NSP
Network Services Platform
Release 24.8

Troubleshooting Guide

3HE-20033-AAAB-TQZZA
Issue 2
July 2025

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

About this document

Purpose

The *NSP Troubleshooting Guide* provides information about using NSP, NFM-P tools, and other functions to troubleshoot customer services and the NSP network management domain.

Scope

The scope of this document is limited to the NSP application and the NFM-P. Many configuration, monitoring, and assurance functions are delivered by NSP. Help for all of these NSP functions is available in the NSP Help Center. The content in this document is divided by relevance to the NSP and NFM-P.

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Please send your feedback to Documentation Feedback.

Part I: Troubleshooting overview

Overview

Purpose

This part provides an overview of NSP troubleshooting.

Contents

1 NSP troubleshooting overview

1.1 Overview

1.1.1 General information

This chapter provides information about the troubleshooting process, guidelines, and tools, along with a process for troubleshooting a problem in the NSP.

The *NSP Troubleshooting Guide* is intended for NOC operators and engineers who are responsible for identifying and resolving NSP performance issues. The guide contains troubleshooting information for the following domains:

- managed network
- NSP functions
- NSP platform
- NFM-P platform

1.1.2 Managed network troubleshooting

The NSP has a number of powerful troubleshooting functions and dashboards that help to quickly pinpoint the root cause of network and service management problems to speed resolution.

You can use the NSP alarm and service monitoring functions to help you troubleshoot the network of managed NEs.

Alarms for network objects

The NSP raises alarms against network objects in response to received SNMP traps from managed NEs. You can then use the alarms function to correlate the events and alarms to the managed object, configured services and policies. A correlated event or alarm can cause fault conditions on multiple network objects and services. For example, an alarm raised for a port failure causes alarms on all services that use the port. You can view the alarm notification from the Network Health dashboard.

1.1.3 Platform troubleshooting

You can troubleshoot NSP platform issues that include the following:

- slow system response, poor performance, or excessive disk activity
- database failure, corruption, disk capacity, or performance degradation
- server communication problems, slow response, system alarms or statistics of concern, or inability to manage new devices

1.2 The troubleshooting process

1.2.1 Identifying network performance issues

The troubleshooting process identifies and resolves performance issues related to a network service or component. The performance issue can result in service degradation, or in a complete network failure.

The first step in problem resolution is to identify the problem. Problem identification can include an alarm received from a network component, an analysis of network capacity and performance data, or a customer problem report.

The personnel responsible for troubleshooting the problem must:

- understand the designed state and behavior of the network, and the services that use the network
- recognize and identify symptoms that impact the intended function and performance of the product

1.2.2 Network maintenance

The most effective method to prevent problems is to schedule and perform routine maintenance on your network. Major networking problems often start as minor performance issues. See the *NSP System Administrator Guide* for more information about how to perform routine maintenance on your network.

1.2.3 Troubleshooting problem-solving model

An effective troubleshooting problem-solving model includes the following tasks:

1. “Establish a performance baseline” (p. 14) .
2. “Categorize the problem” (p. 15) .
3. “Identify the root cause of the problem” (p. 15) .
4. “Plan corrective action and resolve the problem” (p. 16) .
5. “Verify the solution to the problem” (p. 16) .

See 1.4 “Process to troubleshoot a problem in the NSP” (p. 19) for information about how the problem-solving model aligns with using the NSP to troubleshoot a network or network management problem.

Establish a performance baseline

You must have a thorough knowledge of your network and how it operates under normal conditions to troubleshoot problems effectively. This knowledge facilitates the identification of fault conditions in your network. You must establish and maintain baseline information for your network and services. The maintenance of the baseline information is critical because a network is not a static environment.

See the *NSP System Administrator Guide* for more information on how to generate NSP system baseline information.

Categorize the problem

When you categorize a problem, you must differentiate between total failures and problems that result in a degradation in performance. For example, the failure of an access switch results in a total failure for a customer who has one DS3 link into a network. A core router that operates at over 80% average utilization can start to discard packets, which results in a degradation of performance for services that use the device. Performance degradations exhibit different symptoms from total failures and may not generate alarms or significant network events.

Multiple problems can simultaneously occur and create related or unique symptoms. Detailed information about the symptoms that are associated with the problem helps the NOC or engineering operational staff diagnose and fix the problem. The following information can help you assess the scope of the problem:

- alarm files
- error logs
- network statistics
- network analyzer traces
- output of CLI show commands
- accounting logs
- customer problem reports

Use the following guidelines to help you categorize the problem:

- Is the problem intermittent or static?
- Is there a pattern associated with intermittent problems?
- Is there an alarm or network event that is associated with the problem?
- Is there congestion in the routers or network links?
- Has there been a change in the network since proper function?

Identify the root cause of the problem

A symptom for a problem can be the result of more than one network issue. You can resolve multiple, related problems by resolving the root cause of the problem.

Use the following guidelines to help you implement a systematic approach to resolve the root cause of the problem:

- Identify common symptoms across different areas of the network.
- Focus on the resolution of a specific problem.
- Divide the problem based on network segments and try to isolate the problem to one of the segments.

  Examples of network segments are:
  - LAN switching (edge access)
  - LAN routing (distribution, core)
  - metropolitan area
  - WAN (national backbone)
  - partner services (extranet)
  - remote access services
- Determine the network state before the problem appeared.

- Extrapolate from network alarms and network events the cause of the symptoms. Try to reproduce the problem.

Plan corrective action and resolve the problem

The corrective action required to resolve a problem depends on the problem type. The problem severity and associated QoS commitments affect the approach to resolving the problem. You must balance the risk of creating further service interruptions against restoring service in the shortest possible time.

Corrective action should:

1. Document each step of the corrective action.
2. Test the corrective action.
3. Use the CLI to verify behavior changes in each step.
4. Apply the corrective action to the live network.
5. Test to verify that the corrective action resolved the problem.

Verify the solution to the problem

You must make sure that the corrective action associated with the resolution of the problem did not introduce new symptoms in your network. If new symptoms are detected, or if the problem has only recently been mitigated, you need to repeat the troubleshooting process.

1.2.4 Checklist for identifying problems

When a problem is identified in the network management domain, track and store data to use for troubleshooting purposes:

- Determine the type of problem.

  Review the sequence of events before the problem occurred:
  - Trace the actions that were performed to see where the problem occurred.
  - Identify what changed before the problem occurred.
  - Determine whether the problem happened before under similar conditions.
- Check the documentation or your procedural information to verify that the steps you performed followed documented standards and procedures.
- Check the alarm log for any generated alarms that are related to the problem.
- Record any system-generated messages, such as error dialog boxes, for future troubleshooting.
- If you receive an error message, perform the actions recommended in the error dialog box, client GUI dialog box, SOAP exception response, or event notification.

During troubleshooting:

- Keep both the Nokia documentation and your company policies and procedures nearby.
- Check the appropriate release notice from the Nokia Support Documentation Service for any release-specific problems, restrictions, or usage recommendations that relate to your problem.

- If you need help, confirmation, or advice, contact your TAC or technical support representative. See Table 1-1, “General NSP problem types” (p. 20) to collect the appropriate information before you call support.
- Contact your TAC or technical support representative if your company guidelines conflict with Nokia documentation recommendations or procedures.
- Perform troubleshooting based on your network requirements.

1.3 NSP and NFM-P troubleshooting tools

1.3.1 NSP troubleshooting tools

NSP provides various functions and dashboards that can help your troubleshoot network, provide various alarm details, and see the network health.

Network Health dashboard

The Network Health dashboard provides a quick view of essential information relating to the proper function of your network. It presents an abbreviated view of equipment and service alarms, root cause alarms, graphical plots of service-affecting network object counts, and network object status.

Troubleshooting dashboard

The Troubleshooting dashboard provides the user with a centralized view of network equipment and service performance. The dashboard allows a network operator to view summarized performance information, and to drill down into specific objects and view performance details, opening objects in NSP functions where necessary. See the *NSP User Guide* for more information.

Assurance functions

Various NSP assurance and analysis functions are available..

Current Alarms

The alarms management function provides alarm monitoring, correlation, and troubleshooting for the most unhealthy network elements (NE) in the network. You can diagnose problems using various alarm management tools. See the *NSP Network and Service Assurance Guide*.

Data Collection and Analysis

NSP Analytics uses business intelligence software to generate graphical and tabular reports, based on the aggregate statistical data and telemetry collected from NEs. There are four categories of reports available to you: Network and service, Application assurance, Administration, and NSP. See the *NSP Analytics Report Catalog* for more information.

Network and service assurance

The network and service assurance functions help you to monitor the health of core, access, transport, and optical NEs and virtual NFs using a combined NE matrix, pre-defined KPIs, alarms, event timeline, and network map. See the *NSP Network and Service Assurance Guide* for more information.

1.3.2 NFM-P troubleshooting tools

The NFM-P supports a number of troubleshooting tools and event logs to help identify the root cause of a network or network management problem.

OAM diagnostics

The NFM-P supports configurable in-band and out-of-band, packet-based OAM diagnostic tools for network troubleshooting and for verifying compliance with SLAs. See 6.2.1 “STM OAM diagnostics for troubleshooting” (p. 333) for more information.

Ethernet CFM diagnostics

Ethernet CFM diagnostic tests detect connectivity failures between pairs of local and remote maintenance end points, or MEPs, in a MEG. Each MEP is a reference point that can initiate or terminate one of the following diagnostic tests:

- CFM continuity check
- CFM loopback
- CFM link trace
- CFM Eth test
- CFM two-way delay
- CFM one-way delay
- CFM single-ended loss (7705 SAR only)
- CFM two-way SLM

See the *NSP NFM-P Classic Management User Guide* for more information about Ethernet CFM diagnostic.

RCA audit tool

The NFM-P RCA audit tool allows you to perform on-demand or scheduled verifications of the configuration of services and physical links to identify possible configuration problems. Except for physical links, the NFM-P provides a solution, which, at your request, can automatically be implemented to make all the required configuration changes.

You can perform RCA audits of the following objects:

- VLL services
- VPLSs
- VPRN services
- physical links
- OSPF interfaces, areas, and area sites (NFM-P/CPAM integration only)
- IS-IS interfaces and sites (NFM-P/CPAM integration only)

See the *NSP NFM-P Classic Management User Guide* for more information about the RCA audit tool.

NFM-P log files

You can use NFM-P log files to help troubleshoot your network. The log files can consume a large amount of disk space during a long period of significant activity. Ensure that the contents of the various log directories are backed up on a regular basis. See the *NSP System Administrator Guide* for more information about how to perform routine NFM-P system maintenance.

Note: The event log files may be overwritten or removed when you restart an NFM-P server.

NFM-P LogViewer

The NFM-P LogViewer is a system monitoring and troubleshooting utility that parses, formats, and displays the contents of NFM-P log files.

You can use LogViewer to perform the following:

- View and filter real-time log updates.
- View, filter, and sort the entries in a static log view.
- Open compressed or uncompressed log files.
- Compare active logs in real time.
- Automatically send a notification when a specified type of entry is logged.

User activity log

The NFM-P records each NFM-P GUI and OSS user action. The NFM-P User Activity form allows an operator with the appropriate privilege level to list and view the NFM-P GUI and OSS client user activity, and to navigate directly to the object of a user action. You can also open a pre-filtered list of the recent activity for an object from the object properties form.

See the *NSP NFM-P Classic Management User Guide* for detailed information about the user activity log.

1.4 Process to troubleshoot a problem in the NSP

1.4.1 Purpose

Perform the following high-level sequence of actions with respect to the problem-solving model described in 1.2 “The troubleshooting process” (p. 14) .

1.4.2 Stages

1

Establish an operational baseline for your network. See the *NSP System Administrator Guide* for more information.

2

When a problem occurs, identify the type of problem. The table below lists some general NSP problem types.

Table 1-1 General NSP problem types

Type	Example problems
Managed network	• alarms raised against network objects • service degradation with no associated alarms • problem indications on topology maps
Service and network health	• network health issues • error or warning messages related to configuration • problem encountered during diagnose
NSP platform	• pod failure • errored cluster member • disk capacity or performance issues • MDM server issues

3

Identify the root cause of the problem using NSP or NFM-P procedures in the document

a. Use Table 1-2, “NSP functions and dashboards problems or tasks” (p. 20) to identify the appropriate NSP function troubleshooting procedure for the problem.

b. Use Table 1-3, “NSP platform problems or tasks” (p. 21) to identify the appropriate NSP platform troubleshooting procedure for the problem.

c. Use Table 1-4, “NFM-P managed NE network problems or tasks” (p. 21) to identify the appropriate NFM-P managed NE network troubleshooting procedure for the problem.

d. Use Table 1-5, “NFM-P network management domain problems or tasks” (p. 22) to identify the appropriate NFM-P network management domain troubleshooting procedure for the problem.

e. Use Table 1-6, “NFM-P platform problems or tasks” (p. 22) to identify the appropriate NFM-P platform troubleshooting procedure for the problem.

Table 1-2 NSP functions and dashboards problems or tasks

Problem or task
Troubleshooting using alarms
5.2 “Troubleshooting services and connectivity” (p. 112)
5.4 “Onboarding a service into NSP” (p. 155)
Troubleshooting NSP Analytics
5.12 “Troubleshooting data collection” (p. 319)
5.13 “Troubleshooting data storage” (p. 322)
5.14 “Troubleshooting Analytics reporting” (p. 322)

Table 1-3 NSP platform problems or tasks

Problem or task
Troubleshooting NFM-P platform problems
3.1 “To collect NSP log files” (p. 29)
3.2 “To retrieve a list of pods” (p. 30)
3.3 “To retrieve pod information” (p. 30)
3.4 “To recover pods” (p. 30)
3.5 “To recover executor pods” (p. 31)
3.6 “To retrieve a list of cluster members” (p. 32)
3.7 “To retrieve cluster member information” (p. 32)
3.8 “To retrieve detailed information about MDM servers” (p. 33)
3.9 “To rebalance NE load on MDM servers” (p. 34)
3.10 “To verify disk performance for etcd” (p. 35)
3.11 “To verify disk performance for NSP” (p. 36)
3.12 “Problem: NSP data synchronization is not 100%” (p. 38)
3.13 “Problem: Alarms not appearing for rapidly reoccurring faults” (p. 38)

Table 1-4 NFM-P managed NE network problems or tasks

Problem or tasks
Troubleshooting services and connectivity
6.4 “To identify whether a VPLS is part of an H-VPLS” (p. 335)
6.5 “To verify the operational and administrative states of service components” (p. 336)
6.6 “To verify the FIB configuration” (p. 337)
6.7 “To verify connectivity for all egress points in a service using MAC Ping and MAC Trace” (p. 338)
6.8 “To verify connectivity for all egress points in a service using MEF MAC Ping” (p. 340)
6.9 “To measure frame transmission size on a service using MTU Ping” (p. 342)
6.10 “To verify the end-to-end connectivity of a service using Service Site Ping” (p. 343)
6.11 “To verify the end-to-end connectivity of a service tunnel using Tunnel Ping” (p. 345)
6.12 “To verify end-to-end connectivity of an MPLS LSP using LSP Ping” (p. 347)
6.13 “To review the route for an MPLS LSP using LSP Trace” (p. 349)
6.14 “To review ACL filter properties” (p. 350)
6.15 “To view anti-spoof filters” (p. 351)
6.16 “To retrieve MIB information from a GNE using the snmpDump utility” (p. 352)

Table 1-5 NFM-P network management domain problems or tasks

Problem or task
Troubleshooting network management LAN issues
6.22 “Problem: All network management domain stations experience performance degradation” (p. 359)
6.23 “Problem: Lost connectivity to one or more network management domain stations” (p. 359)
6.24 “Problem: Another station can be pinged, but some functions are unavailable” (p. 360)
6.25 “Problem: Packet size and fragmentation issues” (p. 361)
Troubleshooting using NFM-P client GUI warning messages
6.27 “To respond to a GUI warning message” (p. 364)
Troubleshooting with Problem Encountered forms
6.29 “To view additional problem information” (p. 366)
6.30 “To collect problem information for technical support” (p. 367)
Troubleshooting with the client activity log
6.32 “To identify the user activity for a network object” (p. 368)
6.33 “To identify the user activity for an NFM-P object” (p. 369)
6.34 “To navigate to the object of a user action” (p. 370)
6.35 “To view the user activity records of an object” (p. 371)

Table 1-6 NFM-P platform problems or tasks

Problem or task
Troubleshooting NFM-P platform problems
4.2 “To collect NFM-P log files” (p. 44)
4.3 “Problem: Poor performance on a RHEL station” (p. 46)
4.4 “Problem: Device discovery fails because of exceeded ARP cache” (p. 48)
Troubleshooting with the NFM-P LogViewer
4.8 “To display logs using the LogViewer GUI” (p. 53)
4.9 “To configure the LogViewer using the GUI” (p. 58)
4.11 “To show or hide buttons from the LogViewer main tool bar” (p. 62)
4.12 “To set highlight colors and fonts for LogViewer components and levels” (p. 63)
4.13 “To automatically show or hide log messages” (p. 64)
4.14 “To manage filters using the GUI Filter Manager” (p. 65)
4.15 “To specify a plug-in using the LogViewer GUI” (p. 67)
4.16 “To display logs using the LogViewer CLI” (p. 68)
4.17 “To configure the LogViewer CLI” (p. 72)

Table 1-6 NFM-P platform problems or tasks (continued)

Problem or task
4.18 “To specify plug-ins using the CLI” (p. 74)
Troubleshooting the NFM-P database
4.20 “Problem: NFM-P database corruption or failure” (p. 75)
4.21 “Problem: The database is running out of disk space” (p. 76)
4.22 “Problem: Frequent database backups create performance issues” (p. 77)
4.23 “Problem: An NFM-P database restore fails and generates a No backup sets error” (p. 78)
4.24 “Problem: NFM-P database redundancy failure” (p. 78)
4.25 “Problem: Primary or standby NFM-P database is down” (p. 79)
4.26 “Problem: Need to verify that Oracle database and listener services are started” (p. 79)
4.27 “Problem: Need to determine status or version of NFM-P database or Oracle proxy” (p. 80)
Troubleshooting NFM-P server issues
4.29 “Problem: Cannot start an NFM-P server, or unsure of NFM-P server status” (p. 82)
4.30 “Problem: NFM-P server and database not communicating” (p. 86)
4.31 “Problem: An NFM-P server starts up, and then quickly shuts down” (p. 87)
4.32 “Problem: Client not receiving server heartbeat messages” (p. 87)
4.33 “Problem: Main server unreachable from RHEL client station” (p. 88)
4.34 “Problem: Excessive NFM-P server-to-client response time” (p. 89)
4.35 “Problem: Unable to receive alarms on the NFM-P, or alarm performance is degraded” (p. 90)
4.36 “Problem: All SNMP traps from managed devices are arriving at one NFM-P server, or no SNMP traps are arriving” (p. 91)
4.37 “Cannot manage new devices” (p. 92)
4.38 “Problem: Cannot discover more than one device, or device resynchronization fails” (p. 93)
4.39 “Problem: Slow or failed resynchronization with network devices” (p. 94)
4.40 “Problem: Statistics are rolling over too quickly” (p. 95)
Troubleshooting NFM-P GUI and OSS clients
4.42 “Problem: Cannot start NFM-P client, or error message during client startup” (p. 98)
4.43 “Problem: NFM-P client unable to communicate with NFM-P server” (p. 99)
4.44 “Problem: Delayed server response to client activity” (p. 100)
4.45 “Problem: Cannot place newly discovered device in managed state” (p. 101)
4.46 “Problem: User performs action, such as saving a configuration, but cannot see any results” (p. 102)
4.47 “Problem: Device configuration backup not occurring” (p. 104)
4.48 “Problem: NFM-P client GUI shuts down regularly” (p. 105)

Table 1-6 NFM-P platform problems or tasks (continued)

Problem or task
4.49 “Problem: Configuration change not displayed on NFM-P client GUI” (p. 106)
4.50 “Problem: List or search function takes too long to complete” (p. 106)
4.51 “Problem: Cannot select some menu options or save some configurations” (p. 107)
4.52 “Problem: The NFM-P client GUI does not display NE user accounts created, modified, or deleted using the CLI” (p. 107)

4

Plan corrective action using information in the *NSP User Guide* and *NSP System Administrator Guide*.

5

Verify the solution.

2 Obtaining Technical Assistance

2.1 Before you call support

2.1.1 Monitor NSP KPIs

You can use the NSP logging and monitoring functions to view the current system status using a wide variety of KPIs; see “NSP logging and monitoring” in the *NSP System Administrator Guide* for information.

2.1.2 Gather information

Collect the following information before you contact technical support.

Table 2-1 Required technical-support Information

Information type	Description
Issue description	• recent GUI or XML API operations • screen captures or text versions of error or information messages • actions performed in response to the issue
Platform specifications	• NSP software Release and patch level • NFM-P software release ID • OS type, release, and patch level • hardware information such as: - CPU type - number of CPUs - disk sizes, partition layouts, and RAID configuration - amount of RAM
System logs	System logs are crucial for system troubleshooting; see th appropriate topic in this chapter for specific log-collection information.

2.1.3 To collect NSP system logs

You can run the following script to collect the log files required by technical support:

- on the deployer
  /opt/nsp/NSP-CN-DEP-*releaseID*/NSP-CN-*releaseID*/tools/support/systemDebugInfo/bin/get-debug-info.bash
  where *releaseID* is the NSP load name in the format N.n.n-rel.n, for example, 23.4.0-rel.2994
- on an NSP auxiliary database station:
  /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh getDebugFiles

2.1.4 To collect NFM-P system logs

You can run the following scripts to collect the log files required by technical support:

- on a main server station:
  /opt/nsp/nfmp/server/nms/bin/getDebugFiles.bash
- on an auxiliary server station:
  /opt/nsp/nfmp/auxserver/nms/bin/getDebugFiles.bash
- on a main database station:
  /opt/nsp/nfmp/db/install/getDebugFiles.bash

2.1.5 Check the disk space on your deployer

A common cause of failures during patch upgrades, such as images failing to import, is due to the deployer having run out of disk space. If you experience a failure such as “Error: patch.yml experienced an error” while performing an upgrade, check your deployer’s disk space.

Part II: Troubleshooting the system

Overview

Purpose

This part provides information about NSP and NFM-P platform troubleshooting.

Contents

3 Troubleshooting the NSP platform

3.1 To collect NSP log files

3.1.1 NSP auxiliary database

If required, use a script to collect a comprehensive set of log files.

1

Log in to the station as the root user.

2

Open a console window.

3

Enter the following:

- On an auxiliary database station:
  # **/opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh getDebugFiles *output_dir days*** ↵
  where
  output_dir is a local directory that is to contain the output files
  days is the optional number of days for which to collect log files

Note: You cannot specify /tmp, or any directory below /tmp, as the output directory.

4

Collect the output files:

- *hostname_date*.WsInfoFiles.*checksum*.tar.gz
  Contains station-specific information such as the hardware and network configuration
- *hostname_date*.ServerLogFiles.*checksum*.tar.gz
  Contains server and JBoss logs, and configuration information
- *hostname_date*.DBLogFiles.*checksum*.tar.gz
  Contains NFM-P database logs and configuration information

END OF STEPS

3.2 To retrieve a list of pods

3.2.1 Steps

1

Enter the following command to view a list of pods in the NSP cluster:

```
# kubectl get pods -A ↵
```

END OF STEPS

3.3 To retrieve pod information

3.3.1 Steps

1

Enter the following to view information about a specific pod:

```
# kubectl describe pod --namespace pod_namespace pod_name ↵
```

where *pod_namespace* is the name of the pod's namespace and *pod_name* is the name of the pod

Note: Ensure the full name of the pod is entered for *pod_name*. To find the full name of a pod, see the procedure 3.2 "To retrieve a list of pods" (p. 30).

2

The command output includes many parameters, including any events associated with the pod. For example:

```
Type     Reason            Age         From               Message
----     ------            ----        ----               -------
Warning  FailedScheduling  <unknown>   default-scheduler  0/1 nodes are
available: 1 Insufficient memory.
```

END OF STEPS

3.4 To recover pods

3.4.1 Steps

1

Enter the following command to recover a pod:

```
# kubectl delete pod --namespace pod_namespace pod_name ↵
```

where *pod_namespace* is the name of the pod's namespace and *pod_name* is the name of the pod

Note: Ensure the full name of the pod is entered for *pod_name*. To find the full name of a pod, see the procedure 3.2 “To retrieve a list of pods” (p. 30).

2

The pod is automatically redeployed. You can use the command to recover a pod in an errored state.

END OF STEPS

3.5 To recover executor pods

3.5.1 Executor pods

The following applications use executor and driver pods:

- act-pipeline-app
- rta-anomaly-detector-app
- rta-trainer-app
- rta-windower-app

An executor pod name has the following format:

app_name-instance-exec-*executor_ID*

where

app_name is the application name

instance is the pod instance ID

executor_ID is a number that identifies the executor instance

3.5.2 Steps

1

Enter the following to recover an executor pod, where *pod_namespace* is the name of the pod’s namespace and *app_name* is the application name:

```
# kubectl delete pod --namespace pod_namespace app-name-driver ↵
```

2

The driver pod is automatically redeployed, thereby recovering any associated errored executor pods.

END OF STEPS

3.6 To retrieve a list of cluster members

3.6.1 Steps

1

Enter the following to list the NSP cluster members:

```
# kubectl get nodes ↵
```

END OF STEPS

3.7 To retrieve cluster member information

3.7.1 Steps

1

Enter the following to view information about a specific member:

```
# kubectl describe nodes node_name ↵
```

where *node_name* is the name of the member to view

2

The command output includes member information such as the following:

- member status; for example:

```
Type Status LastHeartbeatTime LastTransitionTime Reason Message
---- ------ ----------------- ------------------ ------ -------
NetworkUnavailable False Wed, 30 Sep 2020 12:19:23 -0400 Wed, 30 Sep 2020 12:19:23 -0400
CalicoIsUp Calico is running on this node
```

- member resource capacity; for example:

```
Capacity:
  cpu:                24
  ephemeral-storage:  67092472Ki
  hugepages-1Gi:      0
  hugepages-2Mi:      0
  memory:             64381888Ki
  pods:               110
```

- running pods on the member; for example:

```
Namespace Name CPU Requests CPU Limits Memory Requests Memory Limits AGE
--------- ---- ------------ ---------- --------------- ------------- ---
default nginx-ingress-controller-8fj7s 100m (0%) 12 (37%) 500Mi (0%) 1000Mi (0%) 7h9m
default nspos-app1-tomcat-8597d67787-wdgxd 5100m (16%) 12100m (38%) 17230Mi (13%) 17230Mi
(13%) 7h10m
default nspos-neo4j-core-default-1 2050m (6%) 2050m (6%) 2650Mi (2%) 2650Mi (2%) 7h10m
default nspos-postgresql-primary-0 6050m (19%) 6050m (19%) 1290Mi (1%) 1290Mi (1%) 7h9m
```

- resources allocated to the member; for example:

```
Resource           Requests          Limits
--------           --------          ------
cpu                22870m (71%)      41150m (129%)
memory             42120228Ki (32%)  44290630912 (33%)
ephemeral-storage  0 (0%)            0 (0%)
```

END OF STEPS

3.8 To retrieve detailed information about MDM servers

Note: The NSP system must be operational before these operations can be performed.

3.8.1 Steps

1

From the NSP deployer host software directory, enter the following to show the MDM server roles, the number of NEs managed using MDM, and which MDM server is hosting which NE:

```
# tools/mdm/bin/server-load.bash --user username --pass
password--detail
```

where

username is the NSP username

password is the NSP password

2

The command output includes information such as the following:

```
{
    "mdmInstanceInfos": [
      {
           "name": mdm-server-0,
           "ipAddress": mdm-server-0.mdm-server-svc-headless.default.
svc.cluster.local,
           "grpcPort": 30000,
           "status": Up,
           "neCount": 0,
           "neIds": null,
           "active": False
           "groupIds": [1, 2],
      },
      {
```

```
            "name": mdm-server-1,
            "ipAddress": mdm-server-1.mdm-server-svc-headless.default.
svc.cluster.local,
            "grpcPort": 30000,
            "status": Up,
            "neCount": 2,
            "neIds": ["1.1.1.1", "1.1.1.2"],
            "active": True
            "groupId": 1,
      },
      {
            "name": mdm-server-2,
            "ipAddress": mdm-server-2.mdm-server-svc-headless.default.
svc.cluster.local,
            "grpcPort": 30000,
            "status": Up,
            "neCount": 2,
            "neIds": ["1.1.1.3", "1.1.1.4"],
            "active": True
            "groupId": 2,
      }
    ]
}
```

END OF STEPS

3.9 To rebalance NE load on MDM servers

Note: The NSP system must be operational before these operations can be performed.

3.9.1 Steps

From the NSP deployer host software directory, enter the following to rebalance the NE load on the MDM servers:

1

```
# tools/mdm/bin/server-load.bash --user username --pass
password--rebalance
```

where

username is the NSP username

password is the NSP password

END OF STEPS

3.10 To verify disk performance for etcd

3.10.1 Steps

1

As the root user, enter the following:

```
# mkdir /var/lib/test
# fio --rw=write --ioengine=sync --fdatasync=1 --directory=
/var/lib/test --size=22m --bs=3200 --name=mytest ↵
```

2

The command produces output like the following:

```
Starting 1 process
mytest: Laying out IO file (1 file / 22MiB)
Jobs: 1 (f=1)
mytest: (groupid=0, jobs=1): err= 0: pid=40944: Mon Jun 15 10:23:23
2020
  write: IOPS=7574, BW=16.6MiB/s (17.4MB/s)(21.0MiB/1324msec)
    clat (usec): min=4, max=261, avg= 9.50, stdev= 4.11
     lat (usec): min=4, max=262, avg= 9.67, stdev= 4.12
    clat percentiles (nsec):
     |  1.00th=[ 5536],  5.00th=[ 5728], 10.00th=[ 5920], 20.00th=[
6176],
     | 30.00th=[ 7584], 40.00th=[ 8896], 50.00th=[ 9408], 60.00th=[
9792],
     | 70.00th=[10432], 80.00th=[11584], 90.00th=[12864], 95.00th=
[14528],
     | 99.00th=[20352], 99.50th=[23168], 99.90th=[28800], 99.95th=
[42752],
     | 99.99th=[60672]
   bw (  KiB/s): min=16868, max=17258, per=100.00%, avg=17063.00,
stdev=275.77, samples=2
   iops        : min= 7510, max= 7684, avg=7597.00, stdev=123.04,
samples=2
  lat (usec)   : 10=64.21%, 20=34.68%, 50=1.08%, 100=0.02%, 500=0.01%
```

3

In the second block of output, which is shown below, the 99th percentile durations must be less than 10ms. In this block, each durations is less than 1ms.

```
fsync/fdatasync/sync_file_range:
    sync (usec): min=39, max=1174, avg=120.71, stdev=63.89
    sync percentiles (usec):
     |  1.00th=[   42],  5.00th=[   45], 10.00th=[   46], 20.00th=[
48],
     | 30.00th=[   52], 40.00th=[   71], 50.00th=[  153], 60.00th=[
159],
     | 70.00th=[  167], 80.00th=[  178], 90.00th=[  192], 95.00th=[
206],
     | 99.00th=[  229], 99.50th=[  239], 99.90th=[  355], 99.95th=[
416],
     | 99.99th=[  445]
  cpu          : usr=2.95%, sys=29.93%, ctx=15663, majf=0, minf=35
  IO depths    : 1=200.0%, 2=0.0%, 4=0.0%, 8=0.0%, 16=0.0%, 32=0.0%,
>=64=0.0%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
     issued rwts: total=0,10029,0,0 short=10029,0,0,0 dropped=0,0,0,0
     latency   : target=0, window=0, percentile=100.00%, depth=1
```

END OF STEPS

3.11 To verify disk performance for NSP

3.11.1 Steps

1

Enter the following as the root user in the /opt/nsp directory to create a file called 'test' in the directory:

```
# fio --randrepeat=1 --ioengine=libaio --direct=1 --gtod_reduce=1
--name=test --filename=random_read_write.fio --bs=4k --iodepth=64
--size=4G --readwrite=randrw --rwmixread=50 ↵
```

2

The command produces output like the following:

```
test: (g=0): rw=randrw, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T)
4096B-4096B, ioengine=libaio, iodepth=64
```

```
fio-3.7
Starting 1 process
test: Laying out IO file (1 file / 4096MiB)
Jobs: 1 (f=1): [m(1)][100.0%][r=22.1MiB/s,w=22.2MiB/s][r=5645,w=5674
IOPS][eta 00m:00s]
test: (groupid=0, jobs=1): err= 0: pid=32439: Mon Sep 21 10:25:11 2020
read: IOPS=6301, BW=24.6MiB/s (25.8MB/s)(2049MiB/83252msec)
   bw (  KiB/s): min=13824, max=39088, per=99.57%, avg=25098.60,
stdev=5316.27, samples=166
   iops        : min= 3456, max= 9772, avg=6274.49, stdev=1329.11,
samples=166
write: IOPS=6293, BW=24.6MiB/s (25.8MB/s)(2047MiB/83252msec)
   bw (  KiB/s): min=13464, max=40024, per=99.56%, avg=25062.73,
stdev=5334.65, samples=166
   iops        : min= 3366, max=10006, avg=6265.57, stdev=1333.67,
samples=166
  cpu          : usr=5.13%, sys=18.63%, ctx=202387, majf=0, minf=26
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%,
>=64=100.0%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.1%,
>=64=0.0%
     issued rwts: total=524625,523951,0,0 short=0,0,0,0 dropped=0,0,
0,0
     latency   : target=0, window=0, percentile=100.00%, depth=64
Run status group 0 (all jobs):
   READ: bw=24.6MiB/s (25.8MB/s), 24.6MiB/s-24.6MiB/s (25.8MB/s-25.
8MB/s), io=2049MiB (2149MB), run=83252-83252msec
  WRITE: bw=24.6MiB/s (25.8MB/s), 24.6MiB/s-24.6MiB/s (25.8MB/s-25.
8MB/s), io=2047MiB (2146MB), run=83252-83252msec
Disk stats (read/write):
  vda: ios=523989/526042, merge=0/2218, ticks=3346204/1622070,
in_queue=4658999, util=96.06%
```

END OF STEPS

3.12 Problem: NSP data synchronization is not 100%

3.12.1 Issue

If you run the procedure “How do I check NSP database synchronization?” in the *NSP System Administrator Guide* and do not get a 100% synchronized result, this indicates that a switchover occurred before the system had stabilized and nsp-tomcat on the standby site had caught up with the active site. The following workaround describes how to synchronize the data.

3.12.2 Steps

1

Perform a switchover to go back to the previous active site.

2

Wait for database instances to sync up.

3

Perform another switchover.

4

Run the procedure “How do I check NSP database synchronization?” again to verify the active and standby databases are 100% synchronized.

END OF STEPS

3.13 Problem: Alarms not appearing for rapidly reoccurring faults

3.13.1 Issue

Alarms are not generated under certain circumstances when the underlying fault is occurring and resolving faster than the duration of the NSP alarm flush interval. This only applies to alarms created by NSP alarm rules, and not to alarms received from other sources, for example using NETCONF. By default, the flush interval is four seconds, and the NSP may not capture events that occur and resolve faster than that, such as an ISIS interface that is flapping once every second.

