBLE)?

Required to access node and perform troubleshooting.

# Flow Diagram



# Work Instructions

## High Level Steps

1. Confirm connectivity and uptime of node from EPNM
2. Check if there was EPNM switchover
3. SSH to node
4. Check the uptime and for logs by running show commands
5. Create IM

## Basic Pre Checks

## Log onto EPNM and check device uptime

Purpose: *Enter below command to check the reachability and uptime of the node reporting alarm.*

Where: EPNM

IP add:10.194.228.4

UN: ftpuser

PW:Optus123

Proxy: socks.optusnet.com.au

Port:1080

Command: ping <Device IP> -c 100

snmpwalk -v3 -l authPriv -u mstn -a MD5 -A mstn12345 -x AES -X mstn12345 <Device IP> system

Example: below for ref

**PASS:**

-bash-4.2$ ping 172.29.81.151 -c 100

PING 172.29.81.151 (172.29.81.151) 56(84) bytes of data.

64 bytes from 172.29.81.151: icmp\_seq=1 ttl=247 time=1.27 ms

64 bytes from 172.29.81.151: icmp\_seq=2 ttl=247 time=1.49 ms

64 bytes from 172.29.81.151: icmp\_seq=3 ttl=247 time=1.39 ms

^C

--- 172.29.81.151 ping statistics ---

**3 packets transmitted, 3 received, 0% packet loss, time 2002ms**

rtt min/avg/max/mdev = 1.279/1.389/1.493/0.092 ms

-bash-4.2$

bash-4.2$ snmpwalk -v3 -l authPriv -u mstn -a MD5 -A mstn12345 -x AES -X mstn12345 172.29.81.151 system

SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS XR Software (NCS-540), Version 7.5.2 version1 Copyright (c) 2013-2022 by Cisco Systems, Inc.

SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.3009

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (4202026) **11:40:20.26**

SNMPv2-MIB::sysContact.0 = STRING: NokiaNMCTXN@nka.optusvendor.com.au

SNMPv2-MIB::sysName.0 = STRING: o2uvaa01.optus.com.au

SNMPv2-MIB::sysLocation.0 = STRING: O2UV.0200.F01.34

SNMPv2-MIB::sysServices.0 = INTEGER: 78

-bash-4.2$

**Fail:**

Ping:

-bash-4.2$ ping 172.29.86.204 -c 3

PING 172.29.86.204 (172.29.86.204) 56(84) bytes of data.

--- 172.29.86.204 ping statistics ---

3 packets transmitted, 0 received, 100% packet loss, time 1999ms

SNMP WALK:

-bash-4.2$ snmpwalk -v3 -l authPriv -u mstn -a MD5 -A mstn12345 -x AES -X mstn12345 172.29.86.204 system

snmpwalk: Timeout (Sub-id not found: (top) -> system)

-bash-4.2$

Note: If ping is successful and SNMP walk fails, SNMP configuration can be incorrect on the device.

**Validation Criteria**

* **Pass: Device is reachable**
* **Fail: Device is not reachable**

Check if there was any recent HA switchover

## Log onto device

From a permitted host, SSH using StaffAuth credentials to the alarmed device.

<IMG to SSH + CRED + PROMPT>

**Pass:**

**nau-cp822001---User name**

**172.29.81.151-Device management IP**

-bash-4.2$ ssh nau-cp822001@172.29.81.151

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* Unauthorised Access Prohibited \*

\* All activity is monitored and logged \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* WARNING: It is a criminal offence to: \*

\* i. Obtain access to data without authority \*

\* (Penalty 2 years imprisonment) \*

\* ii. Damage, delete, alter or insert data without authority \*

\* (Penalty 10 years imprisonment) \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Password: ----🡪 prompt for password and should be able to login to device with TACACS consumer credentials.

RP/0/RP0/CPU0:o2uvaa01#

**Fail: No response**

-bash-4.2$ ssh nau-cp822001@172.29.86.204

^C

-bash-4.2$

**Validation Criteria**

* **Pass: Connection is successfull**
* **Fail: Connection is not successfull**

## Check device reporting alarm/upstream device logs for network events

Purpose: Check for alarms on upstream links in device logs

Where: Node

Command: show logging

**Note:** This will be taken care by advanced correlation and will be implemented in next phase.

**NGCE:**

LINK\_DOWN

ROUTING-ISIS-5-ADJCHANGE

BGP-5-ADJCHANGE

**NGTT+:**

LINK\_DOWN

%ROUTING-OSPF-5-ADJCHG

BGP-5-ADJCHANGE

**Validation Criteria**

* **Pass: no logs matching the alarm name and continue checking upstream network elements**
* **Fail: Logs are avaibalbe**

**X---------------------------------------------------------- End of Document ----------------------------------------------------X**