You can configure the duration of the flush interval to capture rapidly flapping events. However, this impairs the performance of the NSP, as it increases how often the NSP writes to the alarm database. The following procedure describes how to configure the NSP alarm flush interval.

3.13.2 Steps

Note: Performing this procedure involves restarting a component of the NSP, and should not be performed outside of a maintenance window. In the event that resync-fw is upgraded, this procedure must be repeated to change the alarm flush interval again.

1

Log in as the root user on the NSP cluster host. For information about logging in to the NSP, see the *NSP System Administrator Guide*.

2

Open a console window.

3

In the **nspos-resync-fw** Kubernetes pod, open the following file in a text editor:

```
/opt/nsp/os/resync-fw/config/resync-fw-overrides.conf
```

4

The file contains parameter settings in nested declarations. The existing parameters depend on your current NSP configuration. Find or add the flush-buffer-interval-in-second parameter, which is nested under resync-fw > mdm > notification, as shown below:

```
resync-fw
{
  mdm
  {
    notification
    {
      flush-buffer-interval-in-second = 1
    }
  }
}
```

Configure the value of the parameter to the required duration of the NSP alarm flush interval, in seconds.

5

Save the configuration file, and enter the following to restart the **nspos-resync-fw** pod:

```
# kubectl delete pod --namespace pod_namespace pod_name ↵
```

where *pod_namespace* is the name of the pod's namespace and *pod_name* is the name of the pod

Note: Ensure the full name of the pod is entered for *pod_name*. To find the full name of a pod, see the procedure 3.2 “To retrieve a list of pods” (p. 30).

END OF STEPS

4 Troubleshooting the NFM-P platform

4.1 Overview

4.1.1 Purpose

This chapter provides information about troubleshooting the NFM-P platform, database, server, or clients.

4.1.2 Contents

Troubleshooting the NFM-P

4.2 To collect NFM-P log files

4.2.1 Purpose

Perform this procedure to collect the relevant log files for troubleshooting an NFM-P database, server, single-user client or client delegate server station.

Note: When an NFM-P log file reaches a predetermined size, the NFM-P closes, compresses, and renames the file to include a timestamp and sequence number in the following format:

`EmsServer.yyyy-mm-dd_hh-mm-ss.n.log`

During a system restart, NFM-P log files are backed up to directories that are named using a timestamp. A component that runs for a long time can generate multiple log files. Before you restart an NFM-P component, ensure that there is sufficient disk space to store the backup log files.

4.2.2 Steps

1

To collect the logs for a problem specifically related to installation, perform the following steps.

1. Navigate to the installation directory, which is one of the following:
   - NFM-P database—/opt/nsp/nfmp/db/install
   - main server—/opt/nsp/nfmp/server
   - auxiliary server—/opt/nsp/nfmp/auxserver
   - single-user client— typically /opt/nsp/client on RHEL, and C:\nsp\client on Windows
   - client delegate server—typically /opt/nsp/client on RHEL, and C:\nsp\client on Windows
2. Collect the following files:
   - NFM-P_*component*.install.*time*.stderr.txt
   - NFM-P_*component*.install.*time*.stdout.txt
   - NFM-P_*component*_InstallLog.log

   where

   component is the NFM-P component type, such as Main_Server or Main_Database

   time is the installation start time
3. Go to Step 7 .

2

If required, collect the NFM-P database logs.

1. Log on to the NFM-P database station as the Oracle management user.
2. Collect the following files:
   - /opt/nsp/nfmp/db/install/config/dbconfig.properties
   - all files in /opt/nsp/nfmp/db/install/admin/diag/rdbms/*instance*/*instance*/alert

- all files in /opt/nsp/nfmp/db/install/admin/diag/rdbms/*instance*/*instance*/trace
- all files in /opt/nsp/nfmp/db/install/admin/diag/proxy
- all files with a .log extension in the following directories:
  – /opt/nsp/nfmp/db/install
  – /opt/nsp/nfmp/db/install/config

  where *instance* is the database instance name, which is maindb1 in a standalone deployment, or maindb1 or maindb2 in a redundant deployment

3

If required, collect the main or auxiliary server logs; the log files have a .log extension and are in the following directories:

- main server—/opt/nsp/nfmp/server/nms/log
- auxiliary server—/opt/nsp/nfmp/auxserver/nms/log

4

If required, collect the RHEL single-user client or client delegate server log files:

- *install_dir*/nms/config/nms-client.xml
- all files and subdirectories in the *install_dir*/nms/log/client directory

where *install_dir* is the client software installation location, typically /opt/nsp/client

5

If required, collect the Windows single-user client or client delegate server log files:

- *install_dir*\nms\config\nms-client.xml
- all files and subdirectories in the *install_dir*\nms\log\client directory

where *install_dir* is the client software installation location, typically C:\nsp\client

6

If required, use a script to collect a comprehensive set of log files.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter one of the following:
   - On a main server station:
     # **/opt/nsp/nfmp/server/nms/bin/getDebugFiles.bash *output_dir days*** ↵
   - On an auxiliary server station:
     # **/opt/nsp/nfmp/auxserver/nms/bin/getDebugFiles.bash *output_dir days*** ↵
   - On an NFM-P database station:
     # **/opt/nsp/nfmp/db/install/getSAMDebugFiles.bash *output_dir days*** ↵

4. Collect the output files:

   Note:

   On a station that hosts a collocated NFM-P database and main server, all files are present. On a station in a distributed deployment, only two files are present.

   - *hostname_date*.WsInfoFiles.*checksum*.tar.gz
     Contains station-specific information such as the hardware and network configuration
   - *hostname_date*.ServerLogFiles.*checksum*.tar.gz
     Contains server and JBoss logs, and configuration information
   - *hostname_date*.DBLogFiles.*checksum*.tar.gz
     Contains NFM-P database logs and configuration information

7

Store the files in a secure location to ensure that the files are not overwritten. For example, if two NFM-P clients have problems, rename the files to identify each client and to prevent the overwrite of one file with another of the same name.

8

Send the files to technical support, as required.

END OF STEPS

4.3 Problem: Poor performance on a RHEL station

4.3.1 Checking CPU performance

When a RHEL station is taking too long to perform a task, you can check the CPU status to ensure that one process is not using most of the CPU resources, and then use commands to review the CPU usage.

Perform this procedure when CPU usage remains high and performance degrades.

You can also perform other procedures to monitor performance: If you are you performing a large listing operation using the NFM-P client GUI or OSS, check the LAN throughput using the netstat command, as described in 4.44 “Problem: Delayed server response to client activity” (p. 100).

4.3.2 Steps

1

Log on to the station as the root user.

2

Open a console window.

3

Perform the following steps to check for processes that are consuming excessive CPU cycles:

1. To list the top CPU processes using the UNIX utility prstat, type:

   # **top** ↵

   Depending on your system configuration, approximately the top 20 processes are displayed.

2. Review the output.

   The top NFM-P process in the CPU column should be the Java process. However, the Java process should not consume too much CPU time. Some Oracle processes may also consume CPU time, depending on the database load.

3. Press Ctrl-C to stop the command.

4

Perform the following steps to view a CPU activity summary.

1. Enter the following command:

   # **mpstat *time*** ↵

   where *time* is the interval, in seconds, between CPU polls; a value between 10 and 60 is recommended

2. Review the command output.

```
mpstat output example
CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %
guest   %idle
all    0.25    0.00    0.17    0.00    0.00    0.00    0.00    0.
00   99.58
all    0.50    0.00    0.08    0.08    0.00    0.00    0.00    0.
00   99.33
all    0.17    0.00    0.08    0.00    0.00    0.00    0.00    0.
00   99.75
all    0.25    0.00    0.17    0.08    0.00    0.00    0.00    0.
00   99.50
```

mpstat field descriptions

Field	Description (events per second unless noted)
CPU	Processor number; the keyword all indicates that statistics are calculated as averages among all processors
%usr	Percentage of CPU utilization at the user application level
%nice	Percentage of CPU utilization at the user level with nice priority
%sys	Percentage of CPU utilization at the system level; does not include time spent servicing hardware and software interrupts
%iowait	Percentage of CPU idle time during which the system had an outstanding disk I/O request

Field	Description (events per second unless noted)
%irq	Percentage of CPU time spent servicing hardware interrupts
%soft	Percentage of CPU time spent servicing software interrupts
%steal	Percentage of time spent in involuntary wait by the virtual CPU or CPUs during hypervisor servicing of another virtual processor
%guest	Percentage of CPU time spent running a virtual processor
%idle	Percentage of CPU idle time without an outstanding disk I/O request

Review the %usr, %sys and %idle statistics, which together indicate the level of CPU saturation. A Java application that fully uses the CPUs typically falls within 80 to 90 percent of the %usr value, and 20 to 10 percent of the %sys value. A smaller percentage for the %sys value indicates that more time is being spent running user code, which generally results in better execution of the application.

3. Press Ctrl-C to stop the command.

5

If processes are competing for CPU resources, perform the following steps to isolate the information about a single process.

1. Check the state of CPUs by typing:

   ps -aux ↵

   A list of processes is displayed.

2. Review the command output.

   For CPU troubleshooting, the important data is listed in the %CPU row. If a process is taking 90% or more of the CPU resources, there may be a problem with the process. Contact your account or technical support representative for more information.

3. Press Ctrl-C to stop the command.

6

Contact technical support and provide the data obtained in the previous procedure steps.

END OF STEPS

4.4 Problem: Device discovery fails because of exceeded ARP cache

4.4.1 ARP cache and /var/log/messages

When an NFM-P system manages a large number of NEs in a broadcast domain, the ARP cache on a main server station may fill and prevent the discovery of additional devices. When this happens, the /var/log/messages file contains entries like the following:

```
Jan 21 09:37:40 hostname kernel: Neighbour table overflow
```

```
Jan 21 09:37:40 hostname kernel: Neighbour table overflow

Jan 21 09:37:40 hostname kernel: Neighbour table overflow

Jan 21 09:38:00 hostname kernel: __ratelimit:190 callbacks suppressed
```

Perform this procedure when one of the following occurs:

- The /var/log/messages file contains more than 1024 entries like the example entries above.
- You need to increase the ARP cache size to accommodate the network.

The default ARP cache threshold values are the following:

- Threshold 1—128
- Threshold 2—512
- Threshold 3—1024

4.4.2 Steps

1

Log in to the main server station as the root user.

2

Open a console window.

3

Perform one of the following to increase the ARP cache thresholds.

a. To temporarily increase the thresholds, type the following:

```
# echo 8096 > /proc/sys/net/ipv4/neigh/default/gc_thresh1 ↵
# echo 25600 > /proc/sys/net/ipv4/neigh/default/gc_thresh2 ↵
# echo 32384 > /proc/sys/net/ipv4/neigh/default/gc_thresh3 ↵
```

b. To permanently override the default thresholds, perform the following steps.

1. Open the /etc/sysctl.conf file using a plain-text editor such as vi.
2. Add the following lines to the end of the file:

```
net.ipv4.neigh.default.gc_thresh1 = 8096
net.ipv4.neigh.default.gc_thresh2 = 25600
net.ipv4.neigh.default.gc_thresh3 = 32384
```

3. Save and close the file.
4. Enter the following:

```
# sysctl -p ↵
```

4

Close the console window.

END OF STEPS

Troubleshooting using the LogViewer

4.5 LogViewer overview

4.5.1 Managing log files

The LogViewer is a system monitoring and troubleshooting utility that parses, formats, and displays the contents of log files.

You can use LogViewer to perform the following:

- View and filter real-time log updates.
- View, filter, and sort the entries in a static log view.
- Open compressed or uncompressed log files.
- Compare active logs in real time.
- Automatically send a notification when a specified type of entry is logged.

LogViewer is available on NFM-P main or auxiliary server stations, and on single-user client and client delegate server stations as separate GUI and CLI utilities. The GUI has more functions than the CLI, which is designed for use on a character-based console over a low-bandwidth connection such as a Telnet session.

LogViewer can interpret various log formats. The log files must be local server or database logs.

4.5.2 Configuration

The LogViewer GUI and CLI utilities share a set of configuration options; an option change by one utility affects the other utility. Some options apply only to the GUI.

You can customize LogViewer by creating and saving log filters and log profiles that are available to all GUI and CLI users, and can save the GUI configuration, or workspace, to have LogViewer display the currently open logs the next time it starts. LogViewer does not save the current filter and display configuration for a log when you close the log unless you export the configuration to a log profile.

Your operating configuration of LogViewer is stored in the user directory. Any filters, fonts, colors, or other preferences you have set such as location, size and splitter location, are used the next time you start the utility.

For multiple instances of LogViewer running on the same server, you can set the system environment variable LOGV_HOME to make all instances use the same properties file. In this way, properties such as filters, window location, and window size are common to all instances.

4.5.3 Filters

You can use the LogViewer CLI or GUI to create multiple filters that define the log entries that are displayed in a log view. A filter uses Java regular expressions as match criteria to specify which entries to display and optionally uses colors to identify the filtered entries.

4.5.4 Plug-ins

LogViewer supports the use of plug-ins to provide additional functionality. You can specify a plug-in for use with a specific log, or assign a default plug-in configuration that applies to the subsequently opened logs.

LogViewer has default plug-ins that can send notifications, such as e-mail messages and GUI pop-ups, when a new log entry matches a set of filter criteria. The LogViewer e-mail plug-in uses SMTP as the transport.

4.6 LogViewer GUI and Quick Links panel

4.6.1 Accessing log entries

The LogViewer GUI opens to display a Quick Links panel that has shortcuts to the logs that are present on the local file system. When you click on a log shortcut, LogViewer opens a tab that displays the most recent log entries.

Note: If you hover your mouse cursor over a GUI tab, toolbar button, or field, a description or configuration instruction specific to that object appears.

4.6.2 LogViewer GUI and log tabs

Each log that you open using the LogViewer GUI is displayed on a separate tab whose label contains the name of the log profile and an icon that indicates the log type. The log entries are highlighted using the colors configured for the log debug levels. A log tab that displays dynamic log updates also has a tool bar for common operations.

The lower panel of a log tab contains the following sub-tabs:

- Preview—displays the unparsed log-file text for the currently selected log entries
- Filter—lists and permits management of the currently active filters for the log
- Status—displays status information about the current log
- Plugin—displays information about the plug-ins associated with the log
- Legend—displays a legend that correlates log file names to the numbers in the File column on a log tab that contains multiple open logs, for example, merged logs; is not shown for log comparisons

The LogViewer GUI allows you to drag and drop a log file into the GUI window. If you drop a file onto an open log tab, LogViewer provides options such as merging or comparing the log with another.

You can open a tab to list static log entries, such as the contents of an archived log or a snapshot of entries from an active log, and can pause the updates to active logs. The GUI also includes a text-search function.

GUI-based log filtering

The GUI provides a Filter Manager applet that lists the filters defined using the CLI or GUI and allows filter creation, modification, and deletion. A GUI operator can also use Filter Manager to test the regular expressions as filter match criteria.

To rapidly isolate a specific log entry or type of entry, you can create a temporary filter, or quick filter, by entering a regular expression in the field below a column header on a log tab. You can convert a quick filter to a saved filter for later use. A drop-down menu above the Level column allows the immediate filtering of log entries based on the debug level.

You can also create and use simple filters. These filters do not require the use of regular expressions, but instead, perform a case insensitive “contains” filtration of a string you specify. The use of simple filters must be enabled using the Preferences→Options menu option.

A color that is specified as the highlight color for a filter is saved with the filter and applies to all logs that use the filter.

4.7 LogViewer CLI

4.7.1 Accessing log entries using the CLI

The CLI-based LogViewer works like the UNIX tail command when in display mode. The command mode has a multiple-level menu that you can display at any time. You can specify a command or log file using the minimum number of unique characters in the name, and can quickly toggle between the command and display modes. LogViewer buffers new log entries while in command mode and displays them when it returns to display mode.

The LogViewer CLI assigns a different color to each logging level, for example, WARN or INFO, using standard ANSI color attributes that can be specified as CLI startup options or configured through the GUI. The CLI also supports the use of filters, plugins, and quick links.

4.8 To display logs using the LogViewer GUI

4.8.1 Purpose

Perform this procedure to start the LogViewer GUI utility and view one or more logs. Move the mouse cursor over a GUI object to view a description of the object, for example, a tool bar button.

4.8.2 Steps

1

Log in to a station as the nsp user.

2

Open a console window.

3

Enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/logviewerui.bash ↵
```

The LogViewer GUI opens with the Quick Links panel or the log tabs in the saved workspace displayed.

4

To open a log file, perform one of the following:

a. If the Quick Links panel is displayed, click on a link to view the associated log file.

b. Choose Quick Links→*log_name* from the LogViewer main menu.

c. To open a recently viewed log, choose File→Recent Logs→*log_file_name* from the LogViewer main menu.

d. To browse for a log file, perform the following steps:

1. Choose File→Local Log File from the LogViewer main menu or click Open log in the main tool bar. The Local Log File form opens.
2. Use the form to navigate to the log-file location.
3. Select a log file and click Add between the form panels. The log is listed in the panel on the right.

   Note:

   The log file can be in compressed or uncompressed format.
4. If LogViewer cannot determine the type of log that the file contains, for example, if a log file is renamed, it sets the Type to Other. Use the Type drop-down menu to specify the log type, if required.
5. Configure the Max. Messages parameter to specify the maximum number of entries that are listed on the log tab. LogViewer removes the oldest entries as required to keep the number of entries at or below this value.
6. Configure the Auto-Tail parameter to specify whether the log tab dynamically displays the log updates.
7. Click OK. The Local Log File form closes.

e. Drag and drop a log file into a section of the LogViewer main window that does not contain a log tab.

f. Drag and drop a log file onto a log tab in the LogViewer main window. The Add File form opens.

Perform the following steps:

1. Choose one of the following options:
   - New View—specifies that the log is displayed on a new log tab
   - Replace Existing File—specifies that the log tab displays the new log instead of the current log
   - Add to View—specifies that the entries in the new log and the entries in the current log are merged into one list on the same log tab
   - Add to Compare View—specifies that the new log is to be displayed on the same log tab as the current log in a separate panel for comparison
2. Click OK. The new log is displayed as specified.

A log tab opens to display the most recent entries in a log. If the log is active and the Auto-Tail parameter is enabled, the list scrolls upward to display new log entries as they are generated.

Note: The Auto-Tail parameter for a log is enabled by default.

Common display operations

5

To specify which columns are displayed on a log tab, right-click on a column header, and select or deselect the column names in the contextual menu, as required.

6

To reposition a column, drag the column title bar to the desired position, or right-click on the column header and choose Move Left or Move Right.

7

To view the raw log-file text of one or more entries, select the entries. The entry text is displayed on the Preview sub-tab.

8

To restrict the list of displayed entries to a specific debug level, choose a debug level from the drop-down menu under the Level column header.

9

To find log entries that contain a specific text string:

1. Choose Edit→Find from the LogViewer main menu. The Find form opens.
2. Specify a text string to search for using the text field and search options on the form.

   Note:

   The LogViewer Find function does not support the use of regular expressions. To perform a search using a regular expression, use the Find In Path function, as described in 4.10 “To search log files in a path” (p. 61).
3. Click Find, as required, to find the next list entry that contains the text string.
4. To find all list entries that contain the text string, click Find All. The Find form closes and a new log tab opens to display the result of the search.
5. Close the Find form if it is open.

   Note:

   After you close the Find form, you can use the F3 key or the Find next button on the main tool bar to perform repeated find operations for the same text string on the same log tab.

10

To remove one or more log entries from the current view, perform one of the following.

a. To clear all listed log entries, choose Log→Clear All Events from the LogViewer main menu, or click Clear all in the main tool bar.

b. To clear the currently selected log entries, choose Log→Clear Selected Events from the

LogViewer main menu, or click Clear Selected in the main tool bar.

c. To clear all log entries that match the currently selected cell, select a cell and choose Log→Hide All Like Selected from the LogViewer main menu, or click Hide All Like Selected in the main tool bar.

d. To show only log entries that match the currently selected cell, select a cell and choose Log→Show All Like Selected from the LogViewer main menu, or click Show All Like Selected in the main tool bar.

11

To apply a quick filter, enter a regular expression as a match criterion in the field below a column header and press ↵. The list is cleared, and only subsequent log entries that match the criterion are displayed; see 4.14 “To manage filters using the GUI Filter Manager” (p. 65) .

12

Repeat Step 11 to apply an additional quick filter, if required.

13

To apply a saved filter:

1. Choose Log→Add Filter from the LogViewer main menu, or click Add filter in the main tool bar. The Select Filters form opens.
2. Select one or more filters in the list and click OK. The filters are applied to the log view and are listed on the Filters sub-tab of the log tab.

   See 4.14 “To manage filters using the GUI Filter Manager” (p. 65) for information about creating saved filters.

14

To remove a filter from the log, select the filter in the Filter sub-tab and choose Log→Remove Selected Filters, or click Remove filter in the main tool bar.

15

If the log display is static, such as for an archived log or the result of a Find All operation, go to Step 22.

Dynamic view operations

16

To edit the log display properties, choose Edit→Edit Log from the LogViewer main menu, or click Edit log in the log tab tool bar, and perform the following steps.

1. Configure the Max. Messages parameter to specify the maximum number of entries that are listed on the log tab. LogViewer removes the oldest entries as required to keep the number of entries at or below this value.

2. Configure the Auto-Tail parameter to specify whether the log tab dynamically displays the log updates.
3. Click OK to close the Local Log File form.

17

To pause the display of log-file updates, choose Log→Pause from the LogViewer main menu, or click Pause log updates in the log tab tool bar.

18

To resume the display of log-file updates, choose Log→Initialize Connection from the LogViewer main menu, or click Initialize log updates in the log tab tool bar.

19

By default, a dynamic log view focuses on a new log entry. To focus the display on an earlier log entry and prevent the display from automatically focusing on a new log update, click Follow latest updates in the log tab tool bar. Click on the button again to enable the default behavior.

20

To compare logs in real time:

1. Choose Log→Specify Compare from the LogViewer main menu, or click Add log to compare on the log tab tool bar. The Compare Files form opens.
2. Use the form to navigate to the log-file location.
3. Select a log file and click Add between the form panels. The log is listed in the panel on the right.

   Note:

   The log file can be in compressed or uncompressed format.
4. If LogViewer cannot determine the type of log that the file contains, for example, if a log file is renamed, it sets the Type to Other. Use the Type drop-down menu to specify the log type, if required.
5. Click OK. The Compare Files form closes, and a second panel opens on the log tab to display the specified log.

   The log entry lines are synchronized by timestamp. Dynamic log updates to each log are displayed as they occur. Blank entry lines serve as spacers to preserve the chronological order of the combined log entries.
6. By default, the scroll bars in the two panels are synchronized; when you scroll in the right panel, the display in the left panel scrolls by the same amount. Click Synchronize scroll bars between views in the log tab tool bar to disable or re-enable this behavior, as required.
7. To remove the added log from the comparison, choose Log→Clear Compare from the LogViewer main menu, or click Clear compared logs on the log tab tool bar. The right panel is removed from the log tab form.

21

To capture one or more log entries for display in a static view on a separate tab:

a. To capture all listed log entries, choose Log→Full Snapshot from the LogViewer main menu, or click Snap all in the main tool bar.

b. To capture the currently selected log entries, choose Log→Snapshot from the LogViewer main menu, or click Snap selected in the main tool bar.

   A new tab opens to display the captured log entries in a static view.

Static view operations

22

To sort a list of log entries in a static view, right-click on a column header and choose Sort Ascending, Sort Descending, or No Sort. The log entries are sorted accordingly.

Note: You cannot sort the log entries in a dynamic view, but you can sort the entries in a snapshot of a dynamic log view.

23

To copy the text of selected log entries to the clipboard, select one or more log entries in a log tab and choose Edit→Copy from the LogViewer main menu, or click Copy in the main tool bar.

24

To save selected log entries to a file, select one or more log entries in a log tab and click Save Selected in the main tool bar.

25

To save the current workspace for subsequent sessions, choose File→Save Workspace from the LogViewer main menu, or click Save configuration in the main tool bar.

26

Choose File→Exit from the LogViewer main menu to close the LogViewer GUI.

END OF STEPS

4.9 To configure the LogViewer using the GUI

4.9.1 Purpose

Perform this procedure to use the LogViewer GUI to configure general options for the LogViewer GUI and CLI.

4.9.2 Steps

1

Open the LogViewer GUI.

2

Choose Edit→Options→General from the LogViewer main menu, or click Application options in the main tool bar. The Options form opens.

3

Configure the required parameters:

- Last Directory—Click in the parameter field and use the browser form that opens to specify where to save exported log profiles.
- Base File Messages Directory—Click in the parameter field and use the browser form that opens to specify the base log directory.
- Default Character Set—Edit this parameter to specify the character set that LogViewer uses to display the log-file contents.
- Default Log Pattern—Edit this parameter to specify a regular expression that LogViewer uses to interpret log-file contents.
- Default Date Format—Enter a colon-separated string to specify the LogViewer date format using y for year digits, M for month digits, d for date digits, H for hour digits, m for minute digits, s for second digits, and S for millisecond digits, for example, yyyy:MM:dd HH:mm:ss:SSS.
- Regular Expression Help URL—Enter a value to specify the location of the Java regular-expression help web page that opens when you click Help while testing a regular expression for a filter.
- Web Browser Location—Enter a value to specify the location of the local file browser used to open the Java regular-expression help web page.
- Quick Links Refresh Time (ms)—Enter a value to specify how often LogViewer refreshes the Quick Links list.
- Rollover Remove Size—Enter a value to specify the number of log entries to remove from the LogViewer display when the maximum number of displayed log entries is reached.
- Delay for local file polling (ms)—Enter a value to specify, in ms, how long LogViewer waits before it checks local log files for updates.
- Hide Table Tooltips—Select this parameter to suppress the display of tool tips when the mouse pointer moves over log entries in a log tab.
- Use Simple Filters—Select this parameter to allow the use of simple filters.
- Advanced Quick Filter—Select this parameter to display the advanced Quick Filter table header on log tabs.
- Display Advanced Quick Filter—Select this parameter to display the advanced Quick Filter table header on the log tab when a log file is opened.
- Include Host in Title—Select this parameter to display the hostname in the log title.

- Show Memory Monitor—Select this parameter to display the memory monitor at the bottom right corner of the LogViewer window.
- Memory Monitor Clear Messages—Select this parameter to allow the memory monitor to attempt recovery by clearing some messages from live event logs when the memory threshold is exceeded.
- Clear Log on Rollover—Select this parameter to clear the events from the logs when a Style View file rolls over or is moved.
- Style View—Select this parameter to display the styled preview pane.
- Memory Monitor Threshold (%)—Enter a value to specify the percentage of available memory that LogViewer uses before it stops displaying log updates.
- Max. Recent Files—Enter a value to specify the number of files that LogViewer keeps in the list of recently opened files.
- Max. Profile Files—Enter a value to specify the number of profile files that LogViewer keeps in the list of recently opened files.
- LogViewer Log Level—Choose a logging level from the drop-down menu to specify the minimum log level of the LogViewer-specific log messages.
- Enable Viewer Performance Stats—Select this parameter to enable the display of LogViewer performance statistics.
- Stats Timer (seconds)—Enter a value to specify the number of seconds that LogViewer waits between log statistics updates.

4

Click on the Command Line tab to configure the LogViewer CLI.

5

Configure the following parameter:

- Command line buffer size—Enter a value to specify the number of log messages that LogViewer buffers when the CLI is in command mode.

6

Choose an ANSI display attribute from the drop-down menu beside each of the following parameters to specify how the CLI displays the corresponding text.

- Normal Display—for normal text
- Trace Level Display—for trace-level log entries
- Debug Level Display—for debug-level log entries
- Info Level Display—for info-level log entries
- Warning Level Display—for warning-level log entries
- Error Level Display—for error-level log entries
- Fatal Level Display—for fatal-level log entries
- Filter Display—for filtered log entries

7

Configure the Always Use ANSI Display parameter, as required.

8

Click on the NFM-P tab to configure the required parameters that are specific to the NFM-P.

9

Configure the required parameters by clicking in the parameter field and using the browser form that opens to specify a directory:

- Database Location—specifies the base NFM-P database installation directory
- Oracle Location—specifies the base NFM-P Oracle installation directory
- NMS Root—specifies the nms directory under the base NFM-P server installation directory

  Note:

  Your configuration of LogViewer is stored in the user directory. Any filters, fonts, colors, or other preferences you have set are preserved when you install a newer version.

10

CAUTION

Service Disruption

The parameters on the Advanced tab typically require configuration only when LogViewer has performance problems.

Consult technical support before you attempt to modify a parameter on the Advanced tab, as it may affect server performance.

Click on the Advanced tab to configure the required parameters related to LogViewer performance.

END OF STEPS

4.10 To search log files in a path

4.10.1 Purpose

Use this procedure to perform a search on all log files in a specified path using a plain text search or a regular expression.

Note: You can test regular expressions in the Find In Path window by clicking Test beside the expression. Enter sample text in the Example box, and an expression in the Expression box, then click on the green Execute button to test the results of the expression.

4.10.2 Steps

1

Open the LogViewer GUI.

2

Choose Edit→Find In Path from the LogViewer main menu, or click Search all files. The Find In Path window opens.

3

Perform one of the following:

a. To perform a text search, specify the text string to search for in the Text to find parameter and deselect the Regular expression option.

b. To perform a search using a regular expression, enter a regular expression in the Text to find parameter and select the Regular expression option.

4

In the Directory parameter, enter the directory path you need to search, or click Browse and select a directory. To search subdirectories, select the Recursive option.

5

To restrict the search to logs with certain filenames, enter a regular expression in the File Mask parameter. To search all logs in the specified path, leave this parameter blank.

6

Click Find. The log entries matching the search parameters are displayed in a new tab.

Note: A new search using the Find In Path function cannot be performed until the search tab is closed.

END OF STEPS

4.11 To show or hide buttons from the LogViewer main tool bar

4.11.1 Purpose

Perform this procedure to show or hide specific buttons from the LogViewer main tool bar.

4.11.2 Steps

1

Open the LogViewer GUI.

2

Choose Edit→Preferences→Manage Toolbar from the LogViewer main menu. The Manage Toolbar page opens divided into a Palette and Toolbar section.

3

Use the directional arrows to manage which buttons appear in the main tool bar, and the order in which the buttons appear.

4

Click OK to save your settings.

END OF STEPS

4.12 To set highlight colors and fonts for LogViewer components and levels

4.12.1 Purpose

Perform this procedure to set highlight colors and fonts for the various LogViewer components and levels.

4.12.2 Steps

1

Open the LogViewer GUI.

2

Choose Edit→Preferences→Highlight Colors from the LogViewer main menu. The Highlight Color Selection form opens.

3

Set the item for which you want to specify colors and/or fonts by choosing it from the Component/Level drop-down menu.

4

For the item that you want to change, choose the foreground or background plane as required, by clicking on the appropriate tab. The foreground is the text contained in a field. The background is the fill color of the field behind the text.

5

For foreground text items, set the font type, style, and size, as required.

6

For either foreground or background items, set the color as required. You can choose a color from the samples shown on the Swatch tab, or you can specify a color by entering its red, green, and blue values in the RGB tab.

Previews of your choices appear in the sample fields at the bottom of the form.

7

Click OK to save your settings.

END OF STEPS

4.13 To automatically show or hide log messages

4.13.1 Purpose

Perform this procedure to automatically filter (show or hide) log messages based on the current selected cell in the message table.

4.13.2 Steps

1

Open the LogViewer GUI.

2

To automatically show or hide log messages:

1. Select a log entry.
2. To hide log messages based on a selected cell in the message table, perform one of the following:
   - Right-click on the cell and choose Hide All Like Selected.
   - Choose Log→Hide All Like Selected from the LogViewer main menu.
   - Click the Hide All Like Selected button in the main tool bar.

   LogViewer hides all messages that contain the selected cell. For example, if you have selected the cell in the “Logger” column that contains the word “samConsole”, all messages that have the logger set to “samConsole” are hidden.
3. Perform one of the following to show log messages based on a selected cell in the message table.
   - Right-click on the cell and choose Show All Like Selected.
   - Choose Log→Show All Like Selected from the LogViewer main menu.
   - Click the Show All Like Selected button in the main tool bar.

   This shows all messages that contain the selected cell. For example, if you have selected the cell in the “Logger” column containing the word “samConsole”, all messages that have the logger set to “samConsole” are displayed.

END OF STEPS

4.14 To manage filters using the GUI Filter Manager

4.14.1 Purpose

Perform this procedure to create, modify, assign or delete a LogViewer filter.

Note: The Filter Manager is opened from within LogViewer, but runs as a separate applet. This enables the dragging and dropping of filters between Filter Manager and the Filters sub-tab of a lob tab.

4.14.2 Steps

1

Choose Log→Filter Manager from the LogViewer main menu. The Filter Manager applet opens.

2

To add a regular filter or a simple filter:

1. Click Add or Add Simple, as required. The Add Filter form opens.
2. Configure the Name parameter by specifying a unique name for the filter.
3. Configure the required parameters that correspond to the fields in a log entry by entering regular expressions for regular filters, or just strings for simple filters as a filter criterion for each:
   - Level
   - Message
   - Thread
   - Logger
   - Timestamp
   - Platform
4. If you are configuring a simple filter, go to Step 2 11 .
5. Test a regular expression that you enter by clicking Test beside the regular expression. The Regular Expression form opens.
6. Paste an example log entry that you want to match using the regular expression into the Example field.
7. Click on the green right-pointing arrow to test the expression. If the expression is invalid, a message is displayed to indicate the error in the expression.
8. Correct the errors in the expression.
9. Repeat Step 2 7 and Step 2 8 until no error message is displayed.
10. Repeat Step 2 5 to Step 2 9 to test additional regular expressions, if required.
11. Enable the Color parameter and click in the field beside the parameter to specify a highlight color for the matching log entries. A standard color chooser form opens.
12. Use the form to specify a color and click OK. The color chooser form closes and the Add Filter form reappears.

13. Click OK. The Add Filter form closes and the Filter Manager form lists the new filter.

3

To create a saved filter based on the current quick filter, perform the following steps:

1. Choose Log→Create from Quick Filter from the LogViewer main menu, or click Create from quick in the main tool bar. The Add Filter form opens and is populated with the quick filter match criteria.
2. Modify the match criteria as required.
3. Click OK to save the filter.

4

To create a saved filter using a log entry as a template:

1. Select a log entry.
2. Choose Log→Create from Selected from the LogViewer main menu, or click Create from entry in the main tool bar. The Add Filter form opens and is populated with the current log-entry field values as match criteria.
3. Modify the match criteria as required.
4. Click OK to save the filter.

5

To move a filter to other instances of the LogViewer:

1. To export a filter, click Export in the main tool bar, or choose Log→Filter Manager from the LogViewer main menu. The Export form opens, and allows you to export a filter to a specified file.
2. To import a filter, click Import in the main tool bar, or choose Log→Filter Manager from the LogViewer main menu. The Import form opens, and allows you to import a filter from a specified file.
3. Click OK to save the filter.

6

To make a copy of a filter, select the filter and click Copy. A copy of the filter is listed on the Filter Manager form.

7

To edit a filter, select the filter and click Edit. Configure the required parameters described in Step 2.

8

To delete a filter, select the filter and click Delete.

END OF STEPS

4.15 To specify a plug-in using the LogViewer GUI

4.15.1 Purpose

Perform this procedure to configure and enable plug-ins for a log file.

4.15.2 Steps

1

Choose File→Local Log File from the LogViewer main menu, or click Open log in the log tab tool bar. The Local Log File form opens.

2

Use the form to navigate to the log-file location.

3

Select a log file and click on the Add object... icon button between the form panels. The log is listed in the panel on the right.

Note: The log file can be in compressed or uncompressed format.

4

Click on the Plugins tab.

5

Choose a plug-in from the Plugin drop-down menu.

6

If you choose the Bring to Front plug-in, perform the following steps:

1. Specify a regular expression as a match criterion in the Message Filter field.
2. Go to Step 8 .

7

If you choose the E-Mail plug-in, perform the following steps:

1. Specify a regular expression as a match criterion in the Message Filter field.
2. Configure the required parameters:
   - Message Filter—specifies a regular expression that is used as a filter to identify the log entries that invoke the plug-in
   - Subject—specifies the e-mail message subject line
   - Body Prefix—specifies the text that precedes the log-entry text in an e-mail message
   - Authenticate? —specifies whether or not authentication is enabled
   - User—specifies a user name associated with the plug-in

- Password—specifies an SMTP password
- Host—specifies the name of an SMTP server
- Use TLS? —specifies whether the mail server uses Transport Layer Security (TLS) encryption
- Use SSL? —specifies whether the mail server uses Secure Sockets Layer (SSL) encryption
- To—specifies the e-mail address of the recipient
- From—specifies the sender e-mail address used by the plug-in
- Minimum E-mail Time (minutes)—specifies the minimum time between messages that the plug-in sends, to prevent e-mail flooding

8

Click OK. The Local Log File form closes.

END OF STEPS

4.16 To display logs using the LogViewer CLI

4.16.1 Purpose

Perform this procedure to start the LogViewer CLI and view one or more logs.

4.16.2 Steps

1

Log in to a station as the nsp user.

2

Open a console window.

3

Enter the following:

`bash$ /opt/nsp/nfmp/server/nms/bin/logviewer.bash argument options parameter` ↵

where

argument is an argument listed in Table 4-1, “LogViewer CLI startup arguments” (p. 68)

options is one or more of the options listed in Table 4-2, “LogViewer CLI startup options” (p. 69)

parameter is a parameter listed in Table 4-3, “LogViewer CLI startup parameters” (p. 69)

Table 4-1 LogViewer CLI startup arguments

Argument	Meaning
--version	Display LogViewer version information.

Table 4-1 LogViewer CLI startup arguments (continued)

Argument	Meaning
--help	Display LogViewer CLI help text.

Table 4-2 LogViewer CLI startup options

Option	Meaning
-counter	Prepend a counter number to each displayed log entry.
-parseAll	Parses and display the entire contents of a file before displaying the real-time updates.
-ansi *level attribute*	Display events and filters using ANSI-specified colors where *level* is a logging level, such as debug *attribute* is an ANSI color attribute, such as 42m to specify the color green
-quit	Quit LogViewer after parsing the log files.

Table 4-3 LogViewer CLI startup parameters

Parameter	Meaning
-xml *file_name*	Read information such as log file, plug-in and filter specifications from the XML file specified by *file_name*. The LogViewer GUI can export this information to an XML file.
file name	Display the specified file when LogViewer starts.

The LogViewer CLI opens in display mode. If a log file is specified as a startup parameter, the most recent entries in the log file are displayed as they are written to the log file. Otherwise, a cursor is displayed.

4

Enter command mode by pressing ↵. The following prompt is displayed:

```
log>
```

This prompt is called the root prompt. The table below describes the options that are available at the root prompt.

Table 4-4 LogViewer CLI root menu options

Option	Function
open	opens a submenu for choosing the logs to view
include	opens a submenu for specifying which log files to list in the *open* submenu
filter	opens a submenu for adding, listing or deleting filters
plugin	opens a submenu for adding, listing or delete plugins

Table 4-4 LogViewer CLI root menu options (continued)

Option	Function
options	opens a submenu for configuring LogViewer CLI and GUI options
list	lists the files in the *open* submenu file list
reset	resets the log message counts
stats	displays LogViewer statistics for the current log
The following options are also available in submenus:	
back	goes to the previous menu
root	goes to the root menu
quit	quits LogViewer
return	returns to display mode

5

Enter the following:

open ↵

The following prompt is displayed:

```
log-open>
```

6

Press ↵ to display the list of available logs.

7

Perform one of the following:

a. To view a log in the list, enter the name of a log and press ↵.

b. To view a log that is not listed, perform the following steps.

1. Enter the following:

   other ↵

   The following prompt is displayed:

   ```
   File Name (full path)?
   ```

2. Enter the absolute or relative path of the log file that you want to open and press ↵. LogViewer opens the file.

8

Enter the following to enter display mode and view the real-time log updates:

return ↵

LogViewer enters display mode. Log updates are displayed as they occur.

9

To add a filter that restricts the types of log entries that are displayed during the current LogViewer session, perform the following steps:

1. Press ↵ to enter command mode.
2. Enter the following to return to the root menu:

   root ↵

   The following prompt is displayed:

   `log>`
3. Enter the following:

   filter ↵

   The following prompt is displayed:

   `log-filter>`

   Note:

   You can also use commands at this menu level to list and delete filters.
4. Enter the following:

   add ↵

   The following prompt is displayed:

   `Filter name:`
5. Enter a name for the filter and press ↵.
6. The following prompts are displayed in sequence:

   `Level:`

   `Logger:`

   `Thread:`

   `Timestamp:`

   `Message:`

   At each prompt, enter a regular expression to use as a match criterion, if required, and press ↵.
7. The following prompt is displayed:

   `Display Filter? (Y/N):`

   Enter y ↵ to apply the filter to the current log display. LogViewer applies the filter.
8. Enter the following to return to display mode:

   return ↵

   LogViewer enters display mode. The log updates are filtered before they are displayed.

10

To list the available log files, perform the following steps:

1. Press ↵ to enter command mode.

2. Enter the following:

   list ↵

   LogViewer lists the available log files.

3. Enter the following to return to display mode:

   return ↵

11

To display statistics about the current LogViewer session, perform the following steps:

1. Press ↵ to enter command mode.
2. Enter the following:

   stats ↵

   LogViewer displays statistics about the current session.

3. Enter the following to return to display mode:

   return ↵

12

To reset the statistics counters for the current LogViewer session, perform the following steps:

1. Press ↵ to enter command mode.
2. Enter the following:

   reset ↵

   LogViewer resets the counters.

3. Enter the following to return to display mode:

   return ↵

13

Enter the following to close LogViewer:

quit ↵

END OF STEPS

4.17 To configure the LogViewer CLI

4.17.1 Purpose

Perform this procedure to use the LogViewer CLI to configure general CLI options.

Note: The options configured in this procedure apply only to the current LogViewer CLI session.

4.17.2 Steps

1

Open the LogViewer CLI.

2

To add a file to the list of files in the *open* menu, perform the following steps:

1. Press ↵ to enter command mode.
2. Enter the following at the root prompt:

   include ↵

   The following prompt is displayed:

   ```
   log-include>
   ```
3. Enter the following:

   add ↵

   The following prompt is displayed:

   ```
   File Name (full path)?
   ```
4. Enter the absolute or relative path of the log file that you want to add and press ↵. LogViewer adds the file to the list in the *open* menu.

   Note:

   The LogViewer CLI supports file drag-and-drop functionality.
5. Enter the following to return to the root prompt:

   root ↵

3

To configure LogViewer file parsing, perform the following steps:

1. Press ↵ to enter command mode.
2. Enter the following at the root prompt:

   options ↵

   The following prompt is displayed:

   ```
   log-options>
   ```
3. Enter y ↵ to confirm the action.
4. To specify whether LogViewer parses the entire log file, enter the following:

   parseAll ↵

   A confirmation prompt is displayed.
5. To force LogViewer to reparse the current log file, enter the following:

   reparse ↵
6. If you are prompted to enable parsing of the entire log file, enter y ↵.

7. Enter the following to return to the root prompt:

   root ↵

END OF STEPS

4.18 To specify plug-ins using the CLI

4.18.1 Purpose

Perform this procedure to specify a plug-in for the current LogViewer CLI session.

4.18.2 Steps

1

Open the LogViewer CLI.

2

Press ↵ to enter command mode.

3

Enter the following at the root prompt:

plugin ↵

The following prompt is displayed:

```
log-plugin>
```

4

Enter the following:

add ↵

LogViewer displays a list of the available plug-ins and the following prompt:

```
Which plugin would you like to specify? (name)
```

5

Enter the name of a plug-in from the list and press ↵.

6

You may be prompted for plug-in configuration information. Supply the information, as required.

Note: The currently available plug-ins and the associated configuration options are described in 4.15 “To specify a plug-in using the LogViewer GUI” (p. 67).

END OF STEPS

Troubleshooting the NFM-P database

4.19 Database troubleshooting overview

4.19.1 Database status

The NFM-P monitors the primary and standby database status and displays a colored status based on the primary and standby database connection and availability states. The following describes the conditions that determine database status color. These conditions also cause the NFM-P to raise database alarms.

Clear

The database status panel changes to clear status (gray) when the database connection, proxy, and applicable standby entities are up and all database error conditions are cleared.

Yellow

The following conditions cause the panel to change to yellow status:

- A database switchover or failover is complete.
- The database connection is partially down.
- The primary database is up and the standby database is down.
- A problem is detected with synchronization or archiving.

Red

The following conditions cause the panel to change to red status:

- A database switchover or failover is starting.
- The database connection is down.
- The primary database is down.

4.20 Problem: NFM-P database corruption or failure

4.20.1 Solution

You can restore an NFM-P database using a backup copy.

Note: Before you perform a database restore operation, you must shut down the databases and main servers in the NFM-P system. Contact technical support before you attempt to perform a database restore.

In a redundant NFM-P system, you must perform one or both of the following to regain database function and redundancy:

- Restore the primary NFM-P database.
- Reinstantiate the standby NFM-P database.

Both operations are required after a primary database failure. After a standby database failure, no restore operation is required, but you must reinstantiate the standby database to restore redundancy. You can use the NFM-P client GUI or a CLI script to reinstantiate a database.

Note: In a redundant NFM-P system, you can restore a database backup only on a primary database station. To restore a database backup on a station other than the primary station, you must do the following on the station before you attempt the restore:

- Uninstall the NFM-P database, if it is installed.
- Install a primary NFM-P database on the station.

Note: In a redundant NFM-P system, you can reinstantiate a database only on a standby database station. To reinstantiate a database on a station other than the standby station, you must do the following on the station before you attempt the reinstantiation:

- Uninstall the NFM-P database, if it is installed.
- Install a standby NFM-P database on the station.

See the *NSP System Administrator Guide* for information about restoring or reinstantiating an NFM-P main database.

4.21 Problem: The database is running out of disk space

4.21.1 Database disk space

Sufficient database disk space is essential for efficient NFM-P database operation. You can also check whether your database backup schedule is adequate. Underscheduling backups while the database is in ARCHIVELOG mode creates numerous log files.

4.21.2 Steps

1

Verify that the database platform is adequately sized. See the *NSP Planning Guide* or consult technical support.

2

Verify that the thresholds for disk space and archive logs are sufficient for your network, and determine how the disk space is being used. Contact your technical support representative for more information.

3

Check the root database backup directory or partition to ensure that:

- the size of the assigned disk space or slice is sufficient
- the disk directory or slice is sufficient to hold the configured number of database backups

4

If the disk directory has many archived log files due to underscheduling of database backups, contact your technical-support representative for information about deleting archived log files.

5

Back up the NFM-P database, as described in the *NSP System Administrator Guide*.

END OF STEPS

4.22 Problem: Frequent database backups create performance issues

4.22.1 Overscheduling database backups

Overscheduling the number of database backups can affect database performance by consuming excessive system resources.

4.22.2 Steps

1

Choose Administration→Database from the NFM-P main menu. The Database Manager form appears.

2

Click on the Backup tab.

3

Check the Backup Interval and Interval Unit parameters. For example, setting the Backup Interval parameter to 6 and setting the Interval Unit parameter to hour means a backup is performed every 6 hours, or four times a day. Such frequent backups can cause performance issues.

Note: Nokia recommends scheduling database backups to occur once daily.

4

Modify other parameters as required to improve performance.

5

Save your changes and close the Database Manager form.

END OF STEPS

4.23 Problem: An NFM-P database restore fails and generates a No backup sets error

4.23.1 Solution

WARNING

Equipment Damage

Performing NFM-P database modifications using Oracle database tools can cause irreparable harm to the NFM-P database and the network management data, and can void your warranty or support agreement.

Contact your technical support representative for assistance with database troubleshooting.

Database backup sets expire based on a retention period. After the retention period passes, the database backup sets are set to expired. You cannot restore databases from expired backup sets. Contact your technical support representative for assistance with an NFM-P database restore failure.

4.24 Problem: NFM-P database redundancy failure

4.24.1 Steps

WARNING

Equipment Damage

Performing NFM-P database modifications using Oracle database tools can cause irreparable harm to the NFM-P database and the network management data, and can void your warranty or support agreement.

Contact your technical support representative for assistance with database troubleshooting.

1

Ensure that the database redundancy configuration is correct, as specified in the *NSP Installation and Upgrade Guide*:

- The primary and standby database directory structures and disk partition configurations are identical.
- The same OS version and patch level, and the same NFM-P software release and patch level, are installed on the primary and standby database stations.

2

Ensure that there are no network communication problems between the primary and standby database stations; see Chapter 3, “Troubleshooting the NSP platform”.

END OF STEPS

4.25 Problem: Primary or standby NFM-P database is down

4.25.1 Primary or standby database is down

The status bar of the NFM-P client GUI indicates that the primary or standby database is down.

4.25.2 Steps

WARNING

Equipment Damage

Performing NFM-P database modifications using Oracle database tools can cause irreparable harm to the NFM-P database and the network management data, and can void your warranty or support agreement.

Contact your technical support representative for assistance with database troubleshooting.

1

Verify the correct IP address and instance name of the database. From the NFM-P main menu, select Administration→Database to open the Database Manager. Verify the information in the Instance Name and DB Server fields.

2

Verify the network connectivity between the NFM-P primary server and the primary or standby database by ensuring that the primary server and the primary or standby database can ping each other; see Chapter 3, “Troubleshooting the NSP platform”.

END OF STEPS

4.26 Problem: Need to verify that Oracle database and listener services are started

4.26.1 Purpose

Perform the following procedure to determine the status of the Oracle database and listener services, each of which starts automatically during NFM-P database station initialization.

4.26.2 Steps

1

Open an NFM-P GUI client.

2

View the status bar at the bottom of the GUI. The background of the NFM-P database section of the status bar is yellow or red when there is a problem with a service. The status bar text indicates the database service status.

END OF STEPS

4.27 Problem: Need to determine status or version of NFM-P database or Oracle proxy

4.27.1 Purpose

Perform the following procedure to determine the status of the NFM-P database or Oracle proxy, each of which starts automatically during NFM-P database station initialization.

4.27.2 Steps

1

Log in as the Oracle management user on the database station.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/db/install/config/db directory

4

Enter the following command.

```
bash$ ./oracleproxy.sh option ↲
```

where *option* is one of the options in the table below.

Table 4-5 oracleproxy.* flag options

Flag option	Description
start	Starts the Oracle proxy
no option, or help	Lists the available options
proxy_version	Displays Oracle proxy version information
proxy_status	Displays Oracle proxy status information
db_version	Displays NFM-P database version information
db_status	Displays NFM-P database status information

5

Review the command output.

The following sample shows the output of the proxy_status option.

```
Proxy is UP
```

The following sample shows the output of the db_version option.

```
NSP Version Release - Built on Wed Mar 27 03:14:15 EST 20XX
```

6

Close the console window.

END OF STEPS

Troubleshooting NFM-P server issues

4.28 NFM-P server troubleshooting overview

4.28.1 Problems associated with the NFM-P server

NFM-P server statistics collection is a useful troubleshooting tool for memory, alarm, and SNMP issues on an NFM-P main or auxiliary server. See the *NSP NFM-P Statistics Management Guide* for more information.

When no NE is associated with an NFM-P alarm, the alarm Site ID and Site Name properties are populated with the IP address and hostname, respectively, of the NFM-P main or auxiliary server that raised the alarm.

4.29 Problem: Cannot start an NFM-P server, or unsure of NFM-P server status

4.29.1 Server status indicators

The NFM-P main or auxiliary server startup script provides server status indicators that include the following:

- how long the server has been running
- the used and available memory
- the NFM-P database connectivity status
- NFM-P license capacity

4.29.2 Steps

1

Log in to the NFM-P server as the nsp user.

2

Open a console window.

3

To check the status of an NFM-P main server, perform the following steps.

1. Enter the following:
   `/opt/nsp/nfmp/server/nms/bin/nmsserver.bash appserver_status` ↵
   The general server status is displayed.
2. Enter the following at the CLI prompt:
   `/opt/nsp/nfmp/server/nms/bin/nmsserver.bash nms_status` ↵
   Detailed NFM-P server information is displayed.

3. To obtain more specific server status information, run the nmsserver script in step 3 using the appropriate option from the following table in place of the nms_status or appserver_ status option.

NFM-P main-server startup script options

Option	Description
start	Starts the NFM-P main server in a non-interactive mode
stop	Stops the NFM-P main server
debug	Starts the NFM-P server in an interactive mode. **Note:** The server shuts down if the console is closed or if Ctrl-C is pressed.
appserver_status	Returns information about the status of the NFM-P main server (both active and standby servers when the NFM-P is configured for redundancy)
appserver_version	Returns NFM-P software release information that includes the start time of the current NFM-P main server instance
nms_status	Returns the following information: • NFM-P standalone, primary, or standby server start time and running time • total used and available memory • NFM-P database connectivity status • redundancy configuration and status • NFM-P license information • JVM memory-usage information • alarm forwarding information • basic auxiliary server information • number and status of current process threads
-v nms_status	Verbose version of the nms_status option that returns the following additional information: • ID and status of the current process threads • general JMS server information • currently connected JMS subscribers, by topic
-s nms_status	Short version of the nms_status option that returns the following information: • system information • IP address • NFM-P database information • installation information

Option	Description
nms_info	Returns the following information from the NFM-P database: • number of managed devices by device type; for example, 7750 SR • number of MDA ports by type • number of equipped ports by type • number of services by type; for example, IES or VLL • number of access interfaces, connection termination points, and channels, by type • number of alarms, listed in order of severity • lists of enabled statistics, file, and accounting policies, including the counts and the polling frequency for different types of objects
nms_version	Returns NFM-P software release information
jvm_version	Returns version information about the currently running Java Virtual Machine environment
script_env	Returns main server script environment information
read_config	Rereads the nms-server.xml server configuration file while the server is running in order to put configuration file updates into effect
force_restart	Forces the NFM-P main server to restart
force_stop	Forces the NFM-P main server to stop
passwd <*username*> <*current*> <*new*> where *username* is the NFM-P database username, for example, samuser *current* is the current password *new* is the new password	Changes the NFM-P database user password
read_metrics_config	Reads the server metrics configuration file
import_license	Imports a new license zip file for the server
threaddump	Prints a thread dump for every SAM java process running on the station
webstart	Starts the web server
webstop	Stops the web server
webstatus	Prints web server status
webforce_restart	Forces the web server to restart
webforce_stop	Forces the web server to stop and not restart
jmsstart	Starts the JMS server in interactive mode
jmsstop	Stops the JMS server

Option	Description
jmsstatus	Returns information that includes the following: • general JMS server information • currently connected JMS subscribers, by topic
jmsread_config	Reread the JMS server configuration file while the JMS server is running
jmsforce_restart	Forces the JMS server to restart
jmsforce_stop	Forces the JMS server to stop
jmsjvm_version	Returns version information about the currently running Java Virtual Machine environment
jmsappserver_status	Returns the JMS server status
jmsscript_env	Returns the JMS script environment
no keyword, help, or ?	Lists the available command options

4

To check the status of an NFM-P auxiliary server, perform the following steps.

1. Enter the following at the CLI prompt:

   /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash aux_status ↵

   The general server status is displayed.
2. Enter the following at the CLI prompt:

   /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxappserver_status ↵

   Detailed NFM-P server information is displayed.
3. To obtain more specific server status information, run the nmsserver script using the appropriate option from the following table in place of the aux_status or appserver_status option.

   NFM-P auxiliary-server startup script options

Option	Description
auxappserver_status	Returns information about the operational status of the auxiliary server
auxdebug	Starts the auxiliary server in interactive mode
auxforce_restart	Forces the auxiliary server to restart
auxforce_stop	Forces the auxiliary server to stop
auxjvm_version	Returns the auxiliary server JVM version
auxread_config	Directs the auxiliary server to read and apply the settings in the general configuration file

Option	Description
auxread_metrics_config	Directs the auxiliary server to read and apply the settings in the metrics configuration file
auxscript_env	Returns auxiliary server script environment information
auxstart	Starts the NFM-P auxiliary server
auxstatus	Returns information about the auxiliary server that includes the following: • IP address • port number • NFM-P database connections • installed server software release ID
auxstop	Stops the NFM-P auxiliary server
aux_version	Returns auxiliary server software release information
auxthreaddump	Returns a thread dump for every auxiliary server process currently running on the station
auxhelp, *no keyword*, or ?	Lists the available command options

5

Review and record the displayed information for technical support, if required.

6

Close the console window.

7

View the NFM-P server logs for error messages using the LogViewer utility, as described in Chapter 5, “Network troubleshooting using NSP functions”.

8

Report the error messages that you find to a technical support representative.

END OF STEPS

4.30 Problem: NFM-P server and database not communicating

4.30.1 Purpose

Perform this procedure when an NFM-P server cannot connect to an NFM-P database.

4.30.2 Steps

1

Verify network connectivity between both the primary and standby servers and the primary and standby NFM-P databases by ensuring that both the primary and standby servers and the primary database can ping each other. See Chapter 3, “Troubleshooting the NSP platform”.

2

Ensure that the ports specified at installation time are available and not being blocked by firewalls; see Chapter 3, “Troubleshooting the NSP platform”.

3

Perform the following troubleshooting activities for the primary NFM-P database, as described in 4.25 “Problem: Primary or standby NFM-P database is down” (p. 79).

- Verify the NFM-P database IP address and instance name.
- Verify that the database instance is running.
- Verify that the database is running in the correct mode.

END OF STEPS

4.31 Problem: An NFM-P server starts up, and then quickly shuts down

4.31.1 Solution

When a server starts then stops, collect the logs identified in 4.2 “To collect NFM-P log files” (p. 44) and contact your technical support representative.

4.32 Problem: Client not receiving server heartbeat messages

4.32.1 Purpose

Perform this procedure when an NFM-P client is not receiving heartbeat messages.

4.32.2 Steps

1

Verify network connectivity between both the primary and standby servers and the clients by ensuring that both the primary and standby servers and the clients can ping each other. See Chapter 3, “Troubleshooting the NSP platform”.

2

Verify that the NFM-P server and client clocks are synchronized. To set the date and time for NFM-P server and client clocks, see the *NSP System Administrator Guide*.

END OF STEPS

4.33 Problem: Main server unreachable from RHEL client station

4.33.1 Purpose

Perform this procedure to check the IP connectivity between an NFM-P client and main server using ping commands. When the ping commands indicate that IP communication is active but there are still IP reachability issues, the problem could be poor LAN performance.

4.33.2 Steps

1

Perform a ping test to measure reachability, as described in 6.23 “Problem: Lost connectivity to one or more network management domain stations” (p. 359).

2

If you cannot ping the main server from a RHEL single-user client or client delegate server station, ensure that the server hostname is in the /etc/hosts file on the client station.

1. Log on to the client station as the root user.
2. Enter the following:

   ```
   # cd /etc ↵
   ```
3. Open the hosts file with a plain-text editor such as vi.
4. Edit the file, as required, to contain the following:

   ```
   server_IP server_hostname
   ```

   where

   server_IP is the IP address of the main server

   server_hostname is the hostname of the main server
5. Save the changes and close the file.

END OF STEPS

4.34 Problem: Excessive NFM-P server-to-client response time

4.34.1 Increasing available server network management resources

As the number of managed devices grows and as more GUI or OSS clients are brought online, the processing load on the NFM-P system increases. For optimum NFM-P performance, you must ensure that the NFM-P configuration meets the requirements in the *NSP Planning Guide* as your network expands.

You can do the following to increase the available NFM-P server network management resources:

- Deploy the NFM-P system in a distributed configuration.
- Deploy the NFM-P system in a redundant configuration.
- Deploy NFM-P auxiliary servers.
- Reallocate the NFM-P server resources that are assigned to groups of managed devices.

See the *NSP NFM-P Classic Management User Guide*, , and the *NSP Installation and Upgrade Guide* for information about a particular option. Contact technical support for reconfiguration assistance.

Perform this procedure to check the following:

- NFM-P auxiliary server status

  System performance may degrade if the number of available Preferred and Reserved auxiliary servers drops below the number of configured Preferred auxiliary servers.
- NFM-P main server status

  Alarms raised against the NFM-P main server may provide information about the performance degradation.

4.34.2 Steps

CAUTION

Service Disruption

Only Nokia support staff are qualified to assess and reconfigure an NFM-P deployment.

Contact your technical support representative for assistance.

1

Open an NFM-P client GUI.

2

Choose Administration→System Information. The System Information form opens.

3

Click on the Faults tab to view auxiliary server and general NFM-P system alarm information, if required.

4

If your NFM-P deployment includes one or more auxiliary servers, perform the following steps to check the status of each auxiliary server.

1. Click on the Auxiliary Servers tab.
2. Review the list of auxiliary servers.
3. Select an auxiliary server in the list and click Properties. The properties form for the auxiliary server is displayed.
4. Review the information, which includes:
   - the auxiliary server IP address
   - the auxiliary server hostname
   - the auxiliary server port number
   - the auxiliary server type (Reserved or Preferred)
   - the auxiliary server status (Unknown, Down, Up, or Unused)
5. If the auxiliary server status is Down, perform 4.29 “Problem: Cannot start an NFM-P server, or unsure of NFM-P server status” (p. 82) on the auxiliary server.
6. If the auxiliary server status is Unknown, perform 4.39 “Problem: Slow or failed resynchronization with network devices” (p. 94) to check the connectivity between the managed network and the main and auxiliary servers.

5

Close the System Information form.

END OF STEPS

4.35 Problem: Unable to receive alarms on the NFM-P, or alarm performance is degraded

4.35.1 General information

By default, the system begins purging alarms when the outstanding alarm count reaches 50 000, unless historical alarm record logging and purging alarm policies are configured to keep the outstanding alarm count below that level.

4.35.2 Steps

CAUTION

Service Disruption

Exceeding the alarm limit configured in the nms-server.xml file may cause system performance problems.

Contact your technical support representative for assistance.

1

Check the status bar of the NFM-P client GUI status bar for indications that the maximum number of alarms for the system is reached.

2

If required, clear outstanding alarms or delete them to the alarm history record log, as described in the *NSP NFM-P Classic Management User Guide*.

3

If the NFM-P system includes one or more auxiliary servers, perform 4.34 “Problem: Excessive NFM-P server-to-client response time” (p. 89) to ensure that system performance is not degraded because of auxiliary-server unavailability.

4

Contact your technical support representative for more information.

END OF STEPS

4.36 Problem: All SNMP traps from managed devices are arriving at one NFM-P server, or no SNMP traps are arriving

4.36.1 Configuration for SNMP trap notifications

When you install the NFM-P, you specify the port on which SNMP traps arrive.

In addition, the following configuration is required for SNMP trap notifications to work:

- Enable the SNMP parameters on the devices before managing them.
- Ensure that a unique trapLogId is specified for each router to communicate with the NFM-P.

Note: You must have sufficient user permissions, for example, admin permissions, to configure SNMP on a device.

4.36.2 Steps

1

See the commissioning chapter of the *NSP NFM-P Classic Management User Guide* for more information about configuring devices for NFM-P management.

2

Configure SNMP on the device using CLI.

END OF STEPS

4.37 Cannot manage new devices

4.37.1 New devices cannot be managed

The possible causes are:

- The number of managed devices or MDAs exceeds the licensed quantity.
- Large packet sizes from the managed devices are being dropped by intermediate routers because the packets exceed the device MTU, causing resynchronizations to fail.

Additional devices cannot be managed, but can be discovered, when the licensed MDA limit is exceeded.

4.37.2 Steps

CAUTION

Service Disruption

Do not modify other nms-server.xml parameters. Modifying the file can seriously affect network management and performance of the NFM-P.

Consult technical support before you attempt to modify parameters.

1

Check the license key status.

1. The NFM-P generates an alarm when a license limit is exceeded or nearly exceeded. View the NFM-P alarm list in the client GUI, or use an OSS client to monitor the JMS alarm event stream for license alarms.
2. Choose Help→NFM-P License Information from the NFM-P main menu. The NFM-P License (Edit) form opens.
3. Click on the Devices and Quantities Licensed tab.
4. View the information to ensure that the required Remaining quantity is not equal to zero.

   Note:

   If you have a new license that supports a greater number of managed objects, you can dynamically update the license without restarting the main server. See the *NSP NFM-P Classic Management User Guide* for information about updating an NFM-P license.
5. Close the NFM-P License (Edit) form.

2

Ensure that the new devices are configured to send SNMP packets of up to 9216 bytes. Check the MTU size, as described in 6.25 “Problem: Packet size and fragmentation issues” (p. 361).

END OF STEPS

4.38 Problem: Cannot discover more than one device, or device resynchronization fails

4.38.1 General information

Consider the following:

- When using SNMPv3 encryption, the engine ID of the managed device must be unique. As well, SNMP issues may result in Polling Problem alarms. Otherwise, the following issues may occur:
  - unreliable or slow discovery of network devices
  - resynchronization during scheduled polling fails
  - slow communication and synchronization times
  - polling fails completely
- When NFM-P resynchronizes some functions on an NE, for example, BGP configurations for the 7750 SR, the SNMP packets may be broken into two or more smaller packets, when the maximum PDU size of 9216 bytes is exceeded.
- Each MIB entry policy has its own polling interval. When there is insufficient time in a polling interval for a resynchronization to occur, the interval may need to be changed to ensure proper resynchronization.

4.38.2 Steps

1

For resynchronization issues that may be caused due to insufficient MIB polling intervals.

2

Choose Administration→Mediation from the NFM-P main menu. The Mediation (Edit) form opens with the General tab selected.

3

Ensure that the Polling Admin State is Up.

Note: Polling and scanning use system resources, and can increase the amount of management traffic. Consider your network needs and network management domain capabilities before setting these parameters.

4

Check the MIB polling intervals for different managed devices, as required, by clicking on the MIB Entry Policies tab.

A list of MIBs appears, organized by managed device type.

1. Select a MIB in the list and click Properties.
2. Configure the Polling Interval parameter to ensure that sufficient time is configured for the polling to occur.
3. Configure the Administrative State of polling for the MIB entry, if required.

4. Click OK to save the changes and close the form, or click Cancel to close the form without saving changes, as required.

End of steps

4.39 Problem: Slow or failed resynchronization with network devices

4.39.1 General information

When NFM-P performance is slow, especially when performing network device resynchronizations, SNMP and IP performance along the in-band or out-of-band interfaces between the network device and the NFM-P server may be the problem.

Check the following:

- configuration of the LAN switch port and the NFM-P station port match
- configuration of the LAN switch port and the network device management ports match
- mediation policy SNMP timeout and retry values are sufficient to allow the transfer of data between network devices and the NFM-P

4.39.2 Steps

1

Ensure that port configurations are compatible for the NFM-P server, the network device management ports, and the LAN switch. This is normally done by configuring auto-negotiation between the platforms, but your network may require more specific configuration.

2

Check whether all data is being transferred between the network device in-band management port and the NFM-P server.

1. Open a Telnet or SSH session to the device from the NFM-P.
2. Check statistics on the in-band management port of the device:

   ```
   # monitor port 1/2/3
   ```

   Check the output for the following.
   - errors that may indicate a communication problem with the a LAN switch.
   - Over each time interval, is the number of input and output packets constant? This may indicate intermittent traffic.
   - Are there more input packets or octets being transferred than output packets or octets? This may indicate a unidirectional traffic problem.

   The types of error messages displayed determine the action to take.
   - For failure errors, consider increasing the SNMP timeout value
   - For collision errors, consider increasing the SNMP retry value
3. Check the mediation policy for the device using the NFM-P client GUI. Check the SNMP timeout and retry value for the mediation policy.

If the output of step 2 indicates failures, consider increasing the default SNMP timeout value and perform step 2 again.

When the output of step 2 indicates frequent collisions, consider increasing the default SNMP number of retries value, then retest to see if resynchronizations are more reliable. Increasing the number of retries increases the likelihood that an SNMP packet is not dropped due to collisions.

You can check SNMP timeout and retry values from the Administration→Mediation menu. Click on the Mediation Security tab.

CAUTION:

When LAN performance is poor, increasing timeout values may mask an underlying problem. Increasing the SNMP timeout value in an environment where collisions are frequent reduces performance. Timeout values should be based on typical network response times

Check LAN communication issues, as specified in Chapter 3, “Troubleshooting the NSP platform”. If problems persist, collect the logs as specified in 2.1 “Before you call support” (p. 25) and contact your technical support representative.

END OF STEPS

4.40 Problem: Statistics are rolling over too quickly

4.40.1 Problem

Statistics database tables roll over, or lose statistics during an interval, if the tables fill before all statistics are collected or the next collection interval starts.

Solution

To ensure sufficient statistics collection, consider the following:

- the statistics table size, depending on the configuration specified in the *NSP Installation and Upgrade Guide*
- the number of statistics collected, the number of objects with statistics collection enabled, and the frequency of statistics collection, as specified in the *NSP NFM-P Classic Management User Guide*
- the OSS requests data from the statistics tables less frequently than the configured rollover interval
- FTP must be enabled on the managed device in order for the NFM-P to retrieve statistics.

Nokia recommends that statistics collection planning includes the following considerations to prevent the loss of statistics data.

- measure the rate of statistics collection over a sufficient time interval
- determine the appropriate collection interval and statistics database table size based on individual network configurations
- ensure that the polling interval is sufficient for polled statistics

4.41 Problem: Y.1564 service test results not published to Kafka

4.41.1 General information

Y.1564 service test results are not published to Kafka if the test has timed out.

When this situation occurs, the **staleTestTime** duration must be updated to prevent timeouts.

4.41.2 Steps

CAUTION

Service Disruption

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the nms-server.xml file.

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor such as vi.

6

Edit the following line:

`staleTestTime="value"`

Update the value to reflect the required test duration interval to avoid timeout.

7

Save and close the nms-server.xml file.

8

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_sync ↵
```

The NFM-P puts the configuration change into effect.

9

Close the console window.

10

Re-run the Y.1564 service tests, with the **Publish to Kafka** parameter enabled.

END OF STEPS

Troubleshooting NFM-P clients

4.42 Problem: Cannot start NFM-P client, or error message during client startup

4.42.1 Prerequisites

Before you proceed, ensure that the following conditions are present:

- the NFM-P client and server have the same software versions and compatible patch sets
- the login name and password of the user are correct
- there are no OS errors
- a local firewall is running on the client station

4.42.2 Steps

1

If the NFM-P client is installed on RHEL and you receive a “Cannot execute” message when you try to run the client, the client executable file permission may have been reset by an event such as an auto-client update failure. You must ensure that the correct file permissions are assigned.

1. Log in as root, or as the user that installed the client, on the client station.
2. Open a console window.
3. Enter the following:

   # **chmod +x *path*/nms/bin/nmsclient.bash**

   where *path* is the NFM-P client installation location, typically /opt/nsp/client

2

Review the login messages that are displayed when a client GUI attempts to connect to a server. Messages that state things like the server is starting or the server is not running indicate the type of problem.

3

Ensure that the user name and password are correct.

4

To check that the NFM-P server is up and to view additional server configuration information, perform the following steps.

1. Log on to the NFM-P server station as the nsp user.
2. Open a console window.
3. Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

4. Enter the following:

   `./nmsserver.bash appserver_status` ↵

   Server status and configuration information are displayed.

5. To check additional server status conditions, perform 4.29 “Problem: Cannot start an NFM-P server, or unsure of NFM-P server status” (p. 82).

5

Check the client GUI login error message.

When a firewall is running locally on the client station, a login error message may appear indicating that the server is not available. Ensure that a local firewall is not preventing a connection to the server, and that the NFM-P server IP address is in the client host-lookup file.

END OF STEPS

4.43 Problem: NFM-P client unable to communicate with NFM-P server

4.43.1 Prerequisites

Before you proceed, ensure that the following conditions are present:

- The NFM-P client points to the correct IP address and port of the server.
- The problem is not a network management domain LAN issue. See Chapter 3, “Troubleshooting the NSP platform” for more information.
- Firewalls between the NFM-P clients and the server are correctly configured

4.43.2 Steps

1

To check that the NFM-P client points to the correct IP address and port of the server, open the nms-client.xml file using a text editor. The default file location is *installation_directory*/nms/config.

where *installation_directory* is the directory in which the NFM-P client software is installed, for example, /opt/nsp/client

2

Verify the IP address of the server as specified by the ejbServerHost parameter.

3

Verify the server port as specified by the ejbServerPort parameter.

4

Modify the IP address and port values, if required.

5

Save the file, if required.

6

Perform 4.29 “Problem: Cannot start an NFM-P server, or unsure of NFM-P server status” (p. 82) to check the server status. A client cannot connect to an NFM-P server that is not started.

7

If the server is started, compare the firewall and network configuration guidelines in the *NSP Planning Guide* with your network configuration to ensure that it complies with the guidelines.

8

Contact your technical support representative if the problem persists.

END OF STEPS

4.44 Problem: Delayed server response to client activity

4.44.1 Causes

Possible causes are:

- a congested LAN
- improperly sized platforms

Using the netstat command on the client may help troubleshoot network throughput problems. When an Ethernet LAN is highly congested, the actual throughput slows down. This is caused by packets colliding on the LAN as multiple machines begin to transmit at approximately the same time, for example, when multiple GUI or OSS clients are performing tasks simultaneously.

4.44.2 Steps

1

Client GUIs may respond more slowly than normal during resynchronizations of managed devices. Repeat the client GUI action when the resynchronization is complete.

2

Check for LAN throughput issues.

1. Open a shell console window.
2. Enter the following at the console prompt to display local network-interface transmission data over a period of time:

   ```
   # netstat -i s ↵
   ```

where *s* is the time, in seconds, over which you want to collect data. Nokia recommends that you start with 50 s

3. Review the output. The following is sample netstat output:

```
netstat -i 5
input   le0       output           input   (Total)    output
packets errs  packets errs  colls packets errs  packets
errs  colls
6428555 41    541360  80    49998 6454787 41    567592  80
49998
22      0     0       0     0     22      0     0       0     0
71      0     7       0     3     71      0     7       0     3
```

This sample displays the number of input and output packets, errors and collisions on the le0 interface. One column displays the totals for all interfaces. This sample only has one interface, so both sets of columns display the same data.

Calculate the number of collisions as a percentage of the number of output packets. For example, according to the last line of output, there were three collisions and seven output packets resulting in a 42% rate.

This number is high, but the time in which the sampling was obtained (5 s), was low. Change the sample rate to, for example, 50 s for an accurate sampling of the network throughput.

When collisions are between 2% and 5%, congestion on the interface is within the normal operating range.

In a typical network, when collisions are greater than 5%, you may have a serious congestion problem on the interface. Review your LAN topology and design to reduce the number of network bottlenecks.

4. To stop the command, press Ctrl-C.

3

Check that the server and client platforms are appropriately sized. See the *NSP Planning Guide* for more information.

End of steps

4.45 Problem: Cannot place newly discovered device in managed state

4.45.1 Solution

If the newly discovered device cannot be placed in a managed state, ensure that the number of managed MDAs do not exceed the NFM-P license. Also, check for resynchronization problems between the managed network and the NFM-P. See 4.37 “Cannot manage new devices” (p. 92).

4.46 Problem: User performs action, such as saving a configuration, but cannot see any results

4.46.1 Causes

Possible causes are:

- Failed SNMP communication between the server and managed device; see 4.36 “Problem: All SNMP traps from managed devices are arriving at one NFM-P server, or no SNMP traps are arriving” (p. 91).
- Failed deployment of the configuration request.

4.46.2 Steps

1

For the NFM-P client, perform the following:

1. Choose Administration→NE Maintenance→Deployment from the NFM-P main menu.

   The Deployment form opens. Incomplete deployments are listed, and deployer, tag, state and other information is displayed.

   The possible states for a deployment are:
   - Deployed
   - Not Deployed
   - Pending
   - Failed — Resource Unavailable. Failure occurred because one of the resources required to apply the configuration is not present in the NFM-P database
   - Failed — Configuration. Failure occurred because the configuration could not be applied to the specified objects
   - Failed — Partial. Failure occurred at deployment and some of the configuration can been sent to the network
   - Failed — Internal Error. Failure a occurred due to general error conditions. Code is intended as a catch-all code for all other possible errors
   - Cancelled
   - Postponed

   You can also suspend or resume deployment retries by clicking Suspend Retries or Resume Retries. You can clear a deployment by clicking Clear. When you clear a deployer, no further attempt is made to reconcile the network device status with the NFM-P database. Affected objects should be resynchronized.

   If a deployment is not sent to a managed device, the intended configuration change is not made on the device.
2. Choose a failed deployment and click Properties to view additional information. The deployment properties form opens.

2

When a deployment fails and you receive a deployment alarm, check the following steps:

1. Using CLI, check on the device whether the deployment change is on the device.
2. If the change is on the device, the deployment alarm was likely raised because the configuration already exists on the device. Clear the failed deployment and resynchronize the device with the NFM-P.

   If the change is not on the device, collect the information from the deployment properties form and contact your technical support representative.

3

Note: These steps describe how to troubleshoot asynchronous deployment requests only. Nokia recommends that deployment requests be made in asynchronous mode.

For OSS clients, perform the following steps:

1. Browse real-time alarms received via JMS. An alarm denoting a deployment failure contains the following text:

   `Attribute: alarmClassTag Value: generic.DeploymentFailure`

   The alarm also contains additional information, including the object affected by the alarm and the severity of the alarm. See the *NSP NFM-P XML API Developer Guide* for more information.
2. Find the following text in the alarm:

   `Attribute: requestID=`*`requestID`*

   The parameter specifies the request id sent with the original request. The request id should be unique per request.
3. Determine the original request using the request id.
4. Troubleshoot the original request. If there are problems with the original request, clear the deployer, fix the request, and send the new request. See the *NSP NFM-P XML API Developer Guide* for more information.
5. If there are no problems with the original request, the failure may be caused by a network communication or device failure, or by packet collisions caused by conflicting configurations.

   You can:
   - resend the request
   - troubleshoot your network or device

END OF STEPS

4.47 Problem: Device configuration backup not occurring

4.47.1 Steps

1

Use the NFM-P client to check the device database backup settings. Choose Administration→NE Maintenance→Backup/Restore from the NFM-P main menu. The Backup/Restore form opens.

2

Click on the Backup/Restore Status tab. The managed devices are listed and backup and restore status information is displayed.

3

Select the device and click Properties. The NE Backup/Restore Status form opens.

4

View the information in the Backup Status panel. A Backup State other than Successful may indicate a communication problem or a backup policy configuration error.

5

Ensure that the device configuration file and the associated index file are saved on the device and available for backup. Click on the Configuration Saves tab, and ensure that the Config Save State indicator reads Success.

See the appropriate device OS documentation for more information.

6

Click on the Backups tab to view a list of backup operations that are currently in progress. A backup operation disappears from the list after it completes.

7

Click on the Faults tab to view additional troubleshooting information.

8

Close the NE Backup/Restore Status form.The Backup/Restore form is displayed.

9

Use the information obtained from the NE Backup/Restore Status form to check the backup policy configuration, if required. Click on the Backup/Restore Policy tab.

10

Select the backup policy for the device and click Properties. The Backup Policy (Edit) form opens.

11

Ensure that the policy is assigned to the device.

1. Click on the Backup/Restore Policy Assignment tab.
2. If required, configure a filter and click OK.
3. Move the device to the Assigned Sites list if it is not there by selecting the site from the Unassigned Sites list and clicking on the right-arrow button.
4. Click Apply to save changes, as required.

12

Click on the General tab.

13

Verify the parameter settings and modify, if required.

14

Save the changes and close the form.

END OF STEPS

4.48 Problem: NFM-P client GUI shuts down regularly

4.48.1 Causes

The NFM-P client GUI automatically shuts down under the following conditions:

- no activity on the GUI for a specified amount of time
- no communication between the GUI and the server for a specified amount of time.
- when there is an communication error that causes problems between the server and the client

Note: Changing the OS clock setting on the server station can cause communication problems on the client. If the server clock setting changes significantly, the clients must log off and the server must be restarted. Nokia recommends that the server OS clock be tied to a synchronous timing source to eliminate time shifts that may lead to polling and communication problems.

4.48.2 Steps

1

Disable the GUI activity check, if required. Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The Security Management (Edit) form appears with the General tab selected.

2

Set the Client Timeout (minutes) parameter to 0 to disable the GUI inactivity check. Alternately, you can configure a higher value for the parameter, to increase the time that must pass before the client GUI is shut down due to inactivity.

3

Click Apply and close the form.

END OF STEPS

4.49 Problem: Configuration change not displayed on NFM-P client GUI

4.49.1 Solution

The NFM-P supports the configuration of complex objects, for example, services, using configuration forms or templates. Additional configuration forms and steps may be contained by main, or parent, configuration form. For example, when you configure a VLL service, a site configuration form is contained within the main configuration form. In turn, an L2 interface configuration form is contained within the site configuration form. Alternatively, when you use service templates, parent templates for site configuration must also be configured.

Objects configured in contained configuration forms are not saved until the parent configuration form is saved. For example, when you configure a VLL service, sites or L2 interfaces that you configure are not saved during service creation until the parent configuration form is saved. You cannot view new objects or new object configurations in other parts of the GUI, such as the navigation tree, until the service is saved. The NFM-P displays a dialog box to indicate that configured objects in a configuration form are not saved until the parent configuration forms are saved.

4.50 Problem: List or search function takes too long to complete

4.50.1 Solution

You can perform simple listings or complex searches using the Manage menu on the NFM-P main menu to query the database for information about services, customers, and other managed entities.

Depending on the type of information and the number of entries returned, a list or search operation may take considerable time to complete. As a general rule, Nokia recommends that you use filters to restrict the number of items in a list or search operation to 10 000 or fewer.

See the *NSP NFM-P Classic Management User Guide* for information about the NFM-P client GUI list and search functionality. See the *NSP Planning Guide* for information about NFM-P scalability and system capacity guidelines.

4.51 Problem: Cannot select some menu options or save some configurations

4.51.1 Solution

An NFM-P administrator can restrict user access to GUI functions, and limit the ability of a user to configure objects. See your administrator for information about your general user permissions, scope of command, and span of control.

The NFM-P license may also affect user access to functions or objects; see the *NSP System Administrator Guide* for information.

An administrative change to a user or group permission takes effect immediately, and determines which actions are available to the user or user group.

See 4.37 “Cannot manage new devices” (p. 92) to identify which NEs are licensed for NFM-P management.

4.52 Problem: The NFM-P client GUI does not display NE user accounts created, modified, or deleted using the CLI

4.52.1 Cause

When an NE user account is created, modified, or deleted using the CLI, the NFM-P client GUI does not update the user list in the NE User Profiles form. For increased security, the NE does not send a trap for changes made to NE user accounts. You can update the NFM-P with the NE user account changes by resynchronizing the NE.

4.52.2 Steps

1

On the Equipment tree, navigate to the NE. The path is Network→NE.

2

Right-click on the NE and choose Resync.

The Resync menu option specifies that SNMP MIB and CLI information bases are reread to resynchronize them with the NFM-P, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.

END OF STEPS

Part III: Troubleshooting the network

Overview

Purpose

This part provides information about network troubleshooting using NSP functions and NFM-P.

Contents

5 Network troubleshooting using NSP functions

5.1 Overview

5.1.1 Purpose

This chapter provides information about troubleshooting using various NSP functions and dashboards.

For more information on alarm management, see the *NSP Network Service and Assurance Guide*.

5.1.2 Contents

Troubleshooting using NSP assurance functions

5.2 Troubleshooting services and connectivity

5.2.1 Before you begin

This process provides a series of tasks you can perform to identify the root cause of a problem.

See the *NSP System Administrator Guide* for information about other NSP troubleshooting actions such as displaying the system status or checking system performance.

5.2.2 Steps

Assurance supervision function

1

Verify whether the administrative and operational states of each component of the service are Up:

- Sites
- Endpoints
- Tunnel Bindings

See the *NSP Network and Service Assurance Guide* for more information about each component.

2

Check the Alarm List for alarms against the services in your network.

3

Check the Event Timeline to view the history of events related to alarms, configuration, OAM test failures and state change notifications.

Alarms function

4

Verify that there are no alarms associated with any component of the service:

- The Current Alarm List view provides high-level visibility of all alarms in the network.
- Choose the Current Alarms format to see the alarm information in a list you can filter. Select an alarm to view detailed information in an information panel.

5

From the Alarm List, check the Historical Alarms and Merged Alarms lists for further information about root causes of any current alarms.

NFM-P

6

Verify that the NFM-P service configuration aligns with the customer requirements. For example, ensure that NFM-P configuration uses the correct service type and SAP configuration, and that the circuit and site are included in the service.

7

Contact your technical support representative if the problem persists.

END OF STEPS

5.3 Onboarding an NE into NSP

5.3.1 Purpose

This process shows you how to use the NSP to manage an NE, configure attributes, verify component health, and confirm that the NE is up, running, and ready for further configuration.

Prerequisites

This process assumes that the following prerequisites are in place:

- The intent type artifact bundles required for device configuration have been installed:
  - icm-equipment-card_mda
  - icm-equipment-port-connector
  - icm-equipment-port-ethernet
  - icm-router-network-interface
- The NE has been discovered in the NSP.
- Required templates and telemetry subscriptions have been created.
- Power modules and SFMs have been configured on the NE using CLI.

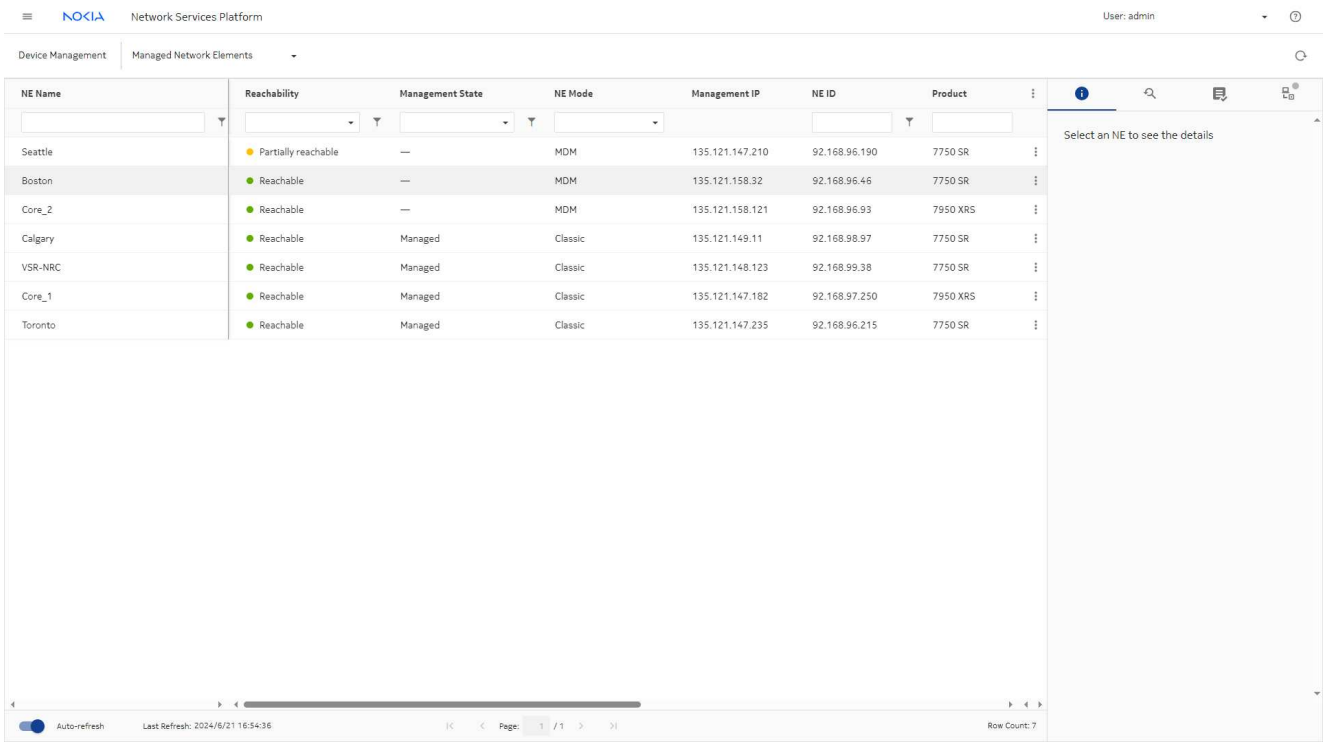
For details about intent type installation, see the *NSP Network Automation Guide*. For device discovery and template creation, see the *NSP Device Management Guide*. For telemetry subscriptions, see the *NSP Data Collection and Analysis Guide*. For CLI, see the NE documentation.

5.3.2 Resync the NE in Device Management

1

First, we'll perform a resync, to ensure that the configuration on the NE is aligned with the NSP. This step is performed immediately after the NE is discovered.

View the NE in **Device Management**, **Managed Network Elements**. A green icon indicates that the NE is reachable.



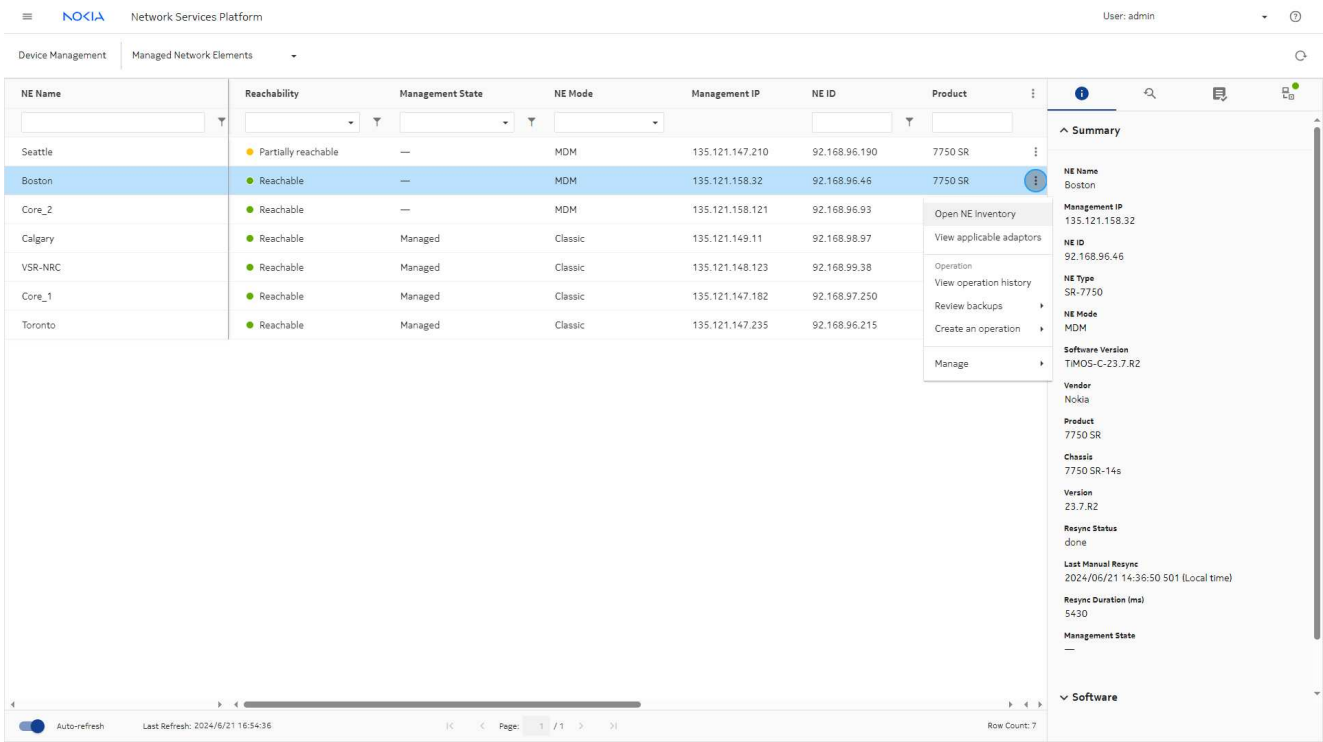
2

Select the NE and choose **Manage**, **Resync** from the table row actions menu (⋮).

5.3.3 Verify the NE inventory pre configuration

1

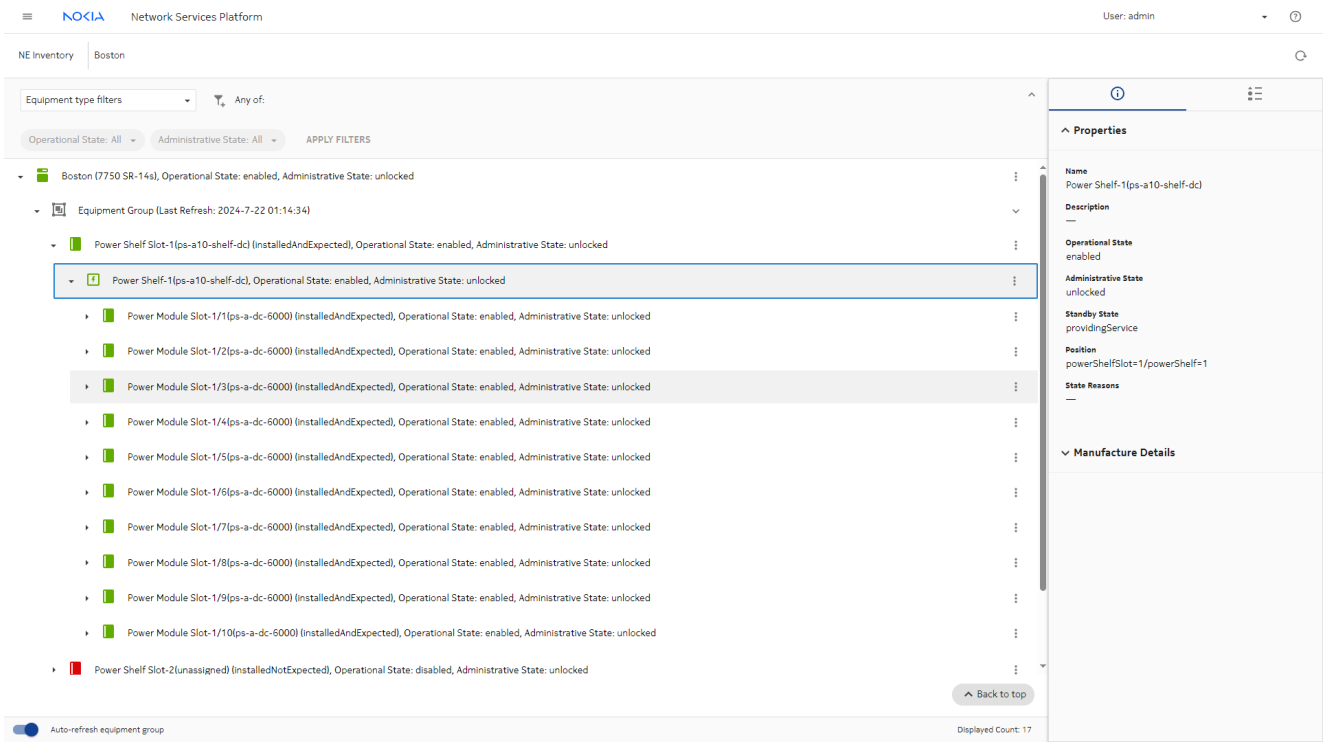
Select the NE and choose **Open in NE Inventory** from the table row actions menu (⋮).



2

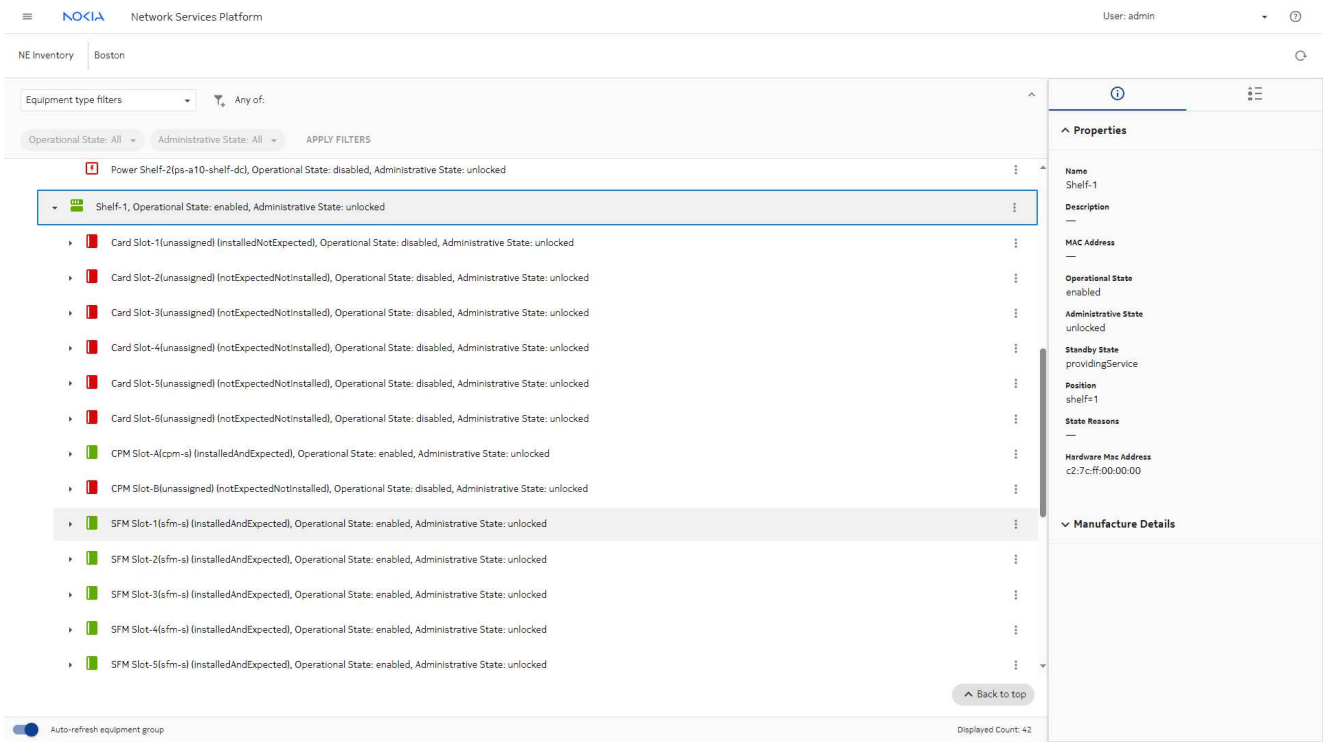
The NE inventory tree view opens in a new browser tab, displaying the components that are already configured using CLI.

Expand the Equipment group to show the status of the power shelf and power modules.



3

Expand the shelf to show the status of the SFMs.



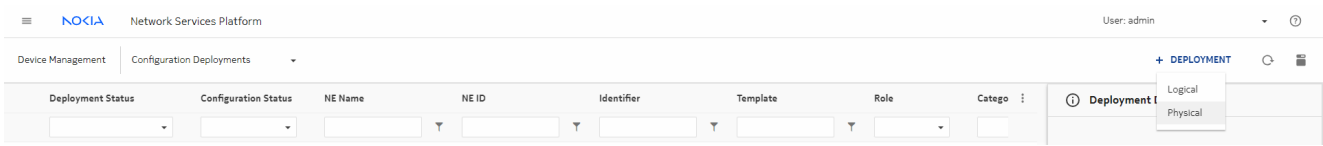
5.3.4 Create device configuration deployments for NE components

1

Next, we'll configure NE components. This can be done by deploying a series of templates in the **Device Management**, **Configuration Deployments** view.

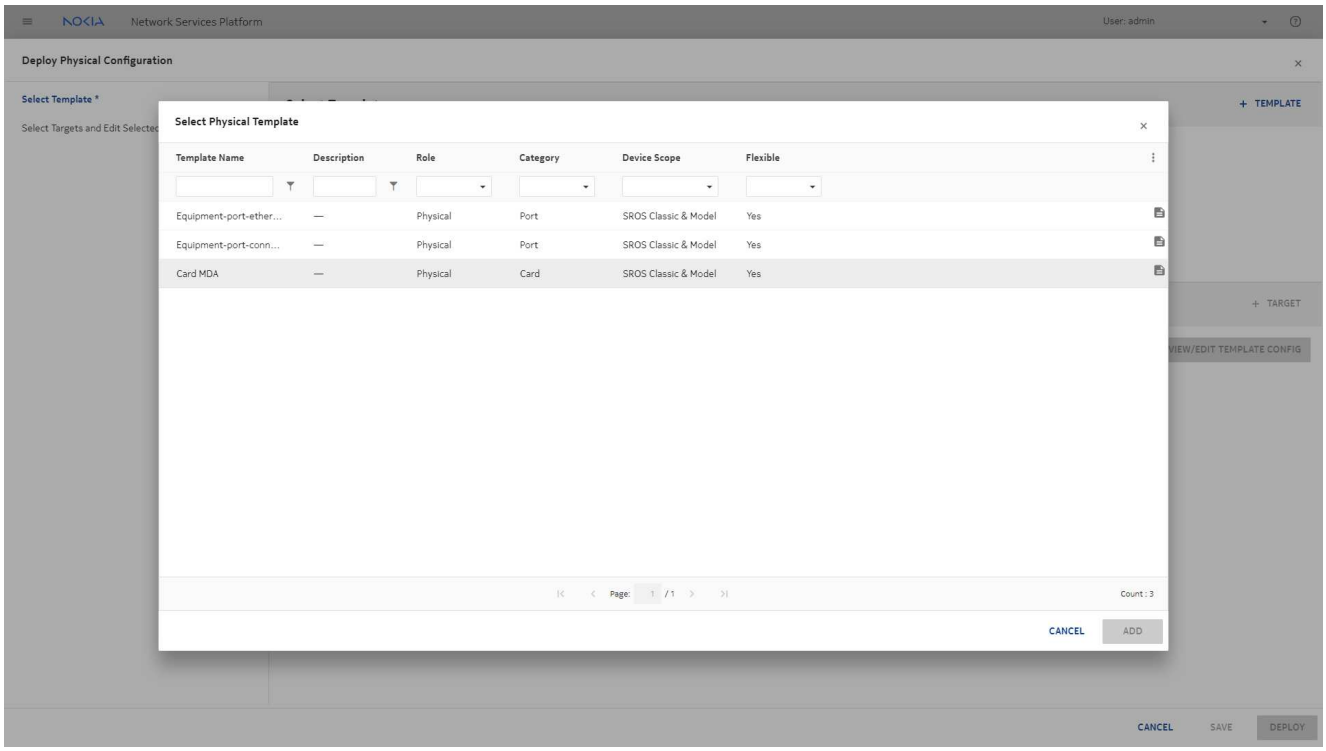
2

From the **Device Management**, **Configuration Deployments** view, click **+ DEPLOYMENT**. We'll start by configuring Cards and MDAs, which are physical components: select **Physical** from the drop-down.



3

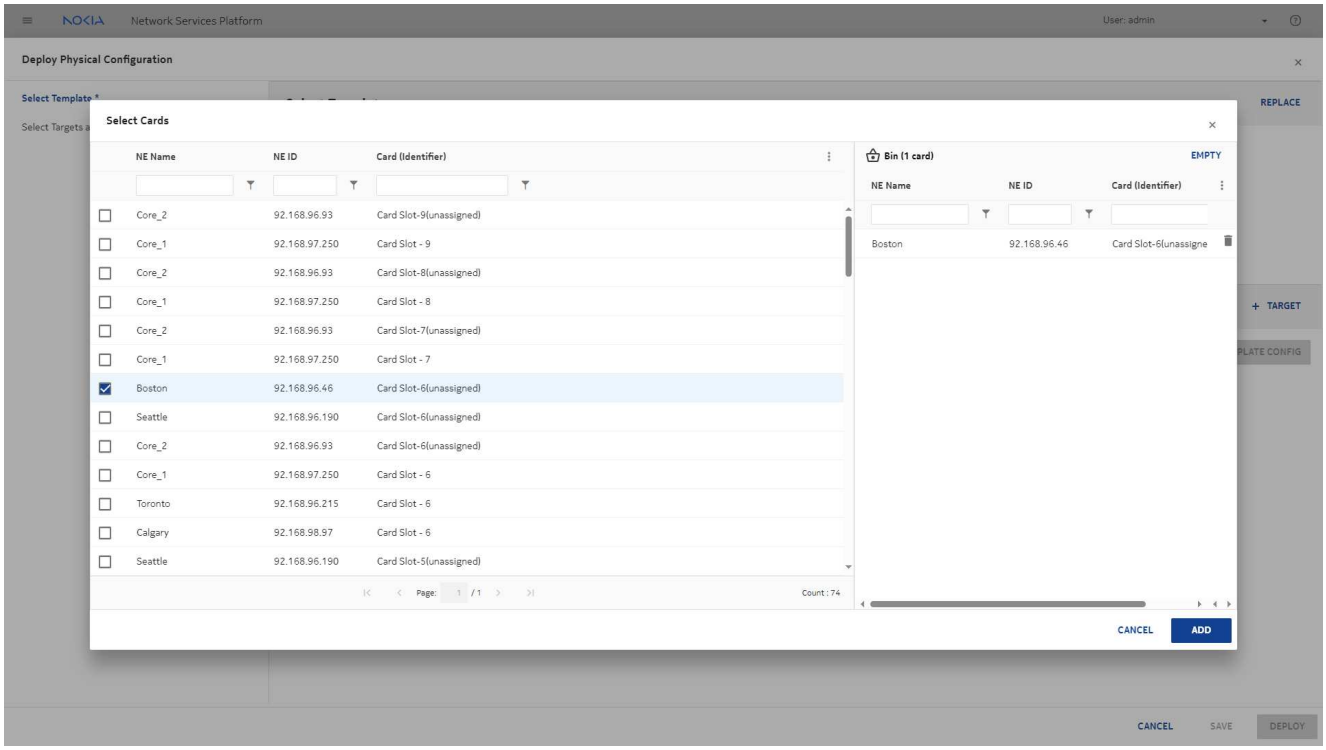
In the form that opens, click **+ TEMPLATE** and choose the template for Card and MDA configuration.



4

Choose a card to add as the target:

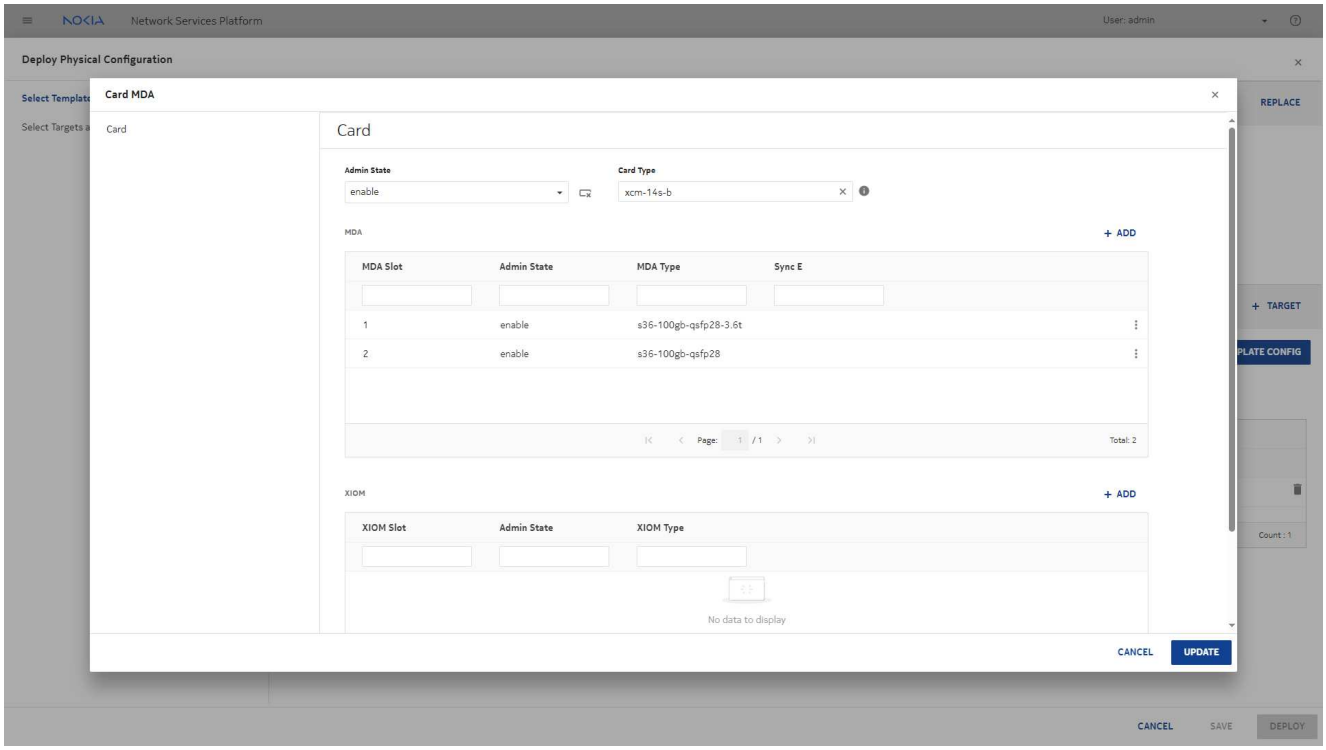
1. Click **+ TARGET** and select **Cards** as the target type.
2. Choose a card slot from the list to add it to the Bin and click **ADD**



5

Click **VIEW/EDIT TEMPLATE CONFIG**. In the form that opens, configure the card parameters:

1. Choose a card type.
2. In the MDA panel, click **+ ADD** and configure the parameters to create an MDA.
3. Click **UPDATE**.



6

Click **DEPLOY** to deploy the configuration.

7

Create physical deployments for additional connectors and ports, using their templates. The overall steps are very similar to creation of a Card and MDA deployment, but the parameters vary by template.

1. Configure deployments for port connectors if applicable, using the template created from the icm-equipment-port-connector intent type.
2. Configure deployments for ports, using the template created from the icm-equipment-port-ethernet intent type.

8

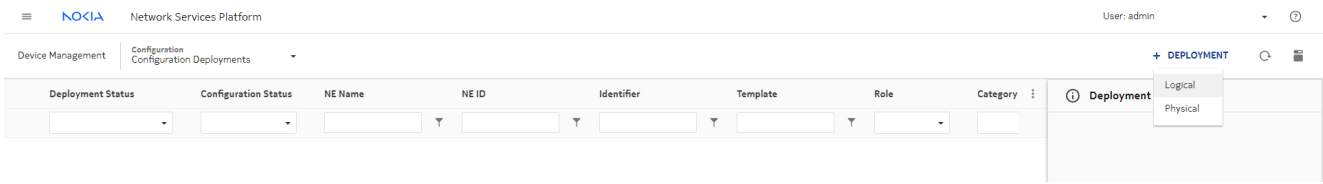
After the port configurations have been deployed, configure OSPF and ISIS routing on the NE using CLI.

9

Now we can create a logical deployment to configure a router interface.

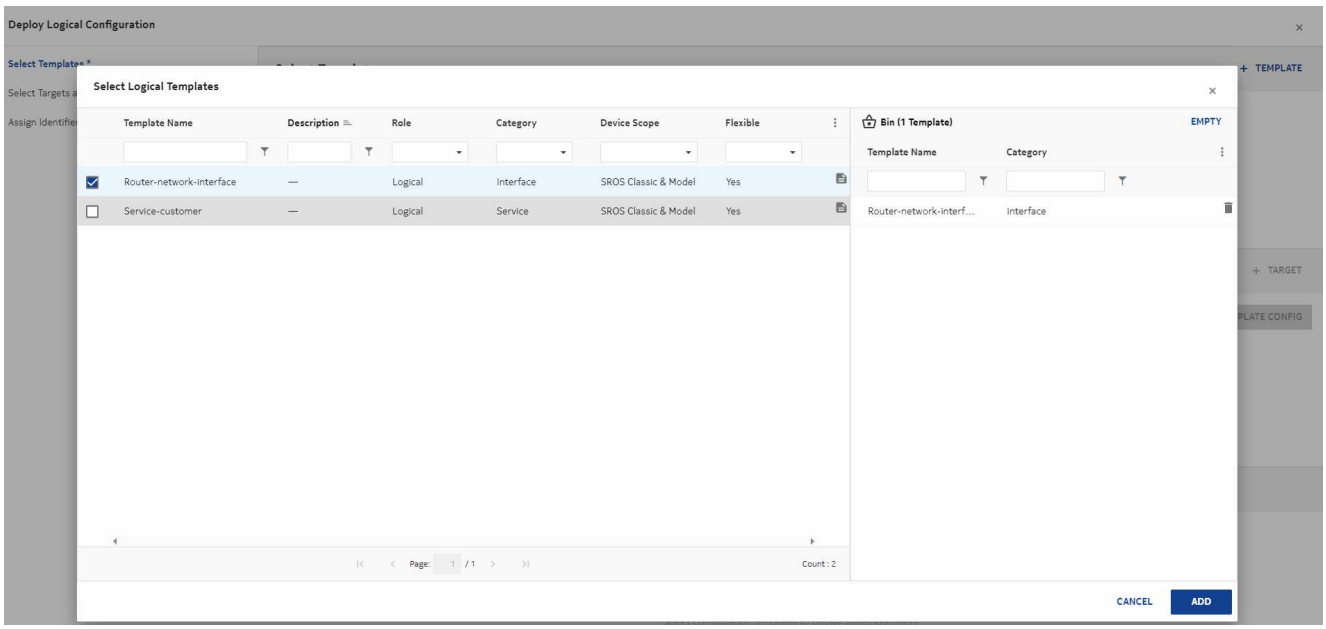
Click **+ DEPLOYMENT** and select **Logical** from the drop-down.

10



11

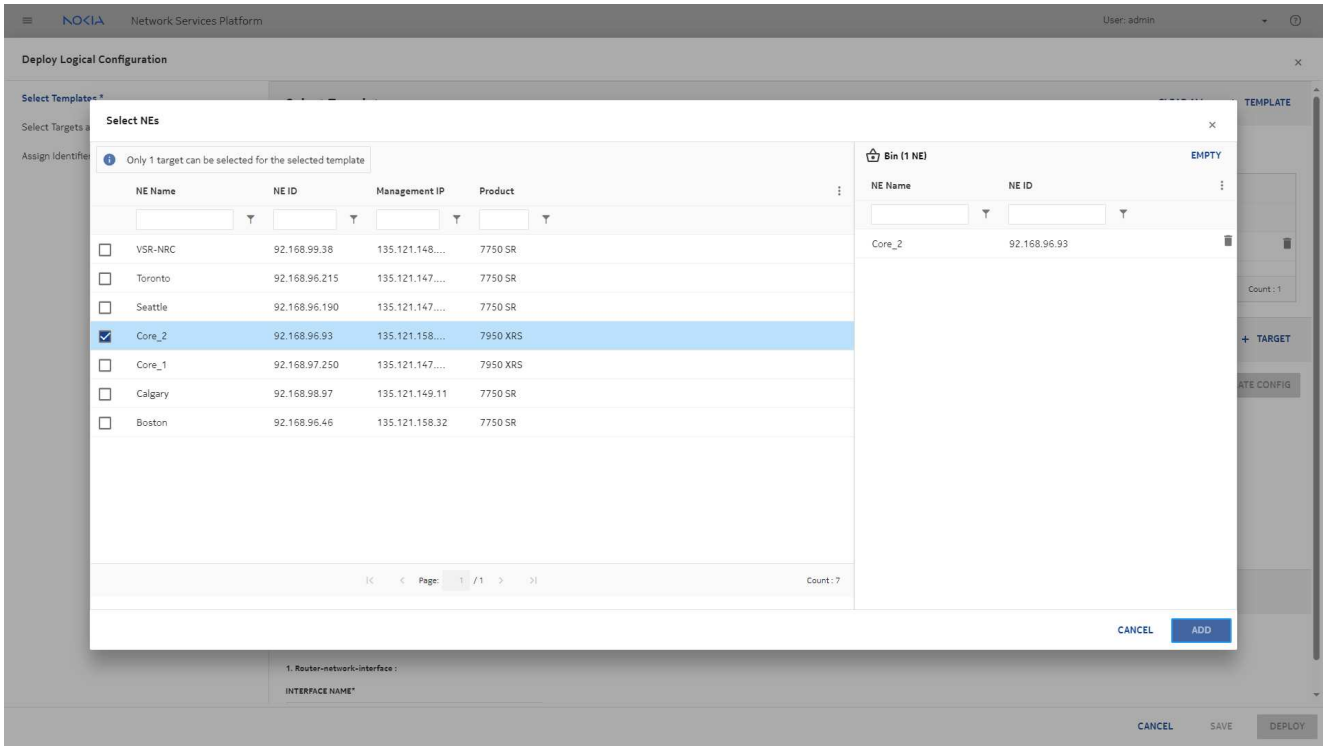
In the form that opens, click **+ TEMPLATE** and choose the template for router interface configuration. Click **ADD**.



12

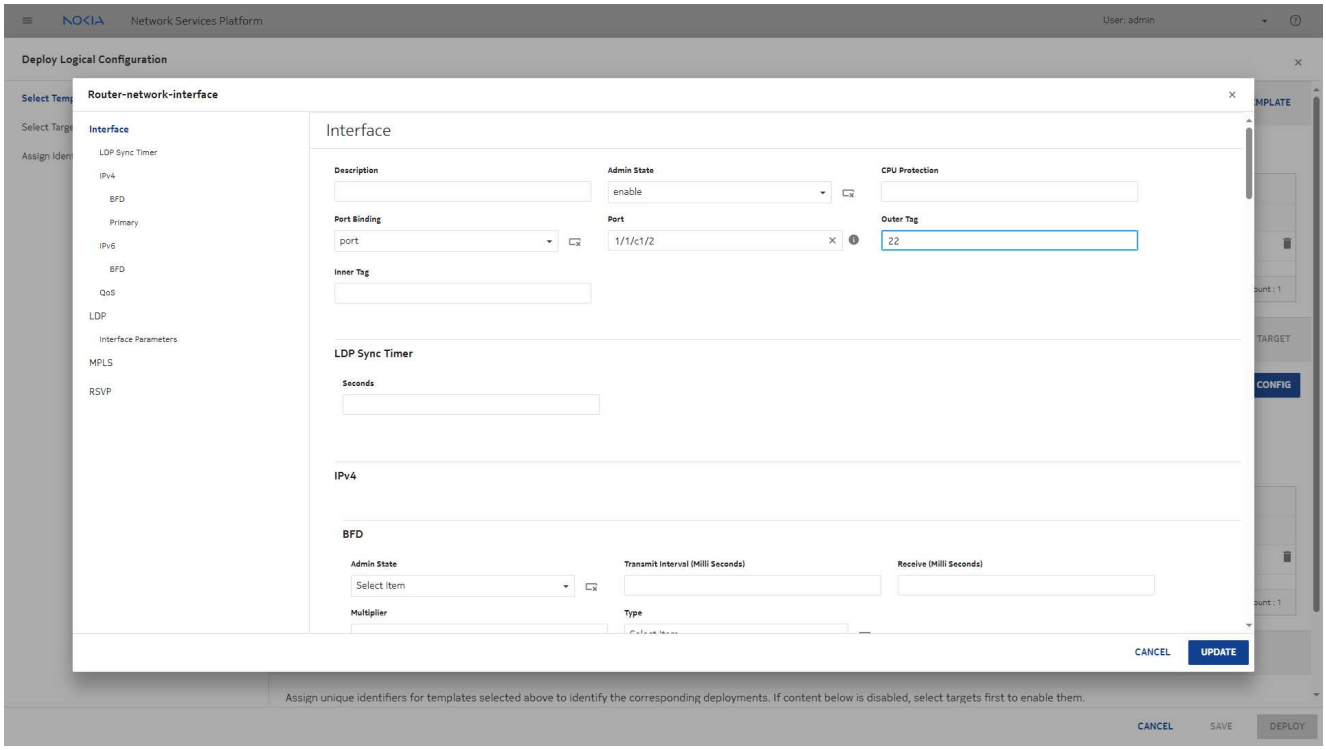
Choose a target:

1. Click **+ TARGET** and choose **NEs** from the drop-down list.
2. Choose an NE from the list to add it to the Bin and click **ADD**.



13

1. Click **VIEW/EDIT TEMPLATE CONFIG**. In the form that opens, configure the interface parameters. Scroll through the form to update parameters as needed.
2. Click **UPDATE**.

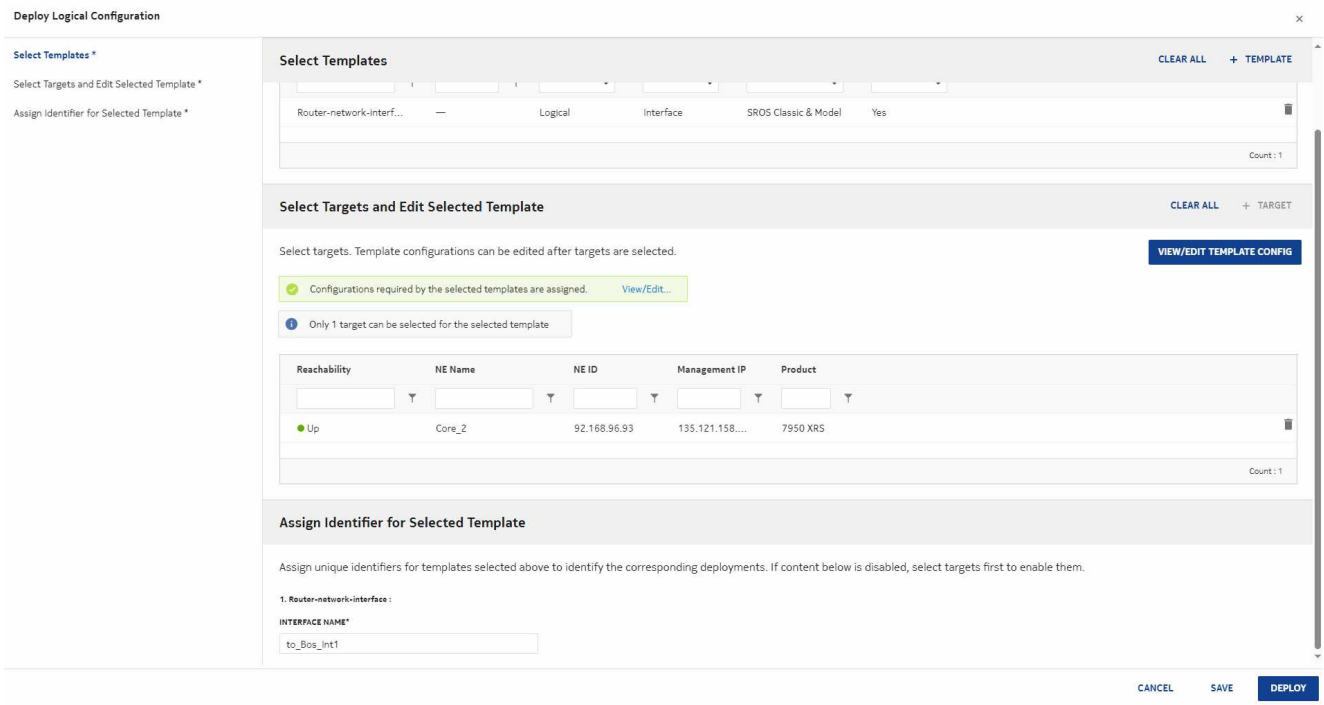


14

Enter a name for the interface in the **INTERFACE NAME** field.

15

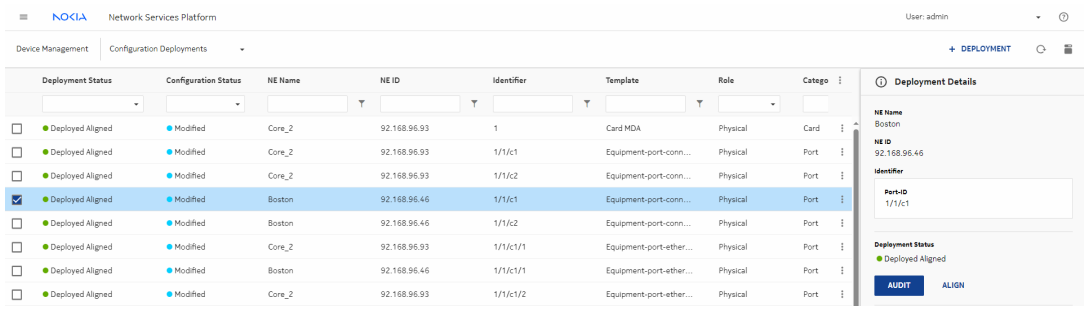
Click **DEPLOY** to deploy the configuration.



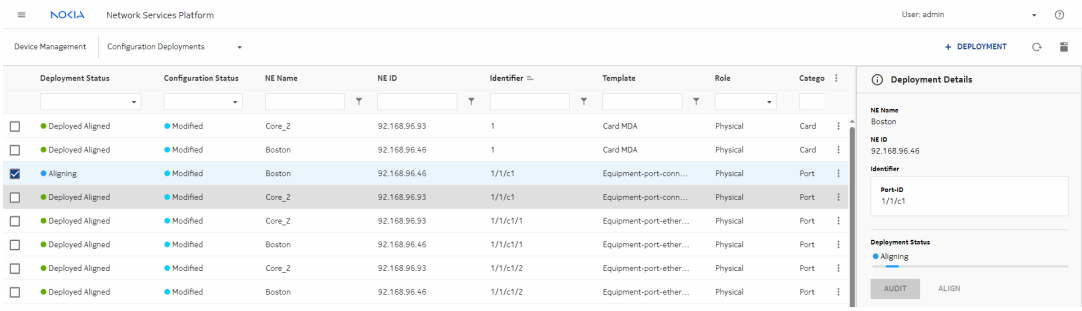
16

Audit and align each deployment:

1. For each of the deployments we created, select the deployment and click **AUDIT**.



2. Click **ALIGN** to ensure that the NE configuration is aligned with the templates.

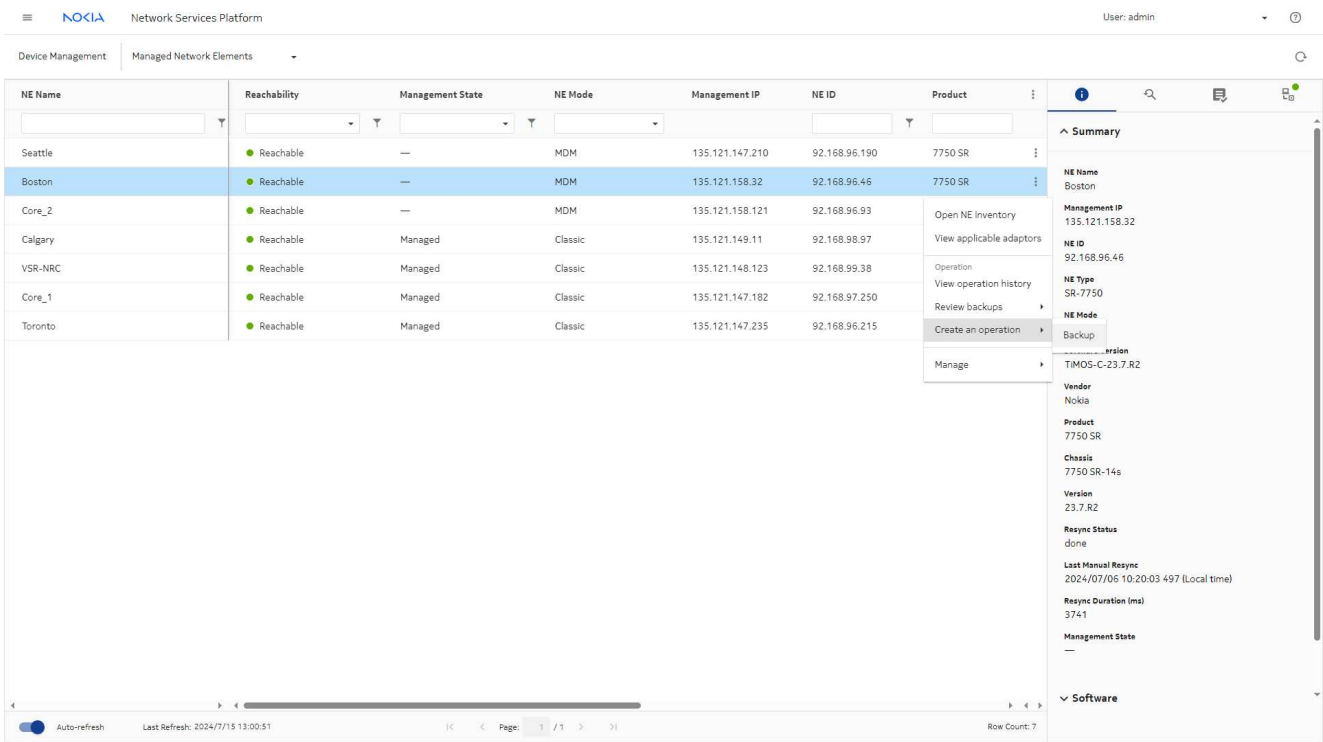


5.3.5 Back up the NE configuration

1

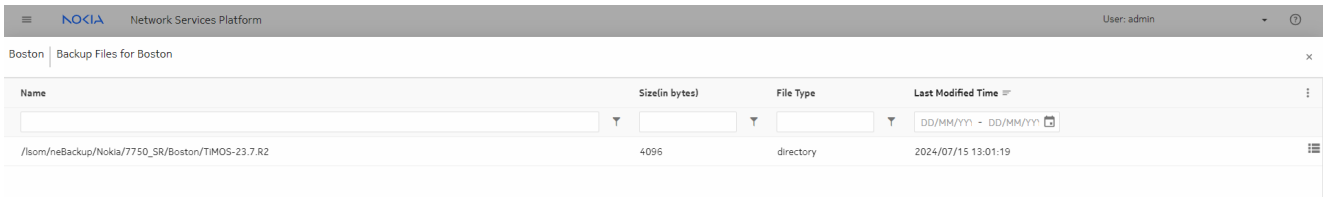
Returning to the Managed Network Elements list, we'll take a backup of the NE.

Select the NE and choose **Create an operation**, **Backup** from the table row actions menu (⋮).



2

We can check the status of the backup by clicking ⋮ (Table row actions), **Review backups**, **View all backup files** to view the list of completed backups.



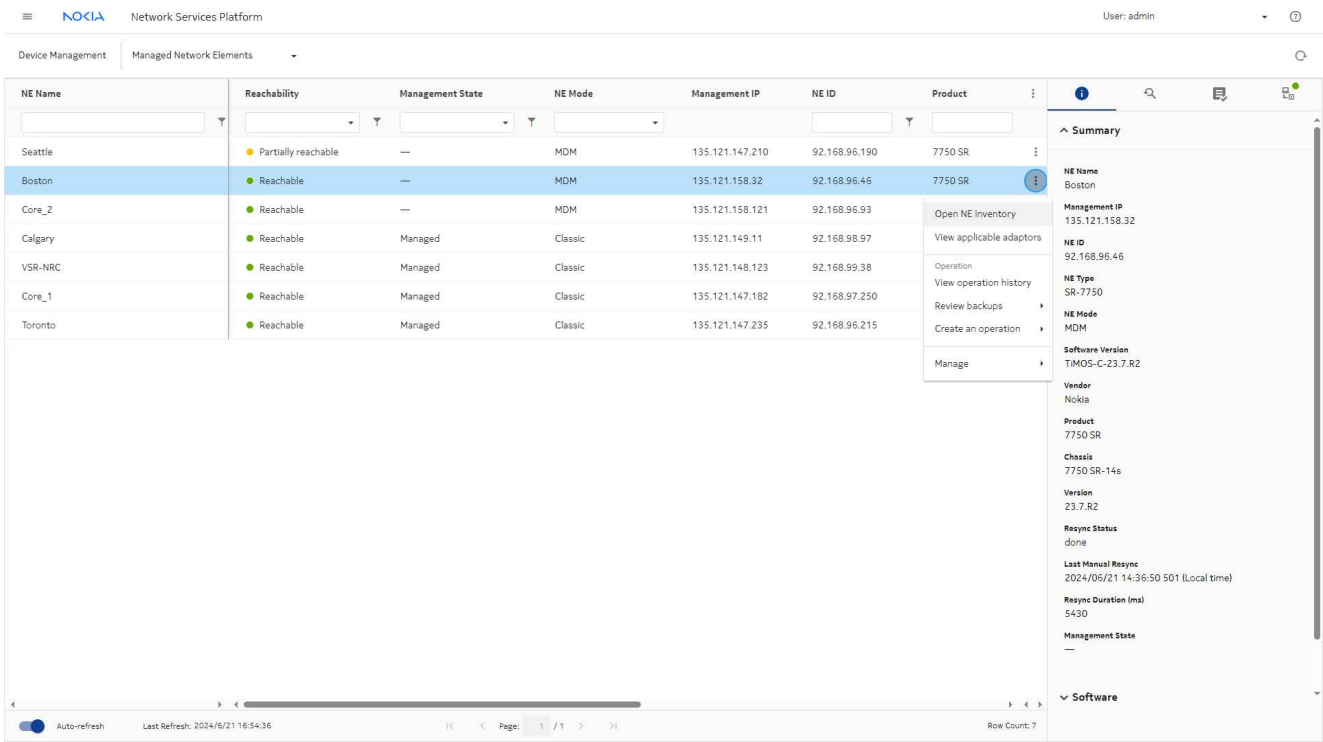
5.3.6 Verify the NE inventory post configuration

1

Return to the list of devices in **Device Management**, **Managed Network Elements**.

2

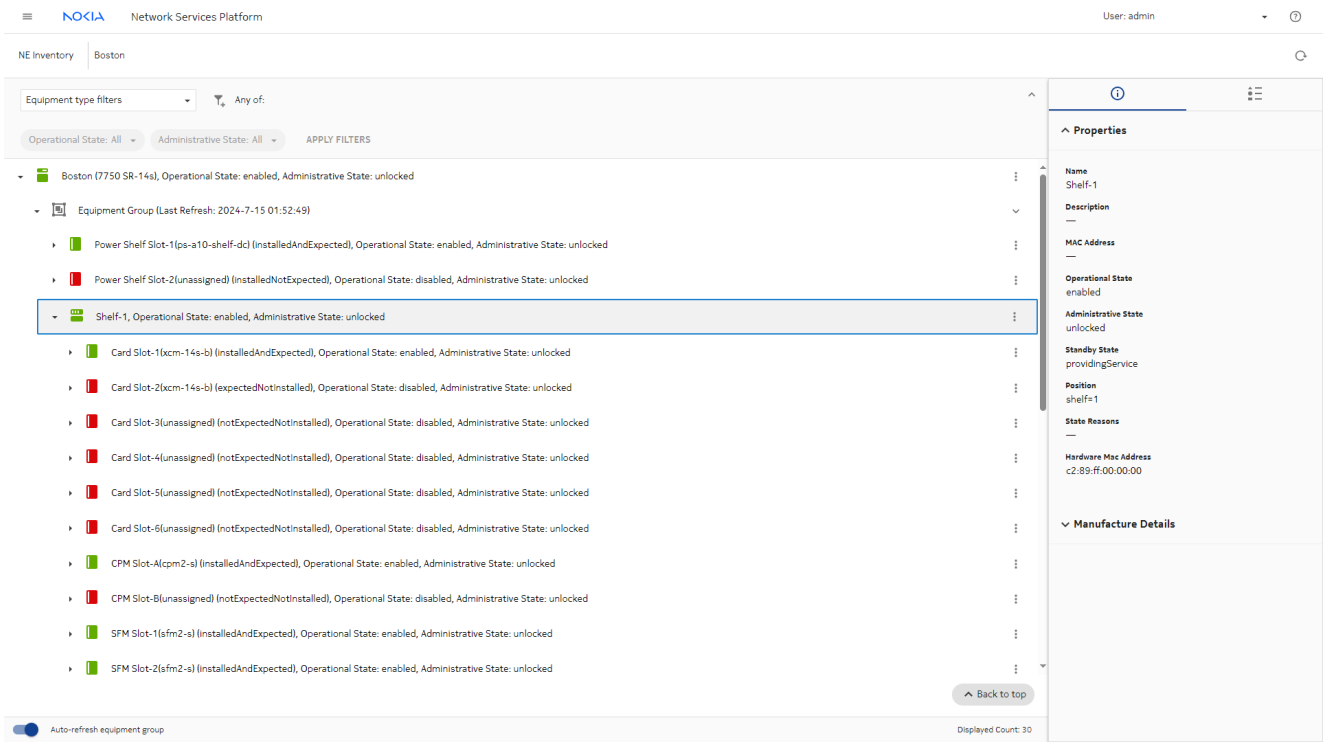
Select the NE and choose **Open in NE Inventory** from the table row actions menu (⋮).



3

The NE inventory tree view opens in a new browser tab, displaying the components that are configured.

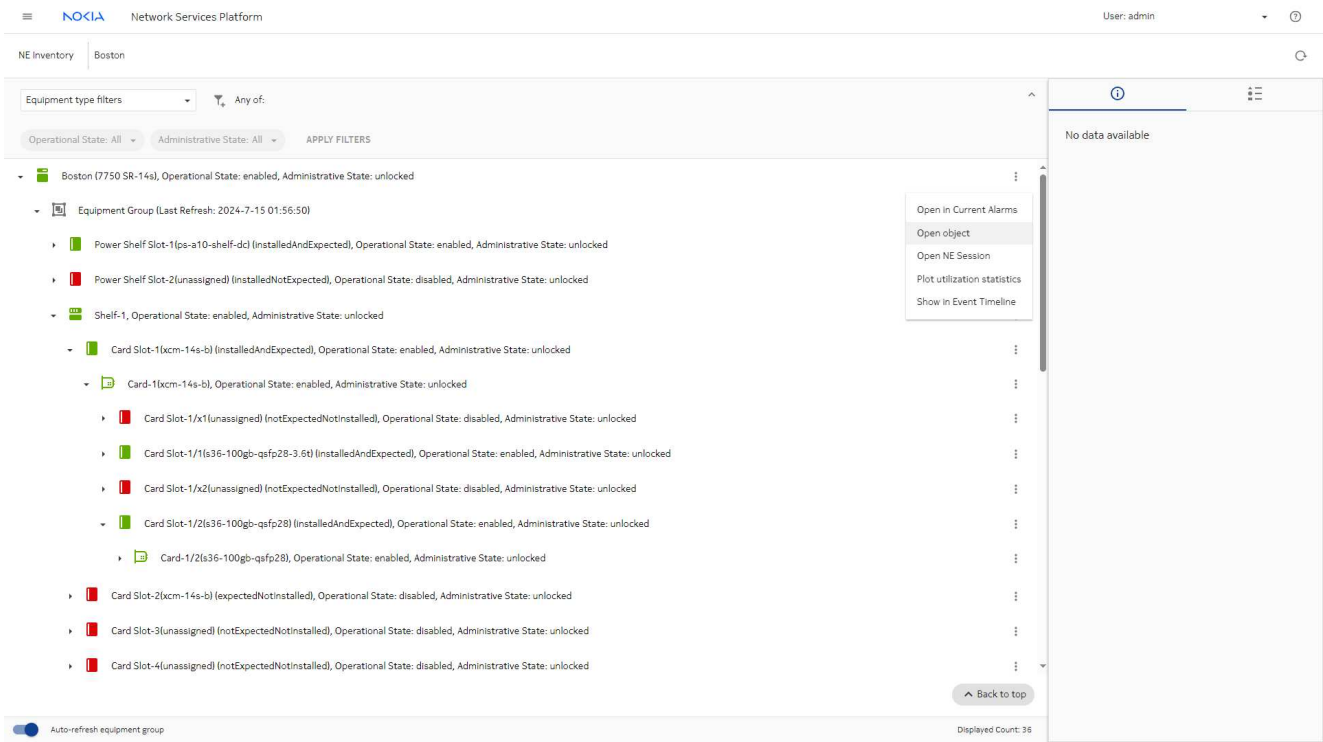
Expand the Equipment group to show the status of the shelves, slots, and cards.



4

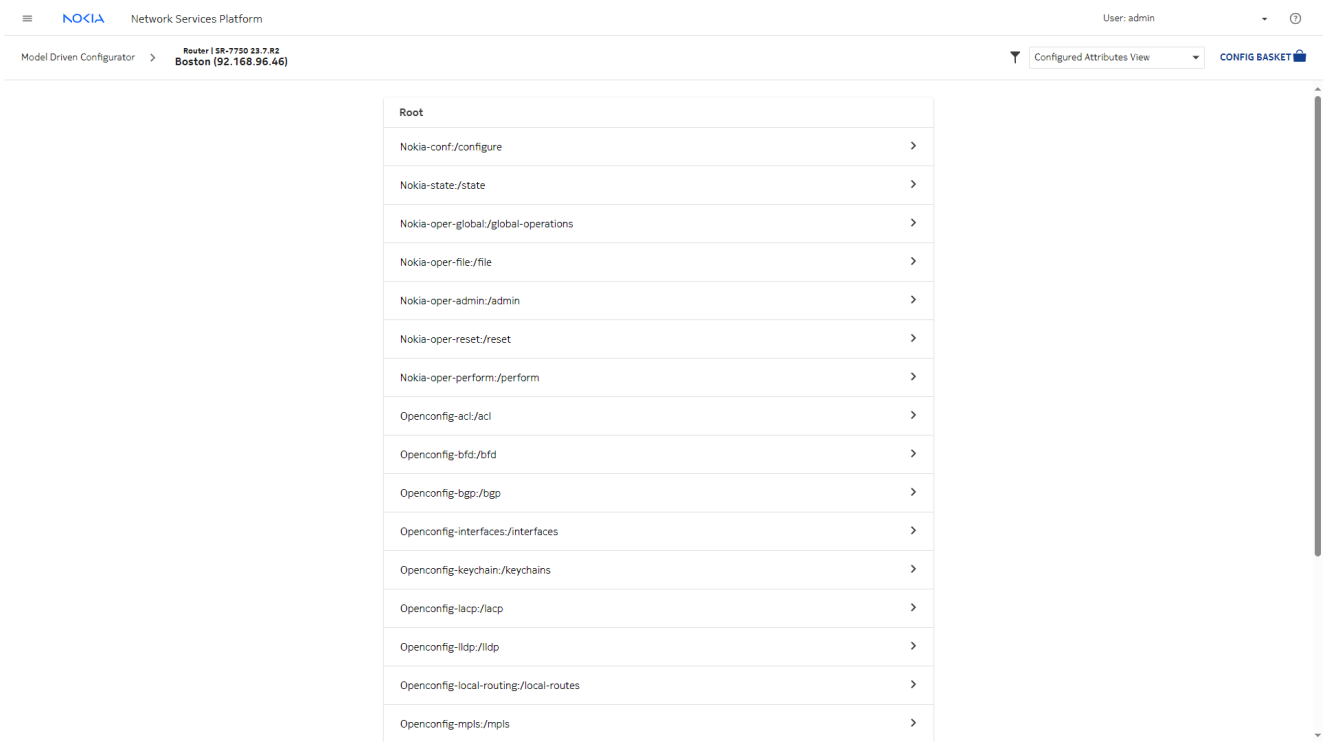
We can also verify configuration details in Modeled Device Configurator.

From the top of the inventory tree, select **Open object** from the More menu (⋮).

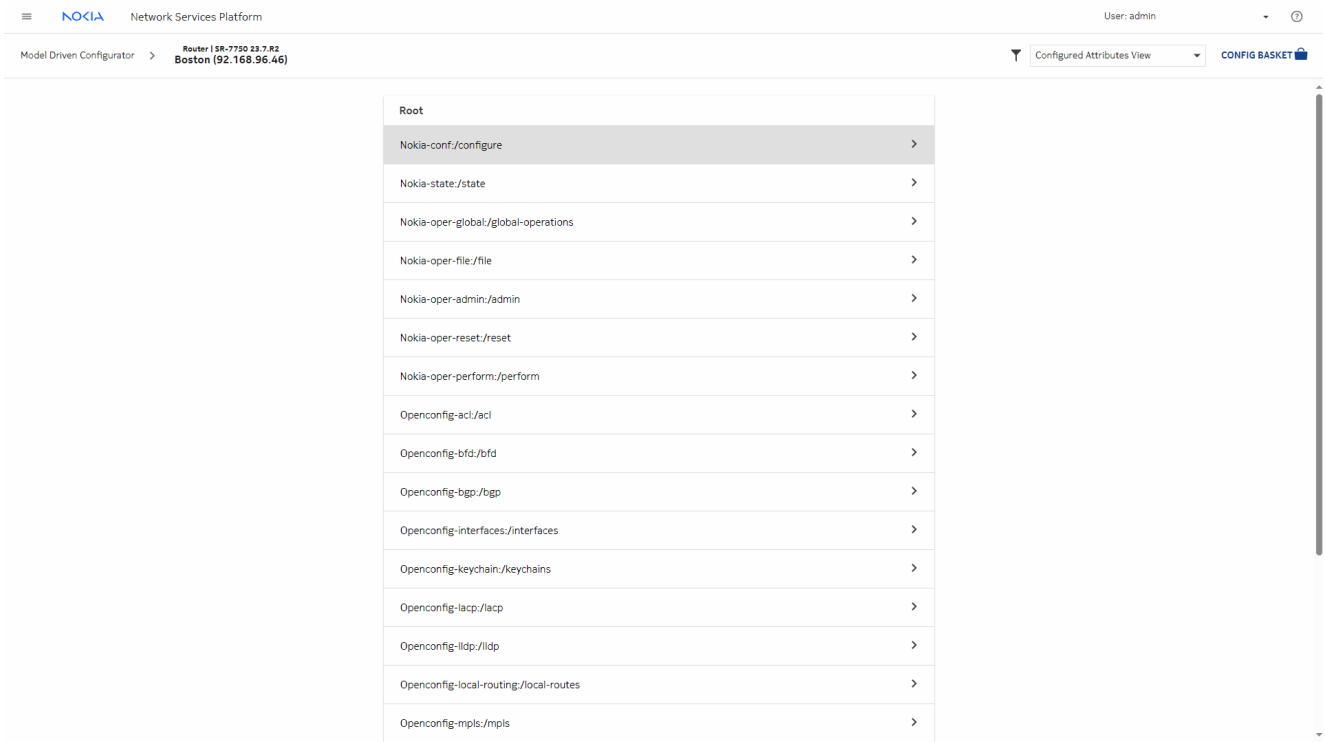


5

Modeled Device Configurator opens in a new tab, showing the configuration and state trees for the NE.



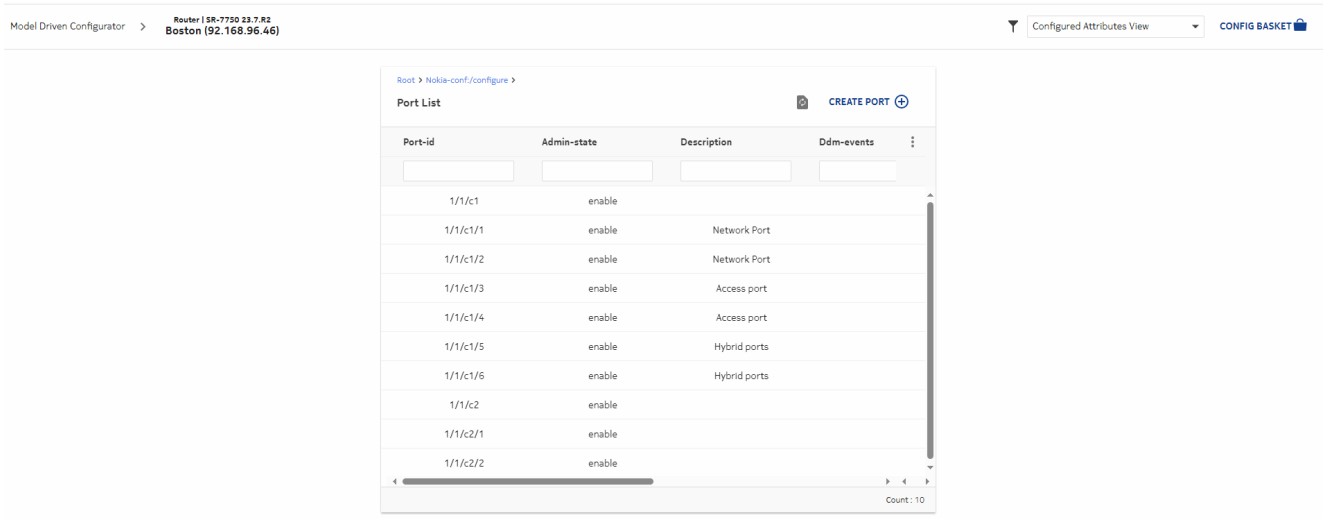
Click the **Nokia-conf:/configure** row to open the configuration tree.



6

Scroll down to see information about the objects we configured.

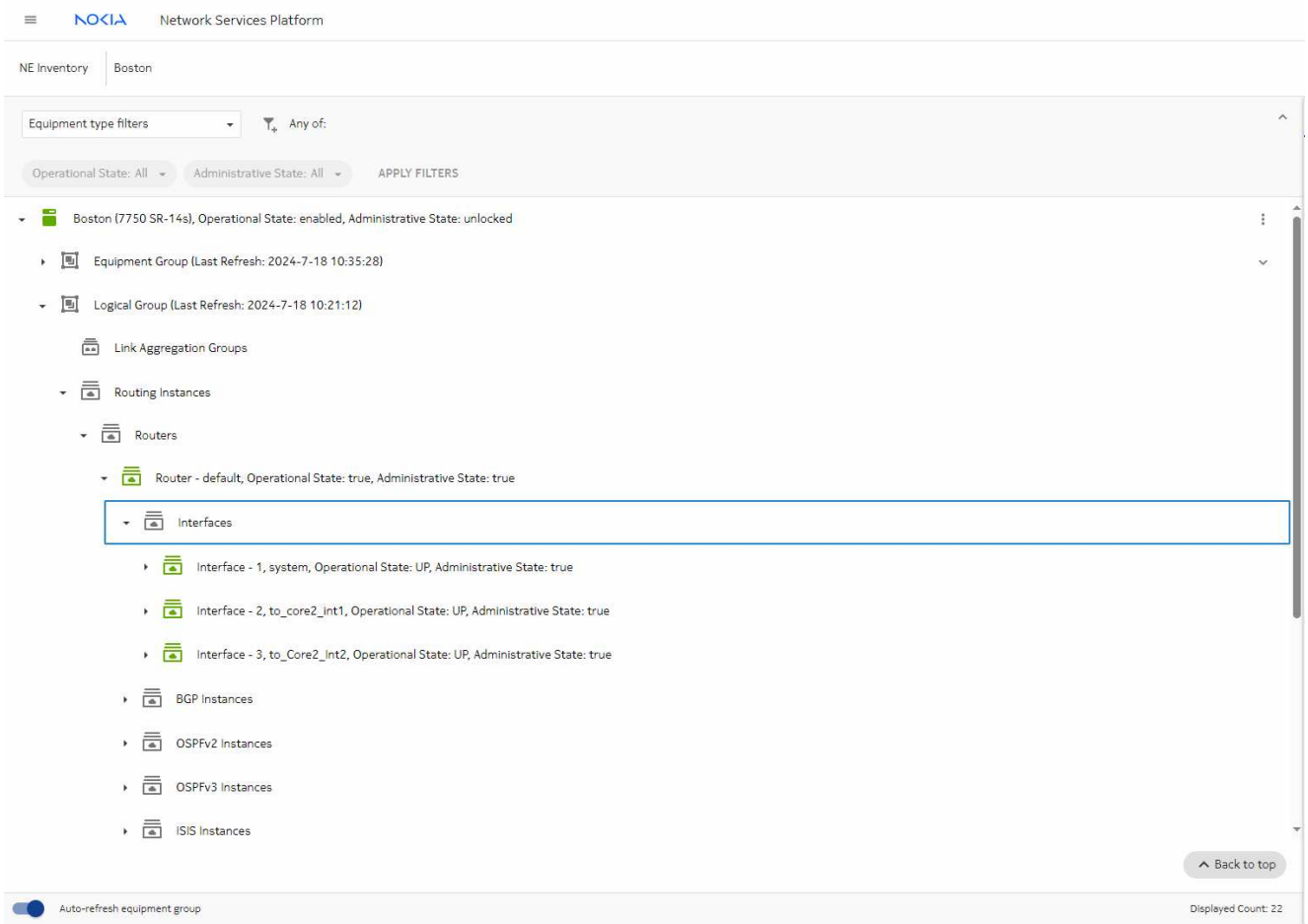
For example, we'll click Port List to see the configured ports.



7

We can also verify our logical configurations from the NE Inventory tab.

Return to the NE Inventory tab and expand the Logical Group. To see interfaces, expand, Routers and Interfaces. Green icons show normal operation.

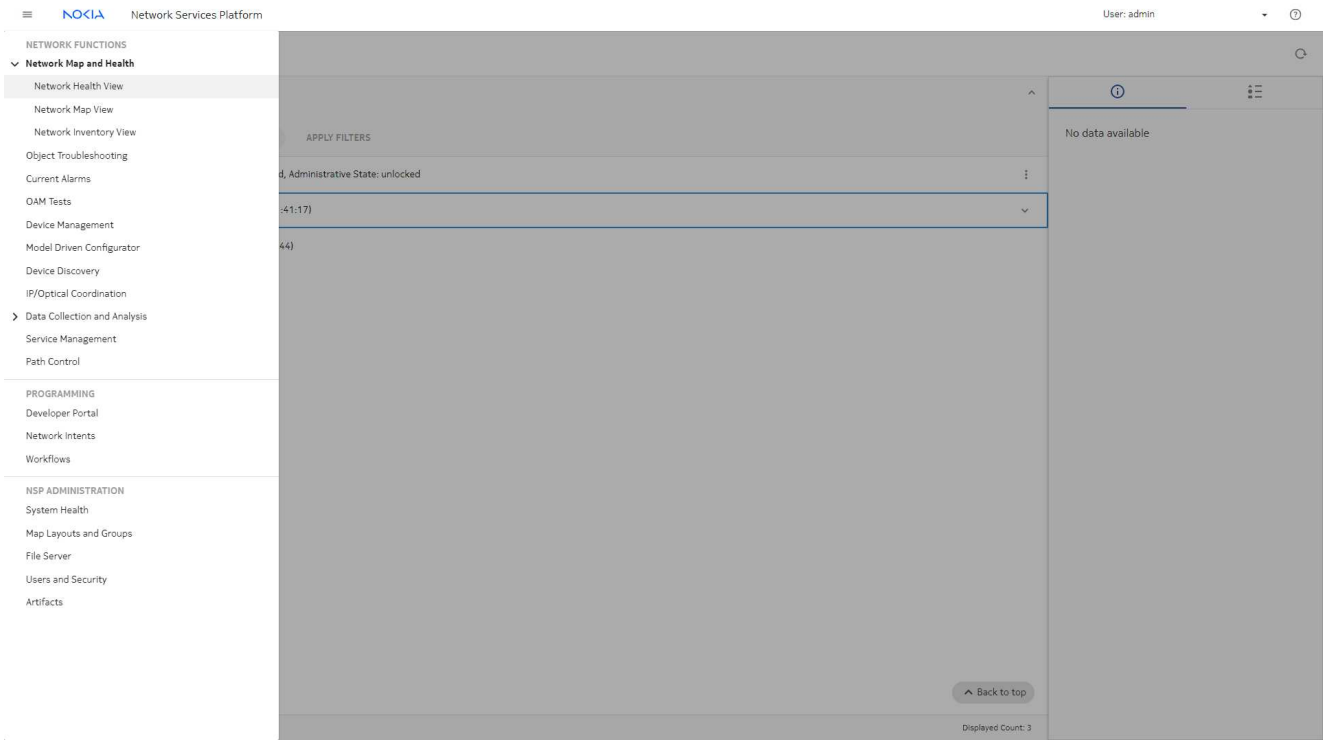


5.3.7 View the NE in the Network Health dashboard

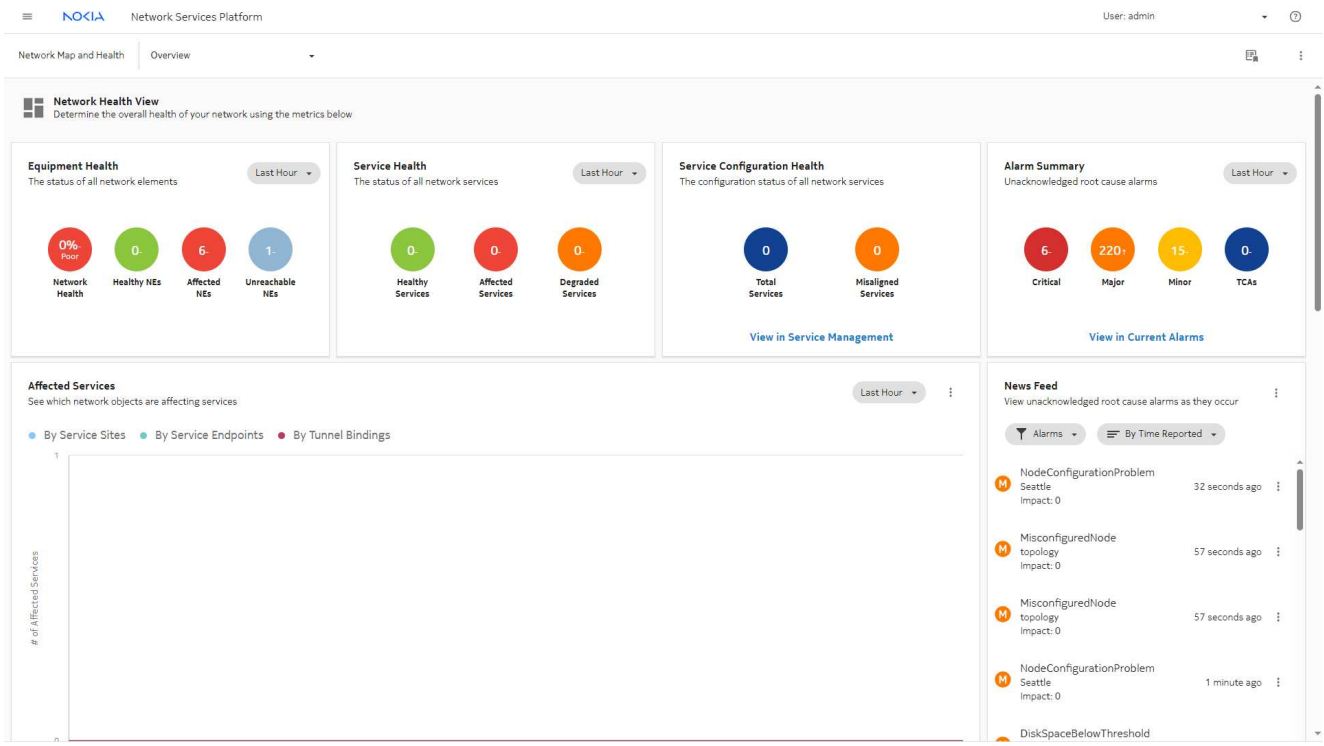
1

The Network Health dashboard is the home screen of the NSP. It provides a quick view of essential information relating to the function of your network and its components.

Choose **Network Health View** from the NSP main menu to open the dashboard.

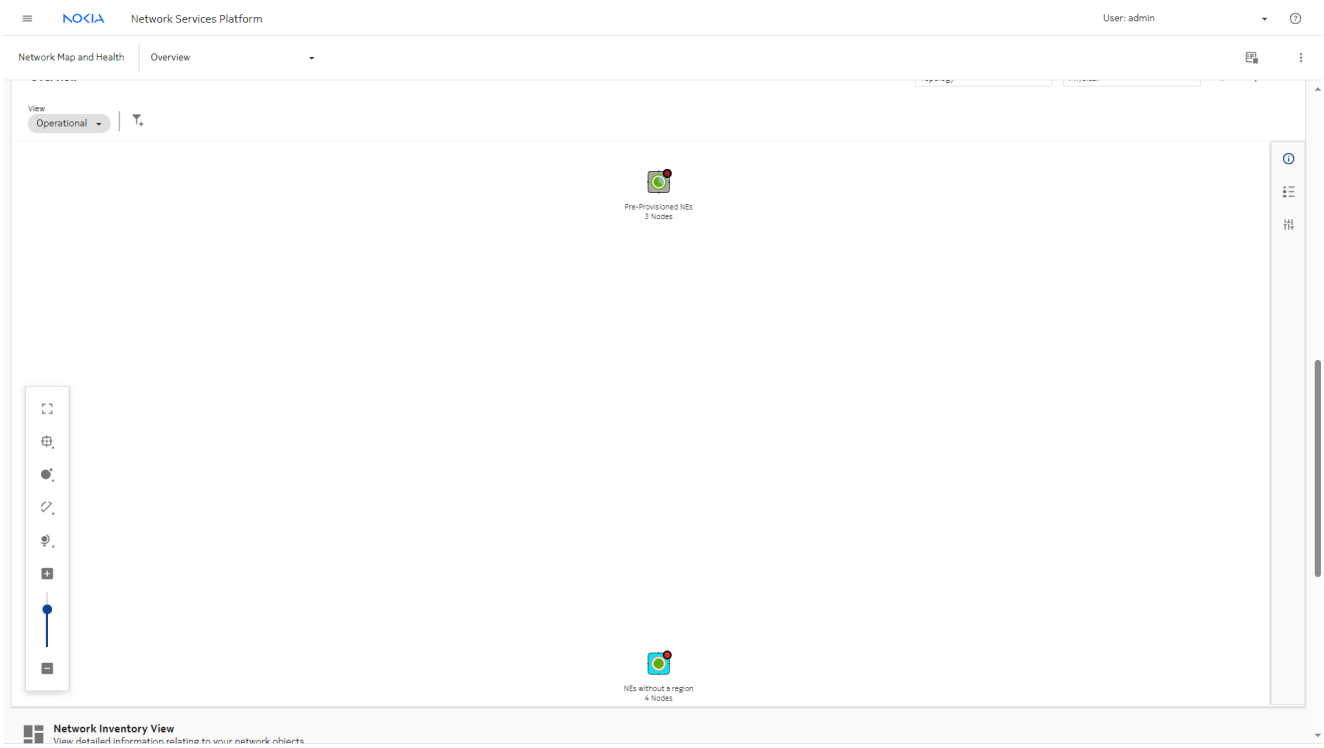


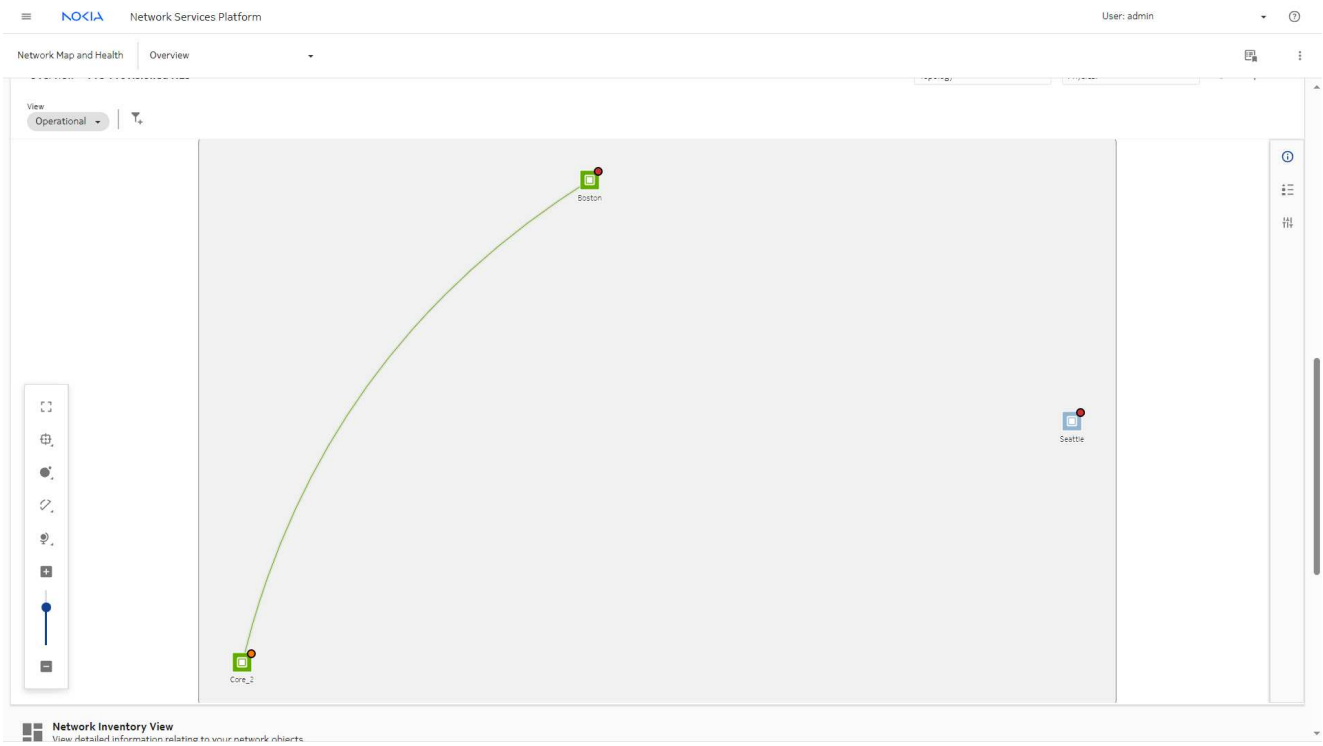
The Equipment Health dashlet shows that six affected NEs are present in the network.



2

Scroll down to see the Map View. Double-click on **Pre-Provisioned NEs** to show our NE, with the link that we created by configuring the router interface.

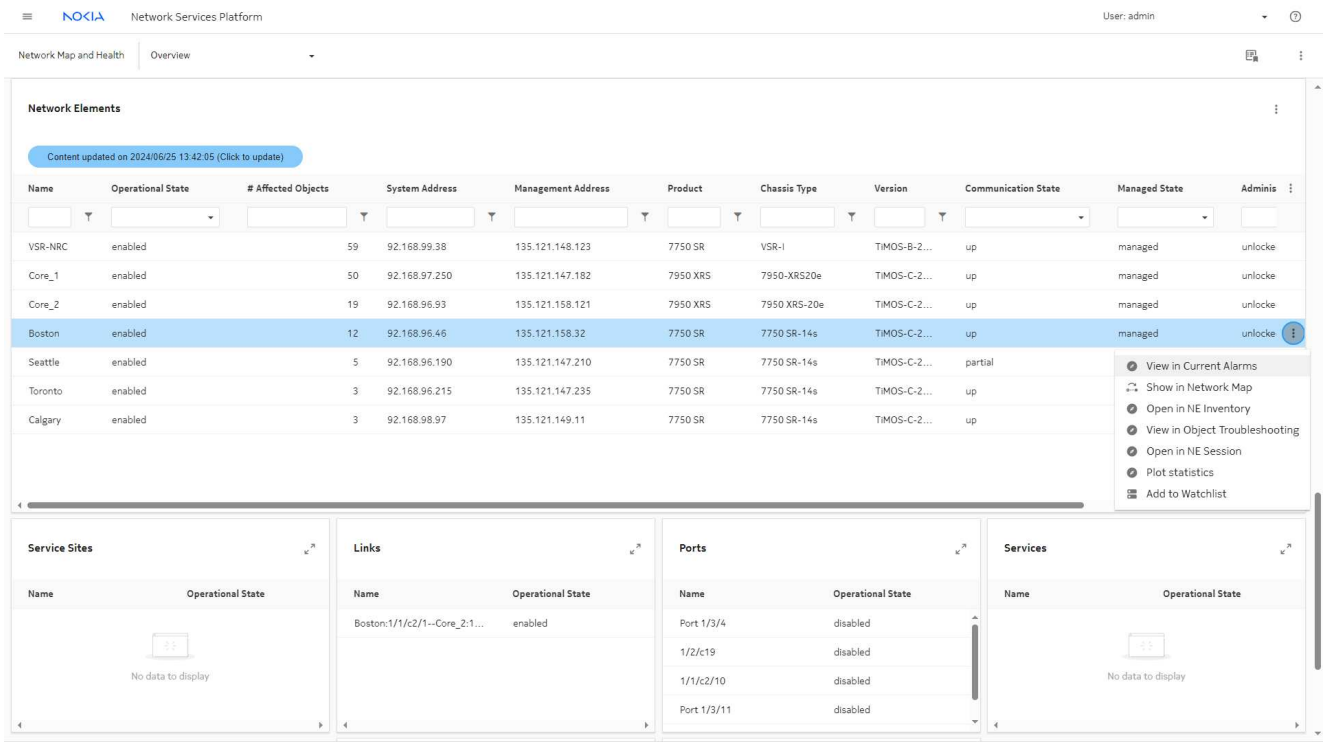




3

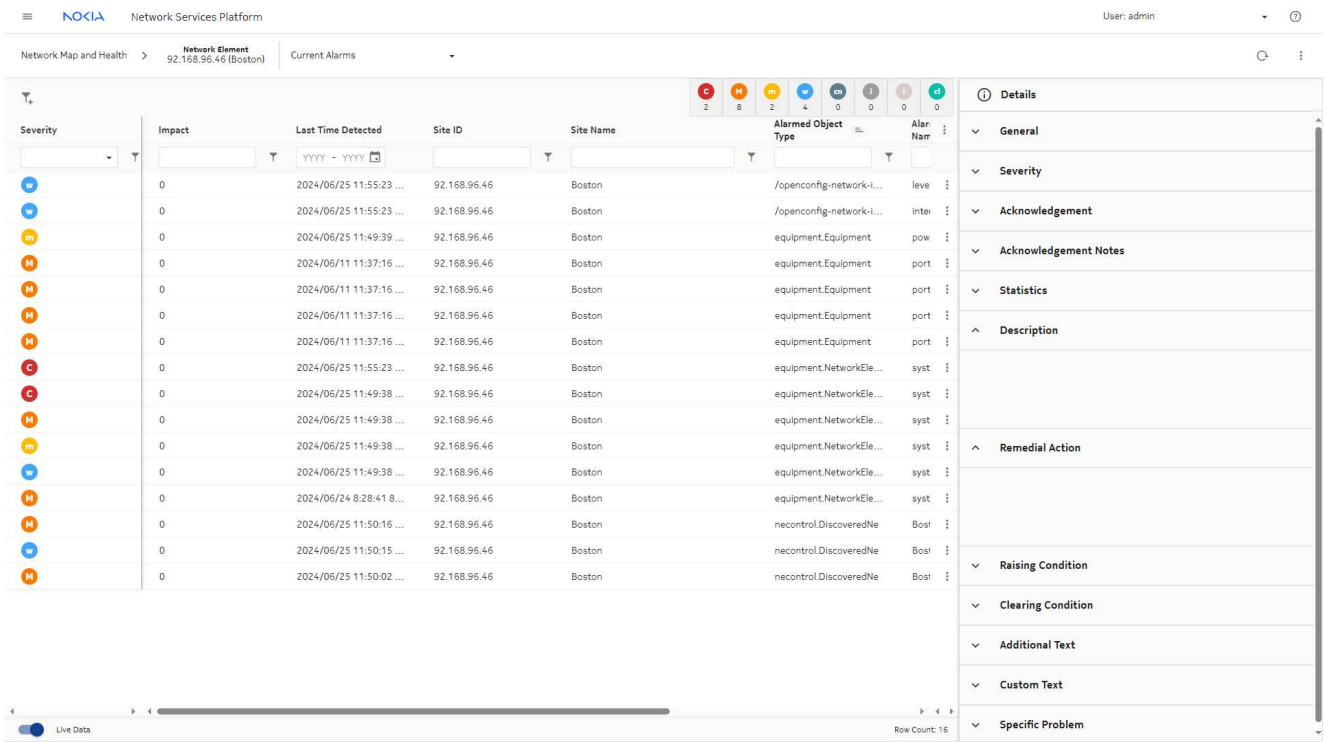
Scroll further down to see further information provided by the dashlets.

Expand the Network Elements dashlet to see the list of NEs. The Table row actions menu shows options. We'll choose **Open in Current Alarms**.



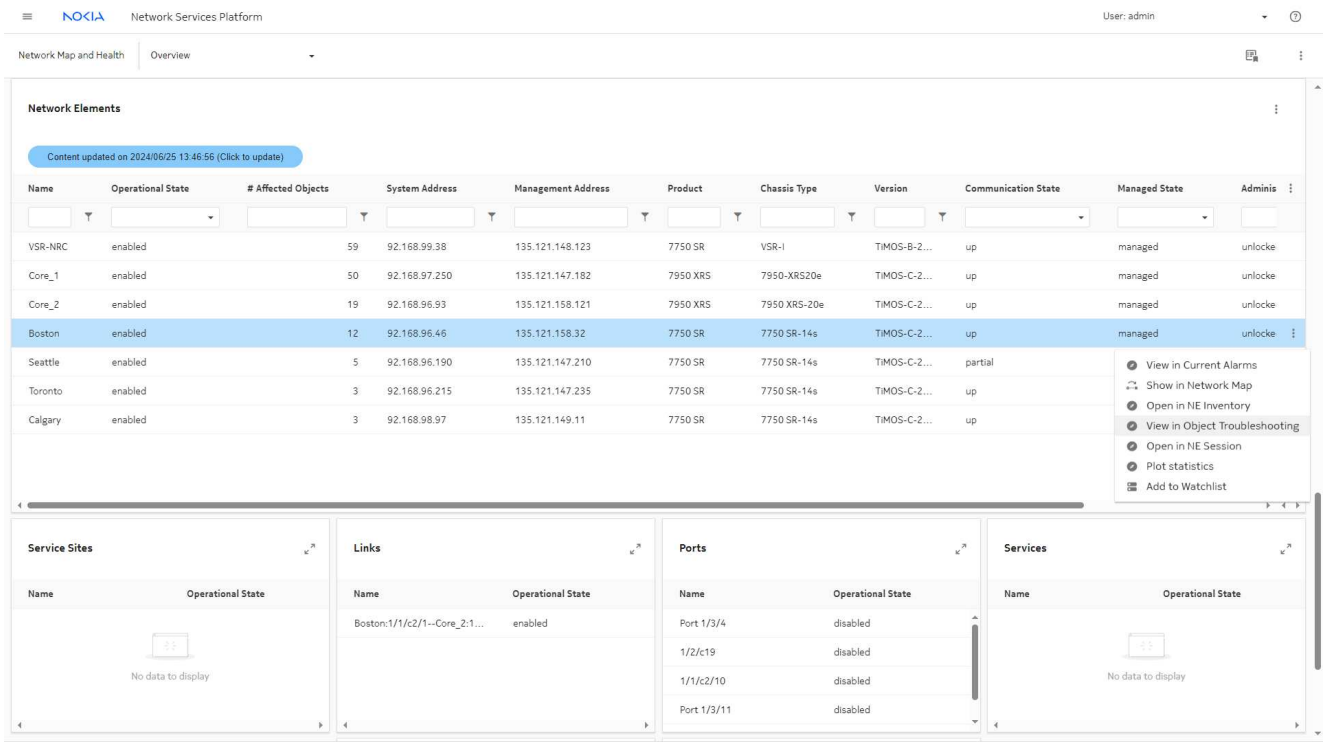
4

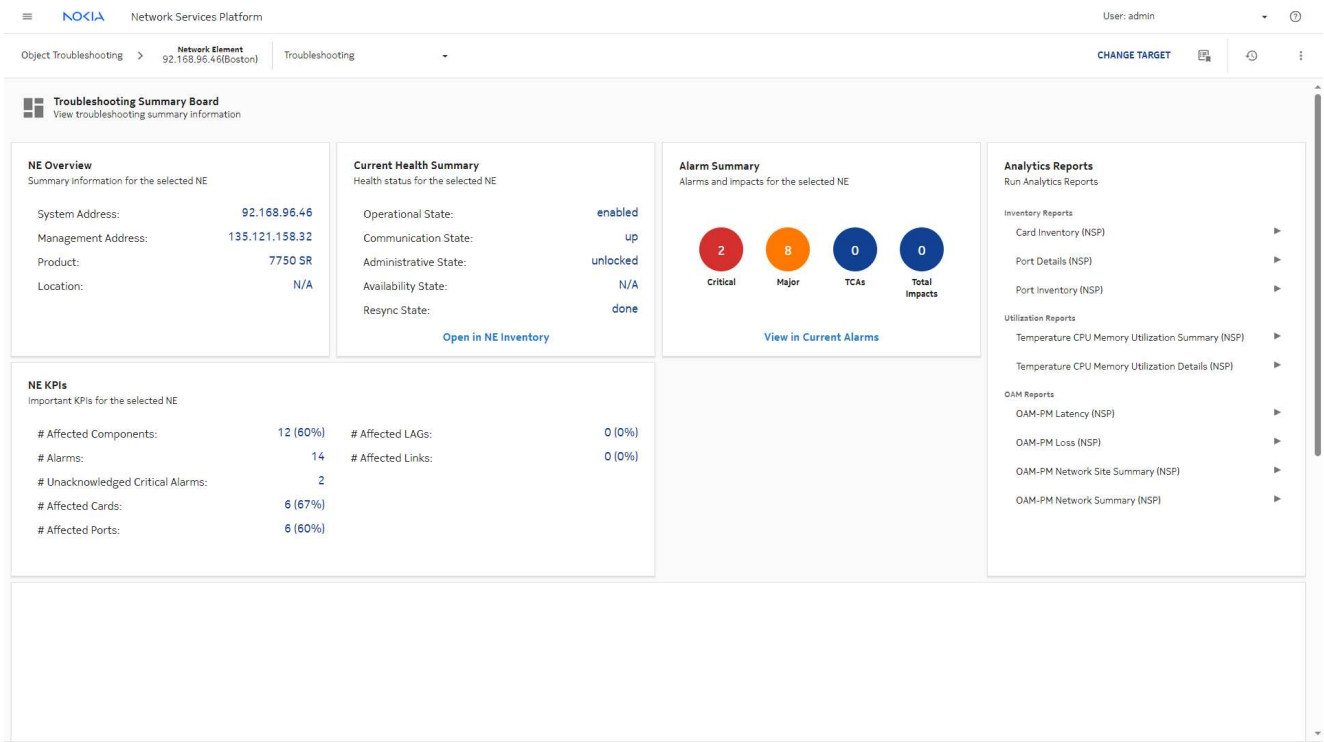
The Current Alarms view opens, filtered to show the alarms on the NE of interest. We can further filter the list if needed.



5

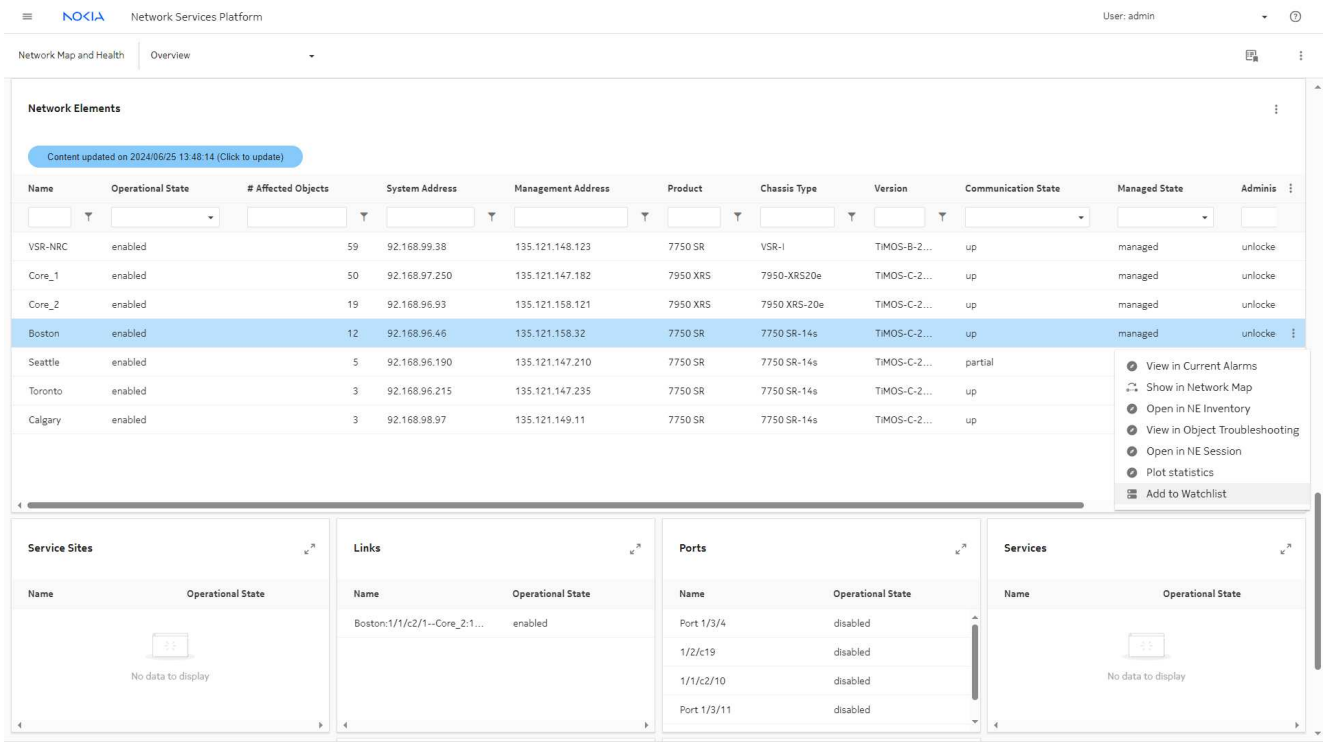
Returning to the Network Elements dashlet, we can also view the NE in the Object Troubleshooting dashboard. The Object Troubleshooting dashboard provides specific performance information about the selected NE.





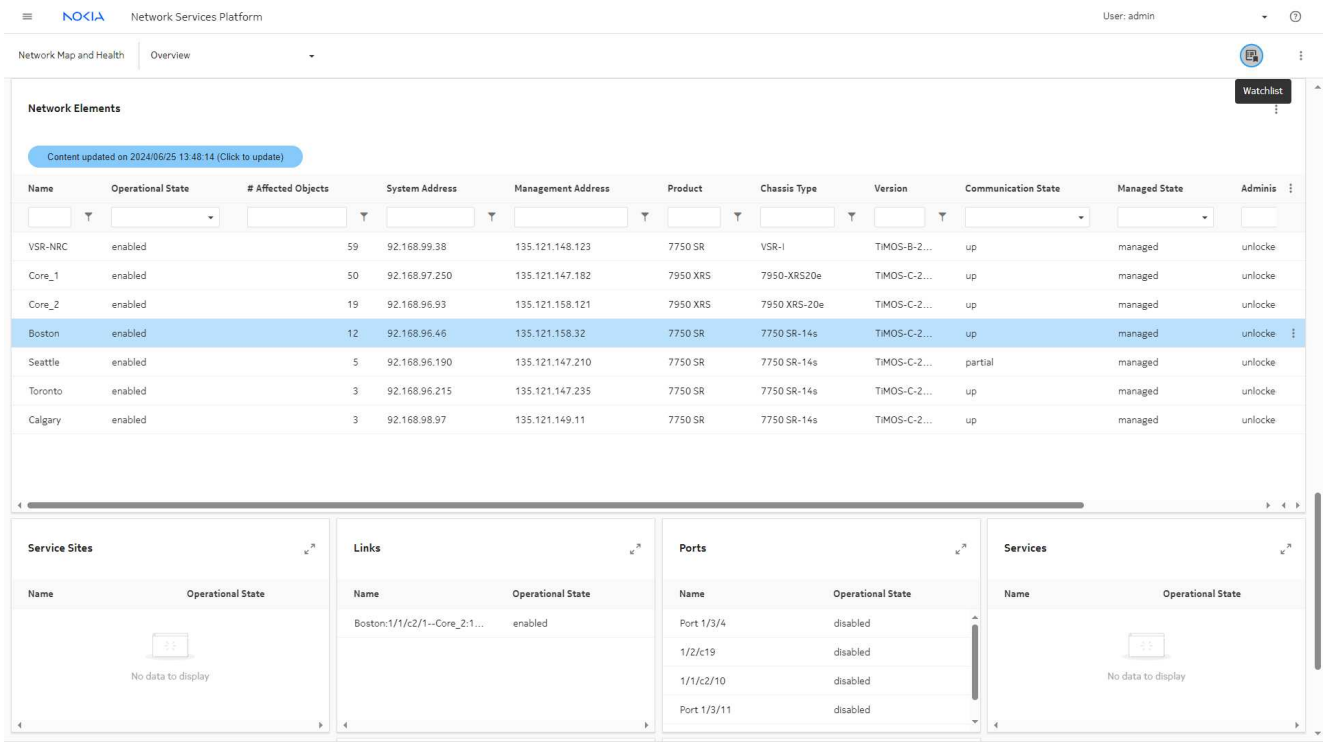
6

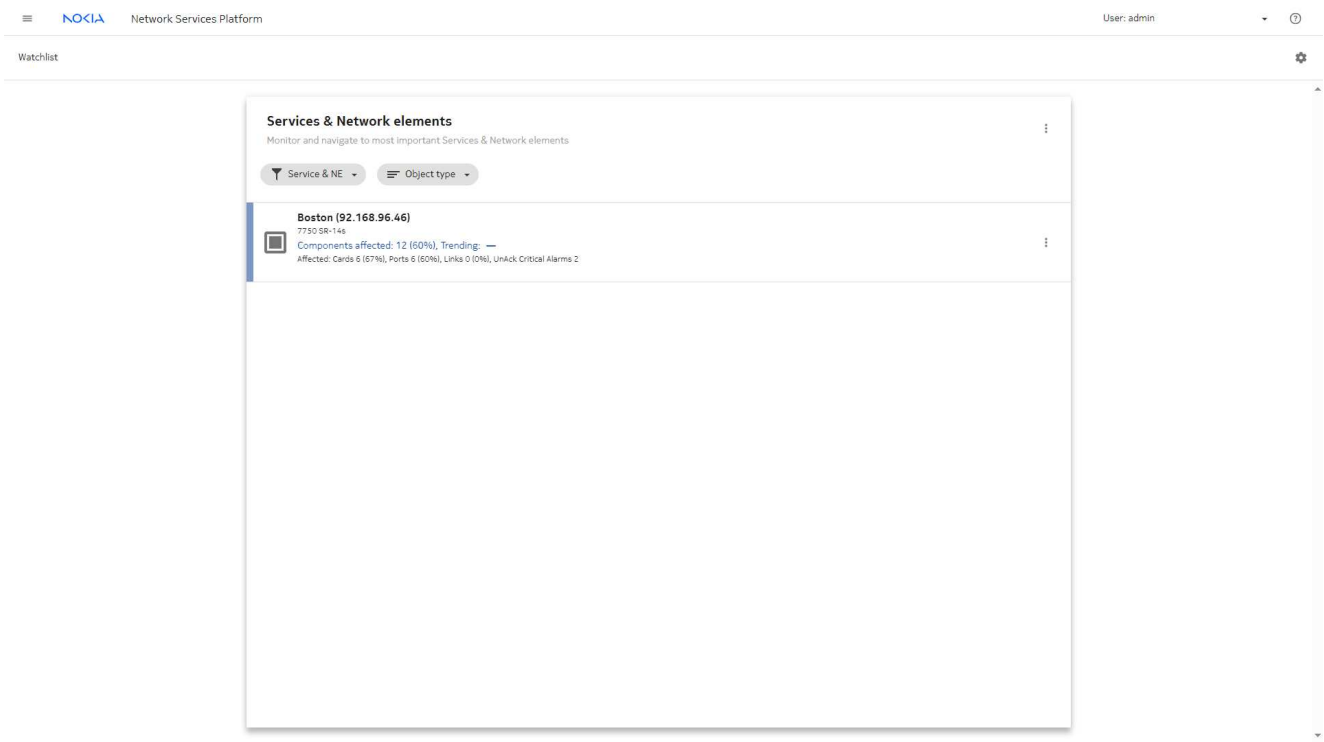
Returning again to the Network Elements dashlet, we can add the NE to the Watchlist to navigate to it easily in future. Choose Add to Watchlist from the Table row actions menu.



7

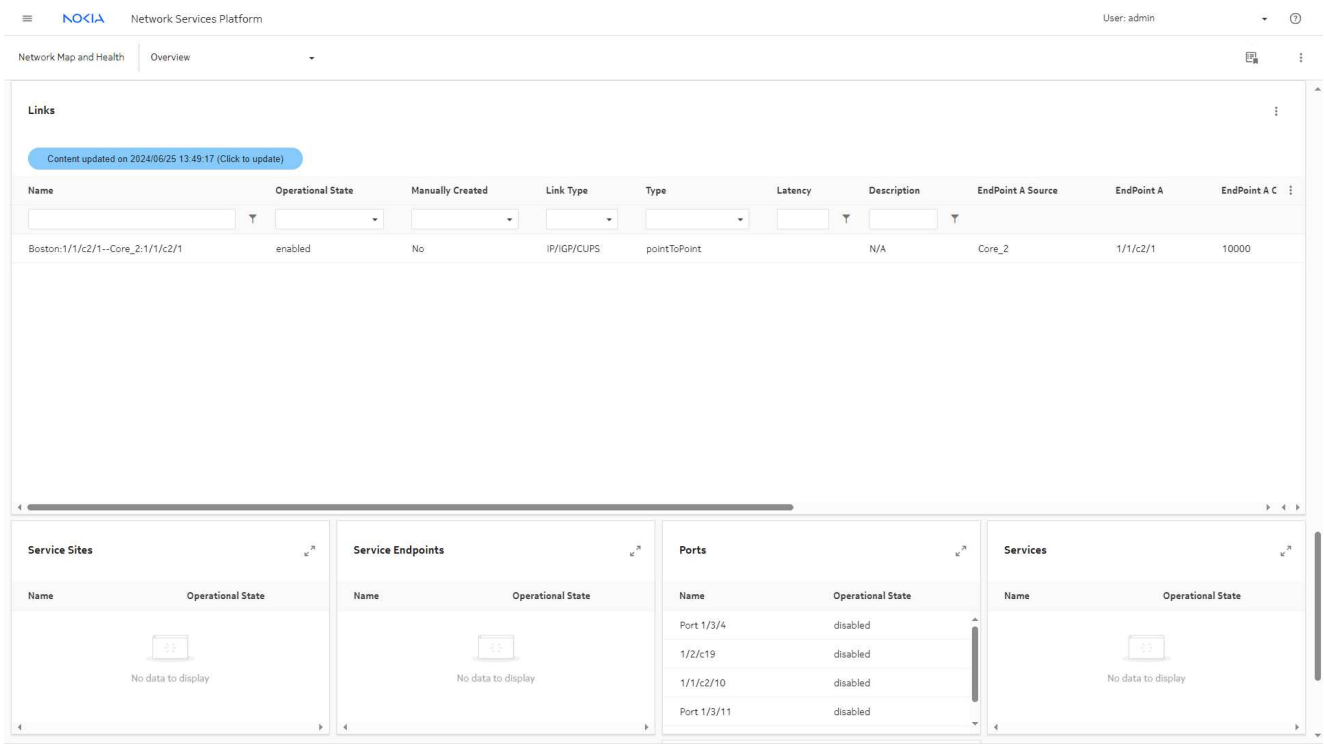
Click Watchlist at the top of the page to navigate to the watchlist.





8

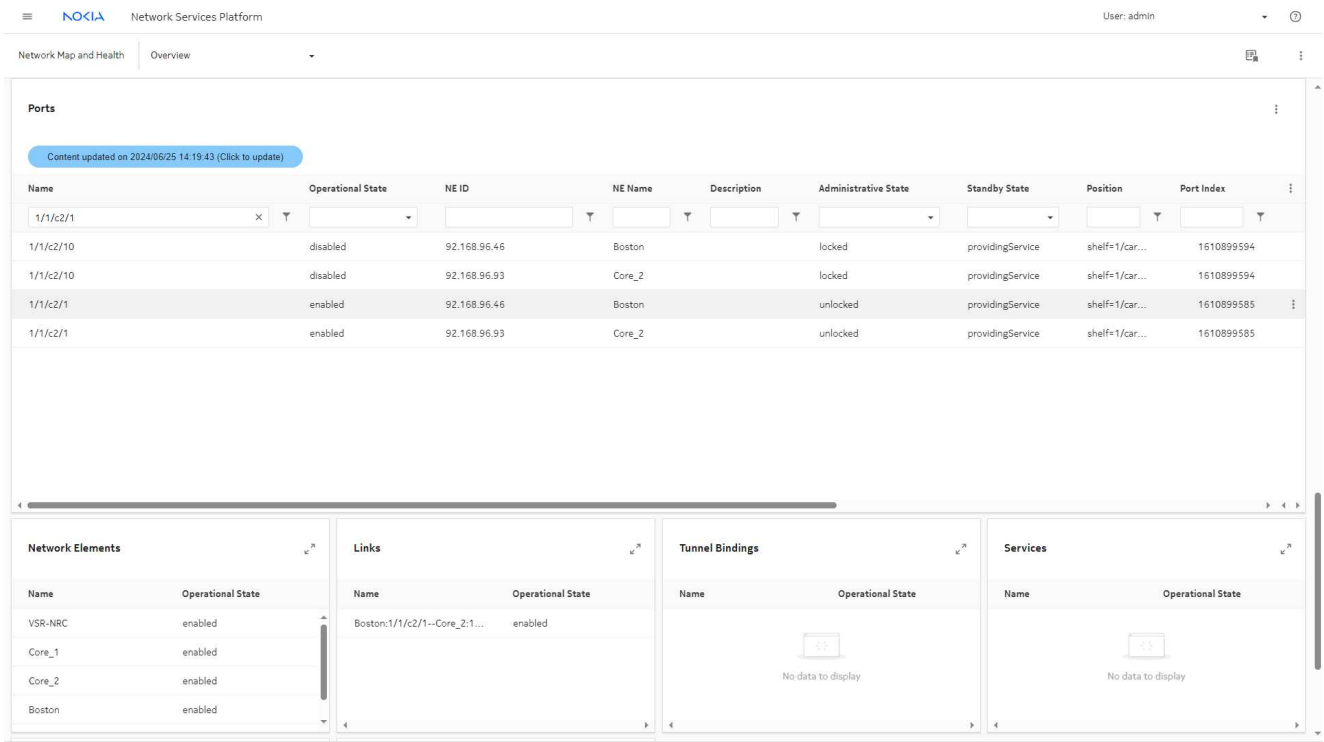
Let’s take a look at other information available on the Network Health dashboard. The Links dashlet shows a list of links configured on the system, showing their attributes.



9

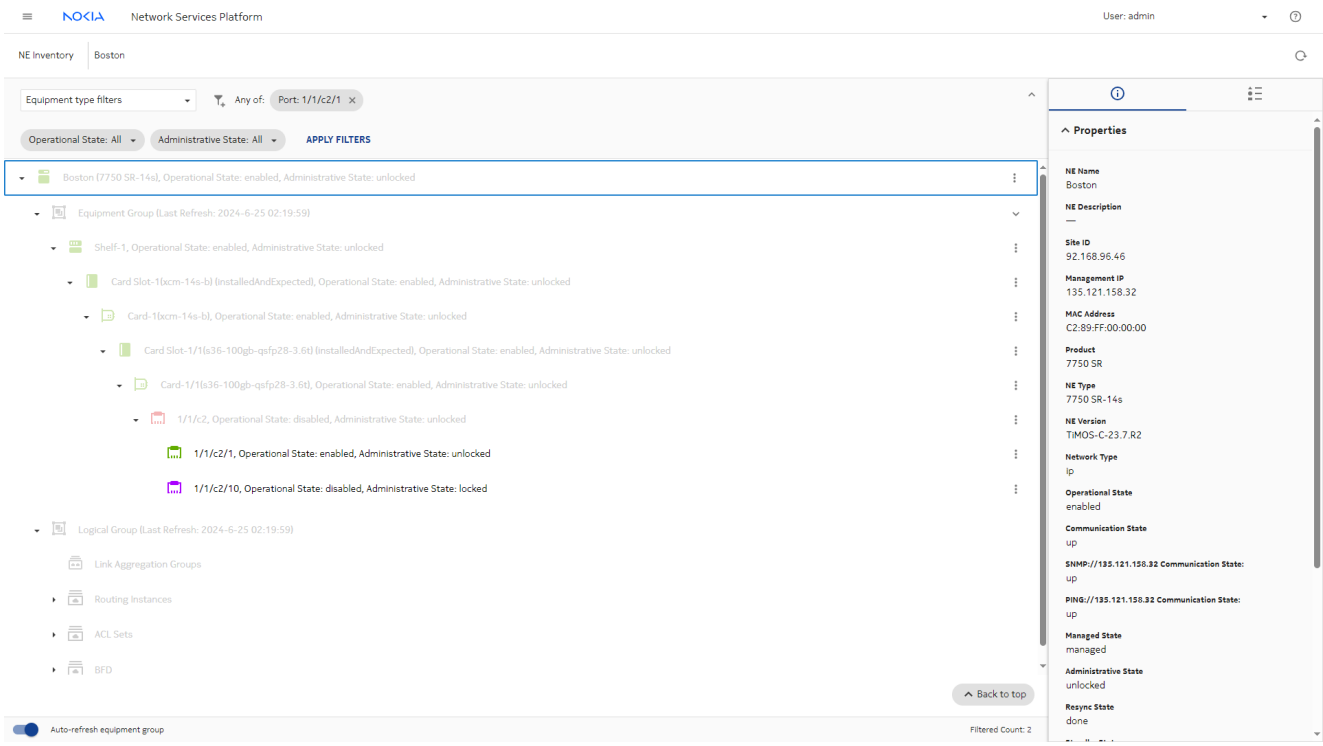
We can access more information from the Ports dashlet.

Expand the Ports dashlet and filter the list to show a port of interest.



10

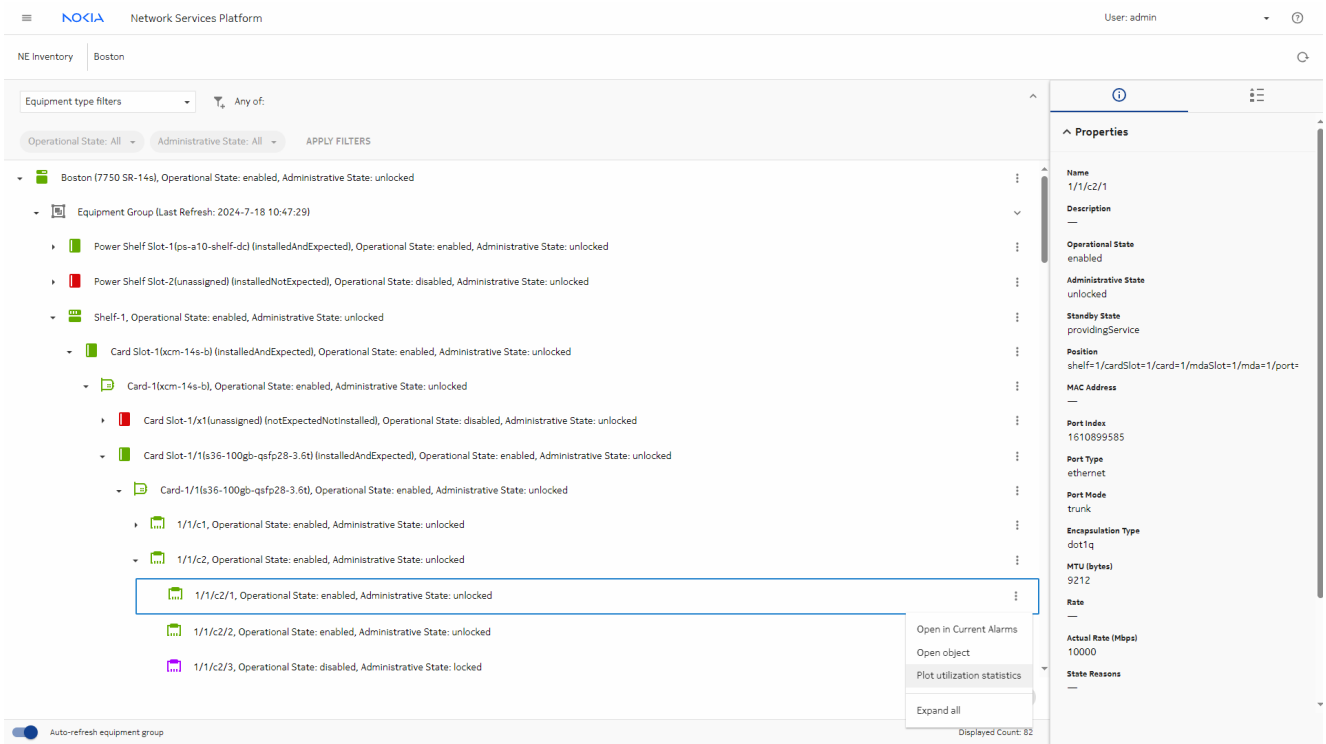
Select the port and choose **Open in NE Inventory** from the Table row actions menu (⋮). An NE Inventory view opens in a new tab, filtered to show the selected port.



11

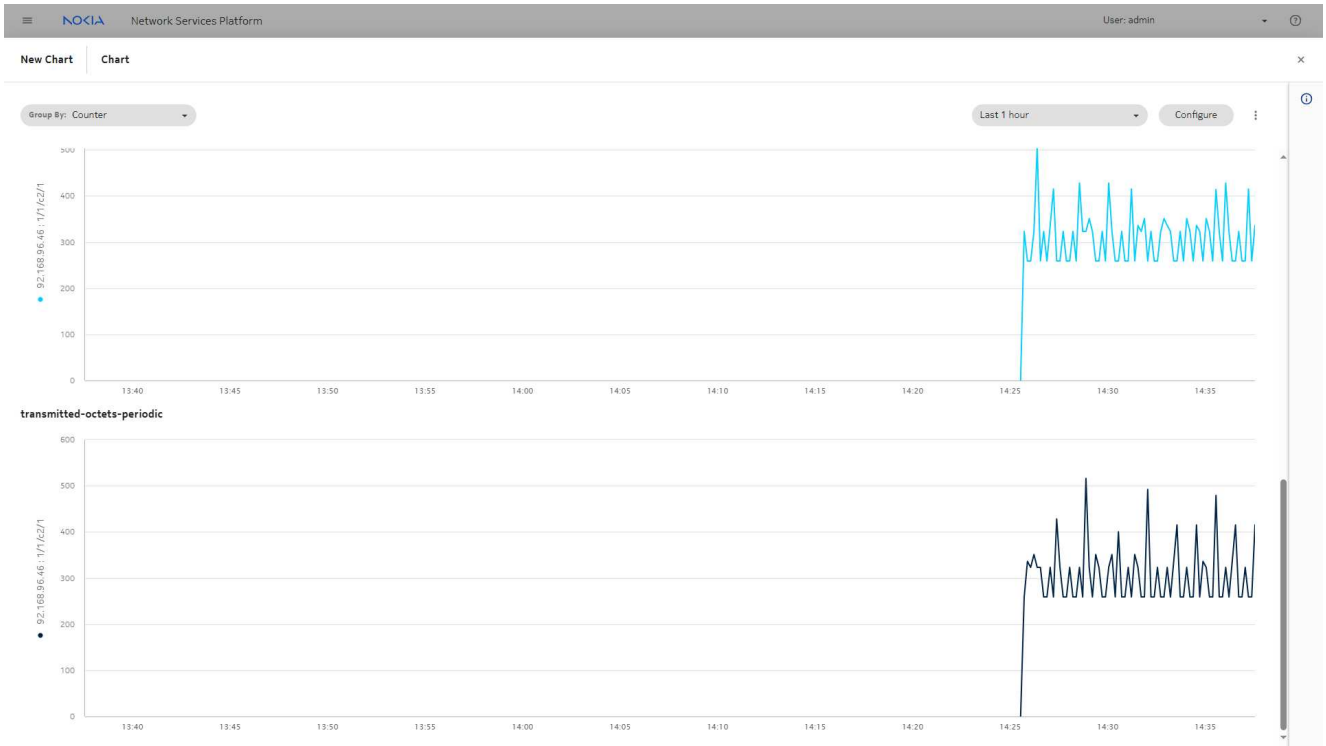
From the NE Inventory, we can plot utilization statistics for the port. This will show that traffic is flowing.

From the port level in the equipment tree, choose Plot utilization statistics from the More menu (⋮).



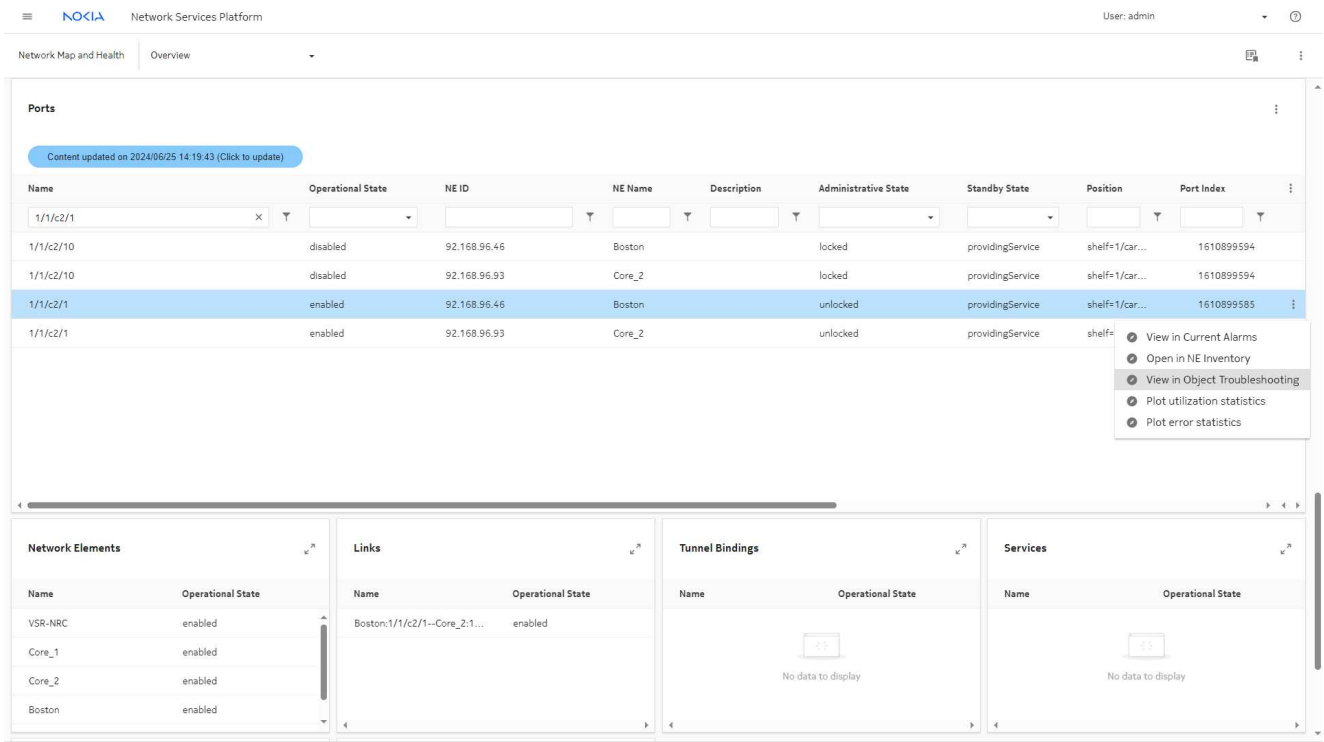
12

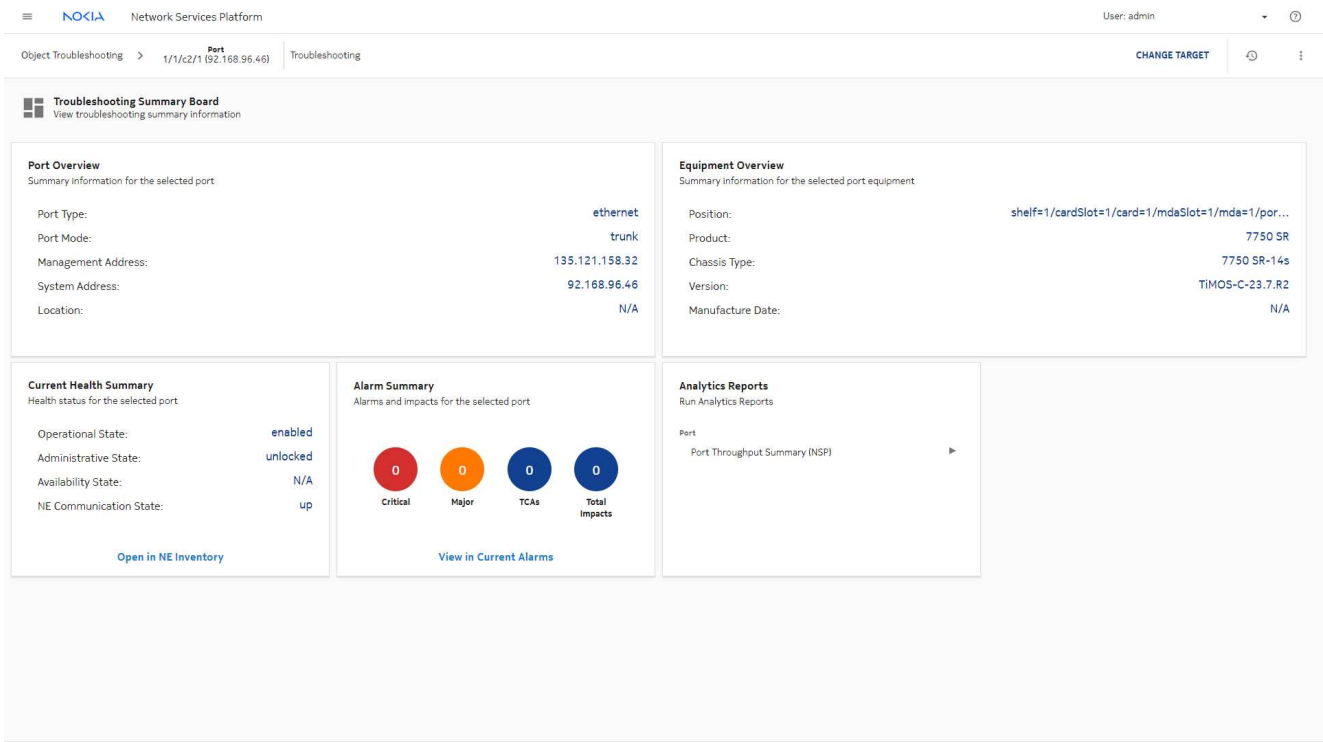
The Data Collection and Analysis Visualizations view opens in a new tab, showing a plot of utilization statistics for the port.



13

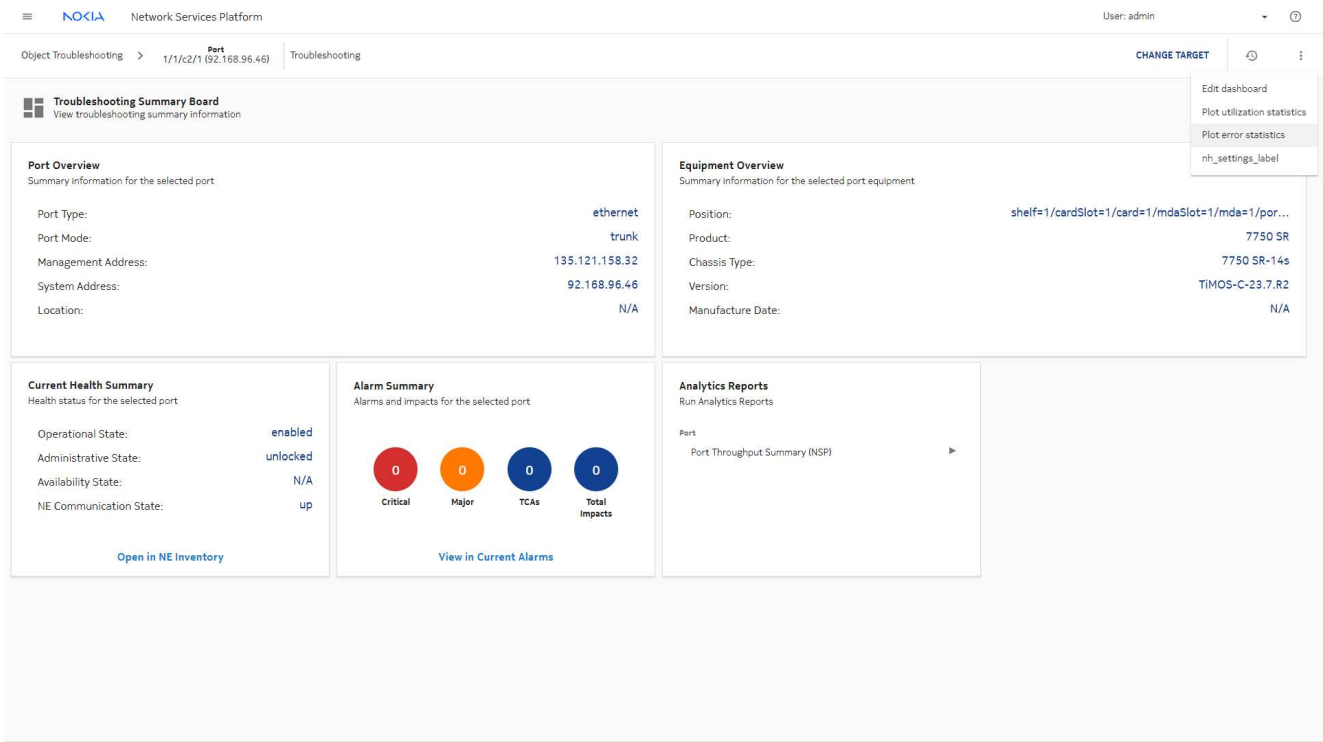
We can close the chart and inventory tabs, and return to the Ports dashlet. Select Open in Object Troubleshooting to see a summary of configuration and health information for the port.



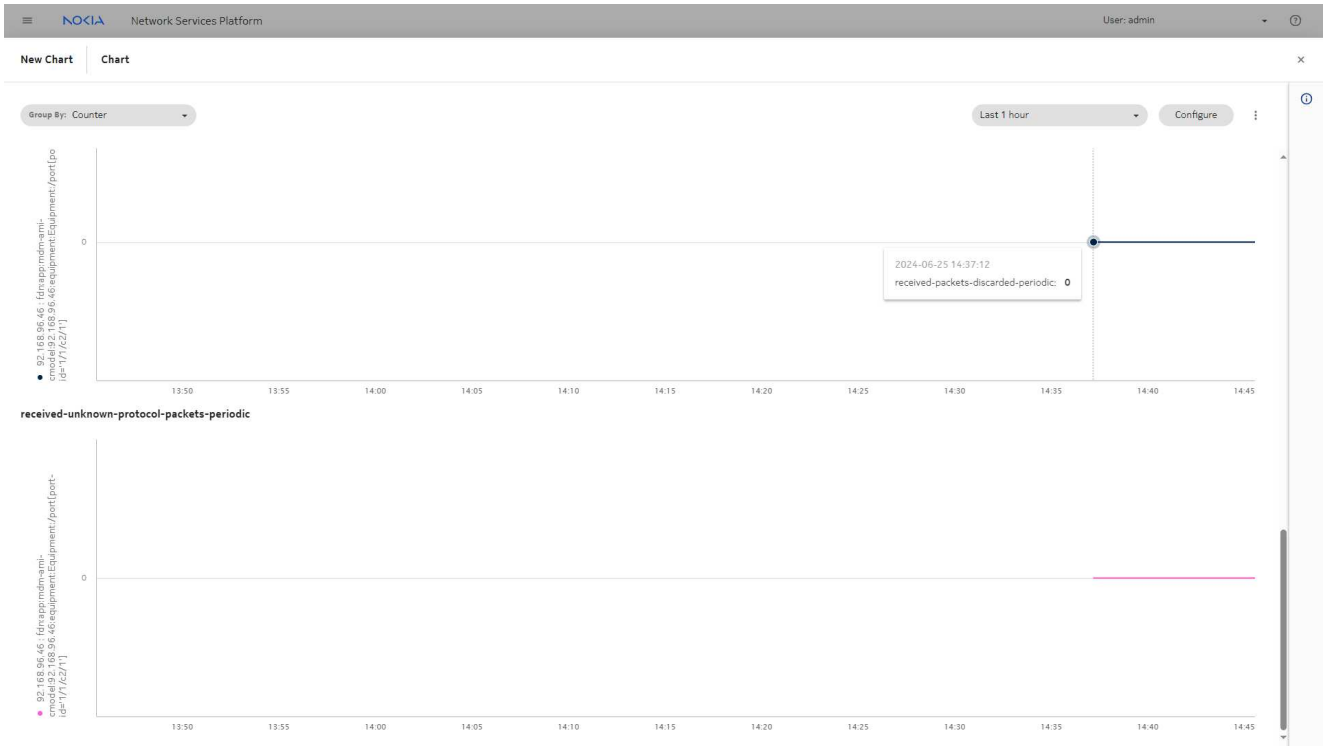


14

From here, we can plot error statistics to see if problems are occurring on the port.



The plot shows no errors.

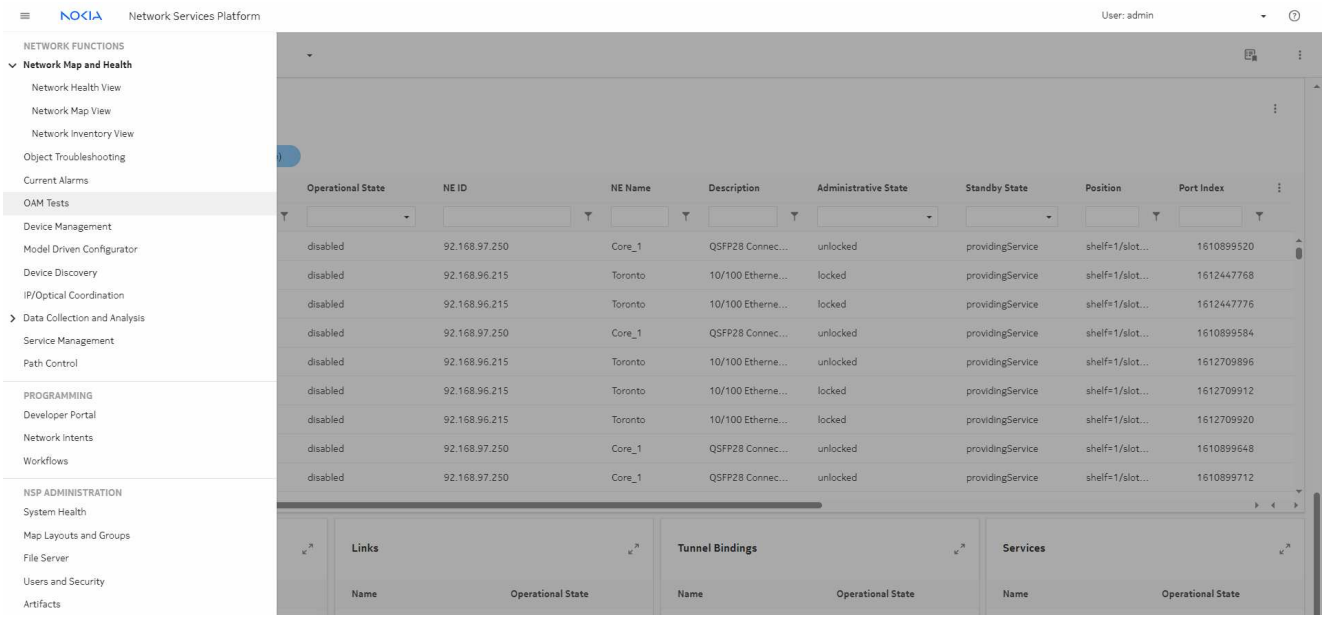


5.3.8 Perform OAM tests

1

Performing OAM tests will provide another way to confirm connectivity of the NE.

Click OAM Tests from the NSP main menu.

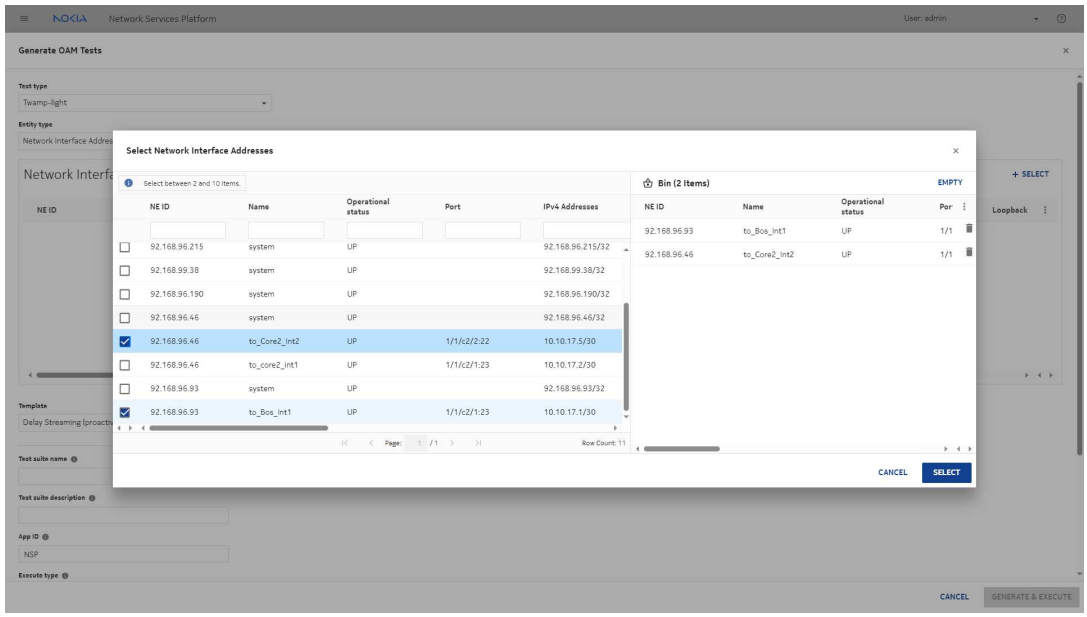


2

We'll create TWAMP Light tests for the interfaces we created:

1. In the **Data Collection and Analysis Management**, **Test Suites** view, click **+ SUITE**.
2. In the form that opens, select Twamp-light from the **Test type** drop-down.
3. Select Network Interface Address in the **Entity type** drop-down.
4. In the form that opens, select the interfaces we configured earlier in this process, and click

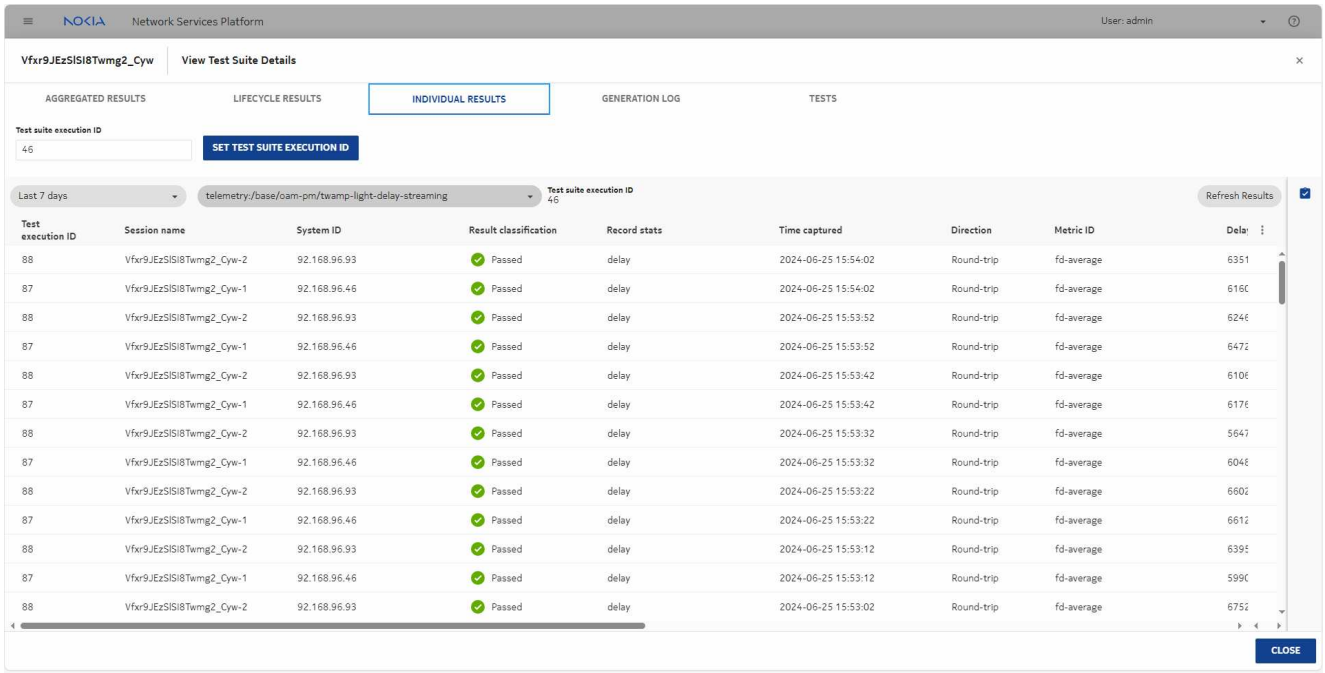
SELECT.



5. Click **GENERATE & EXECUTE** to run the tests immediately.

3

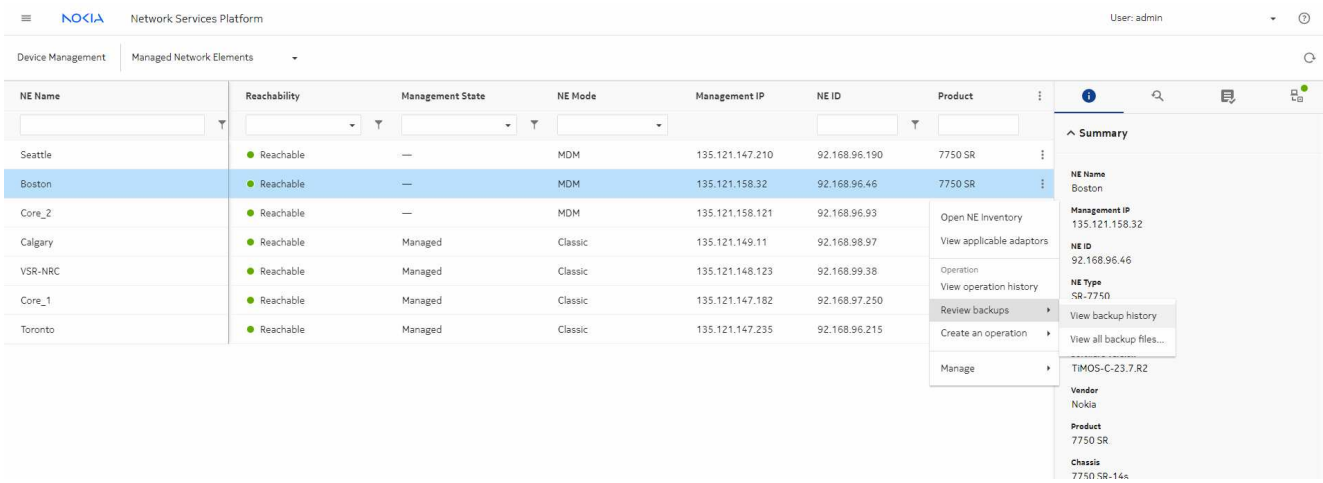
Double click on the test suite to see the results. All tests are passing, verifying connectivity over the link.



5.3.9 Restore the NE configuration

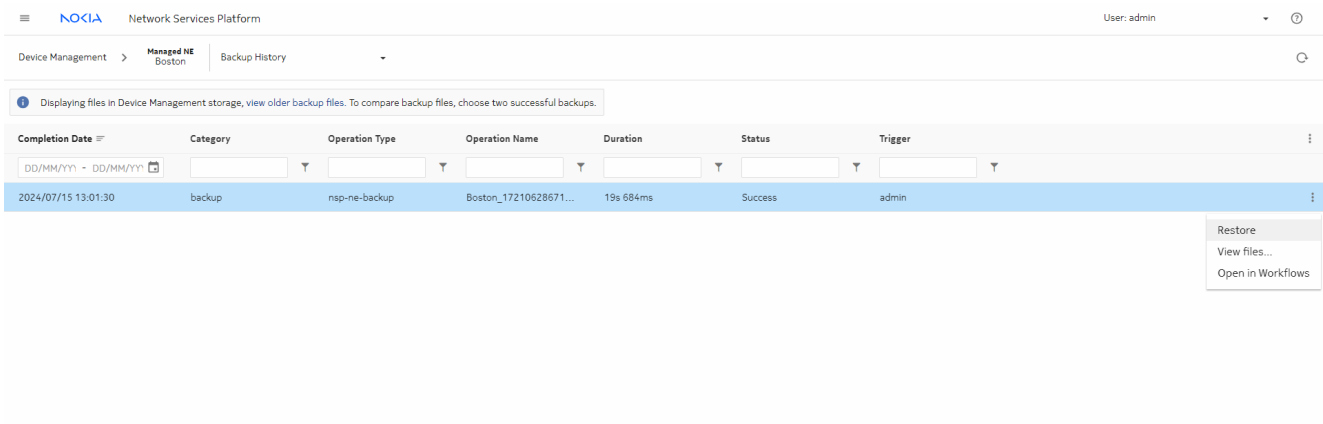
1

Finally, we can perform an optional restore operation. Returning to the Device Management, Managed Network Elements view, choose **Review backups**, **View backup history** from the Table row actions menu (⋮)



2

Select the most recent backup and choose **Restore** from the Table row actions menu (⋮).



3

When the restore is completed, select the NE and click Manage, Resync.

The NE is working and is ready for further configuration.

5.4 Onboarding a service into NSP

5.4.1 Purpose

This process shows you how to use the NSP to create a service and to monitor service health, service components' health, and service performance.

See the *NSP Network and Service Assurance Guide* for detailed procedures.

5.4.2 Create a service using service management

Note: This process assumes that intent types for service creation have already been imported into Network Intents.

1

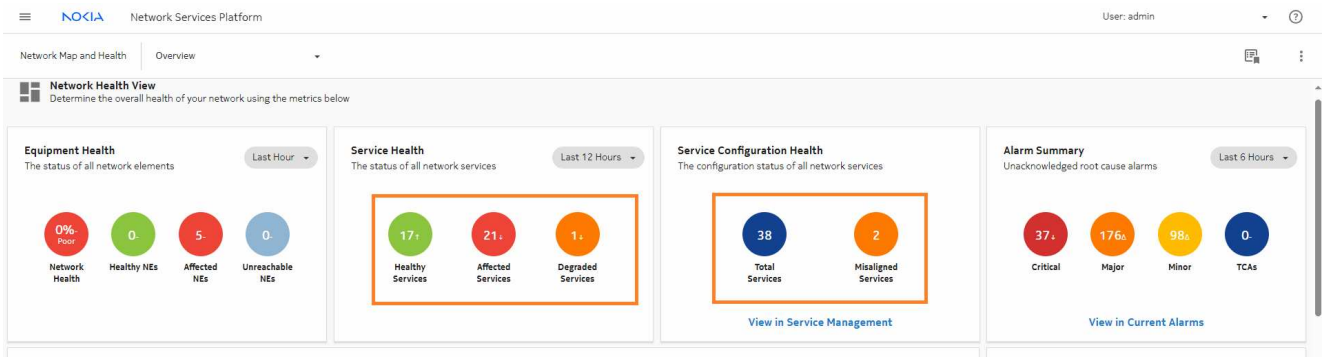
In NSP's service management views, create an Epipe service template, and use the template to create an Epipe service.

See the service creation procedure in the *NSP Service Management Guide*.

5.4.3 View service information in the Network Map and Health dashboard

1

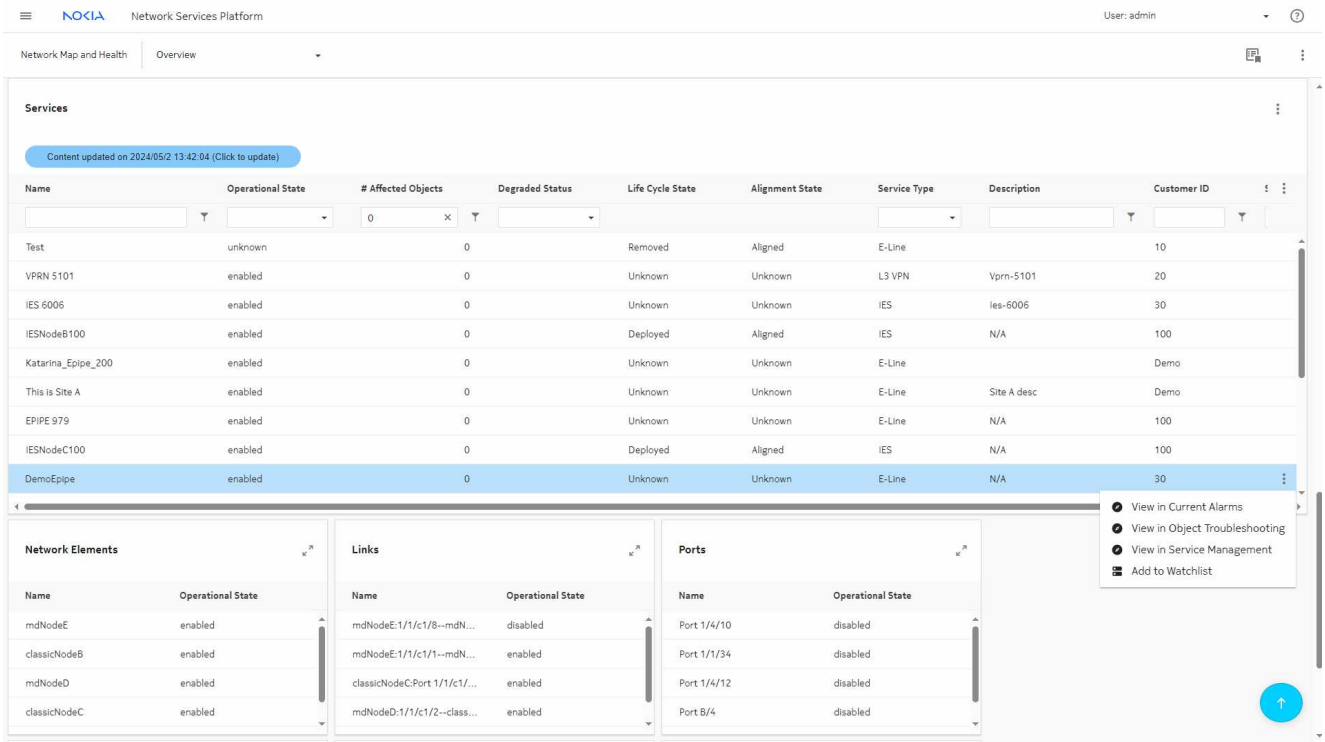
The Network Health View at the top of the Network Map and Health dashboard shows the health and configuration status of the services in the network.



2

Click on the Healthy Services circle in the Service Health dashlet to navigate to a filtered list of services. You can change the filters in this list as needed.

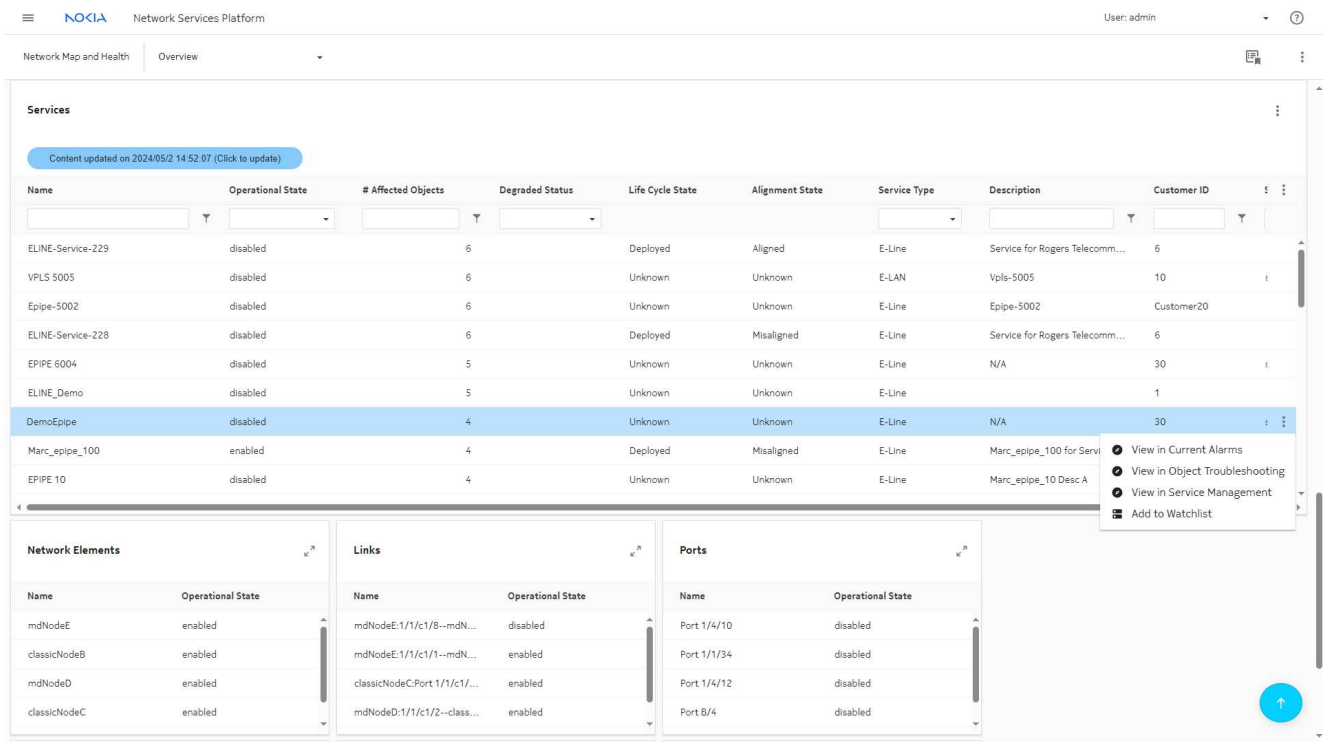
Select a service to navigate to Service Management or to the Object Troubleshooting dashboard from the table row actions menu.



3

Click on the Total Services circle in the Service Configuration Health dashlet to navigate to a list of all services.

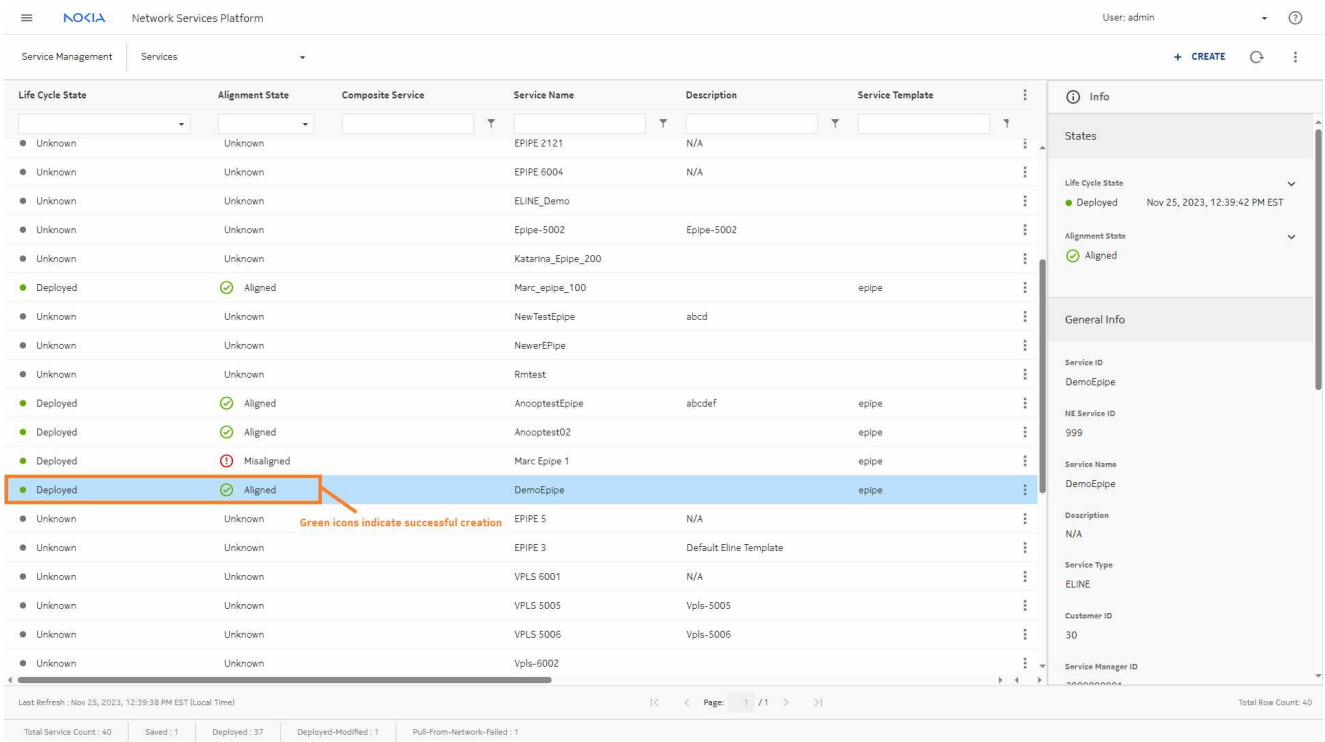
Select a service to navigate to Service Management or to the Object Troubleshooting dashboard from the table row actions menu.



5.4.4 View the service in Service Management

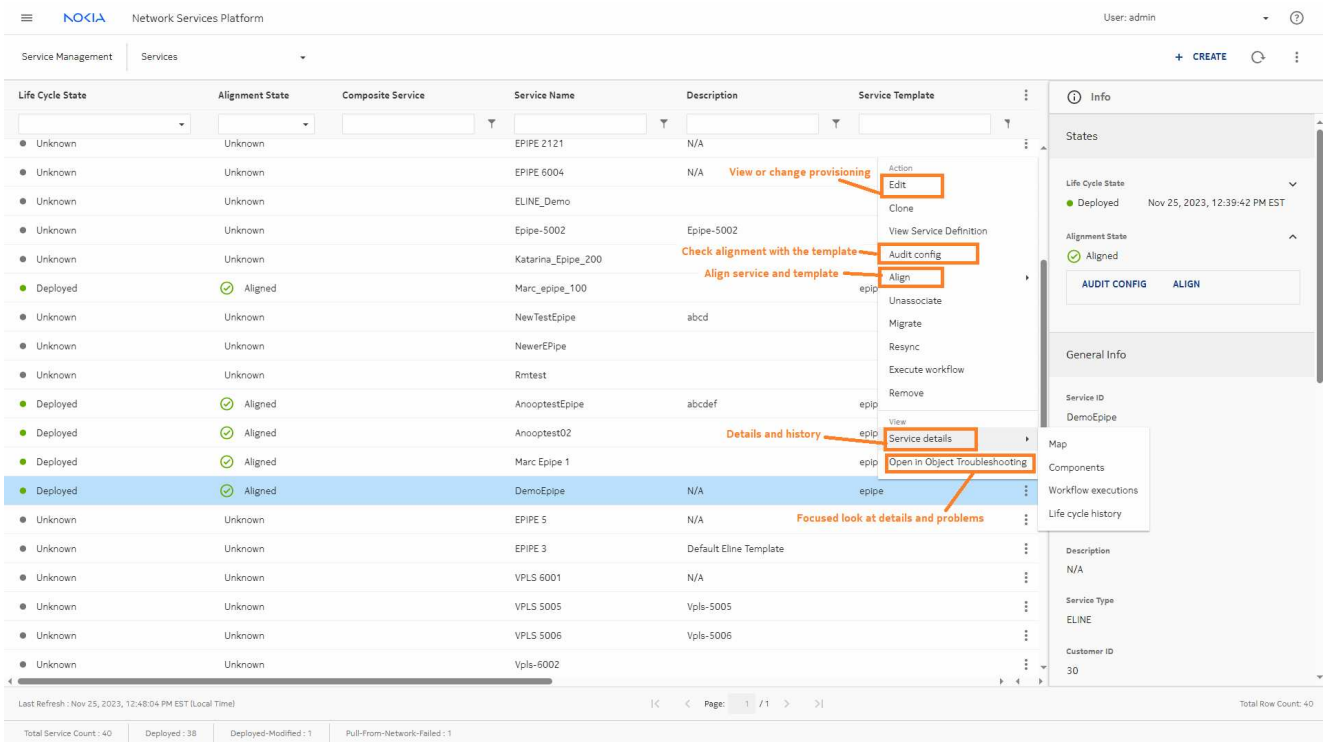
1

Open **Service Management**, **Services**. Green icons indicate that the service was created and deployed successfully and is aligned with the template used to create it.



2

Select the service. In the More ⋮ menu, there are multiple options for more information.

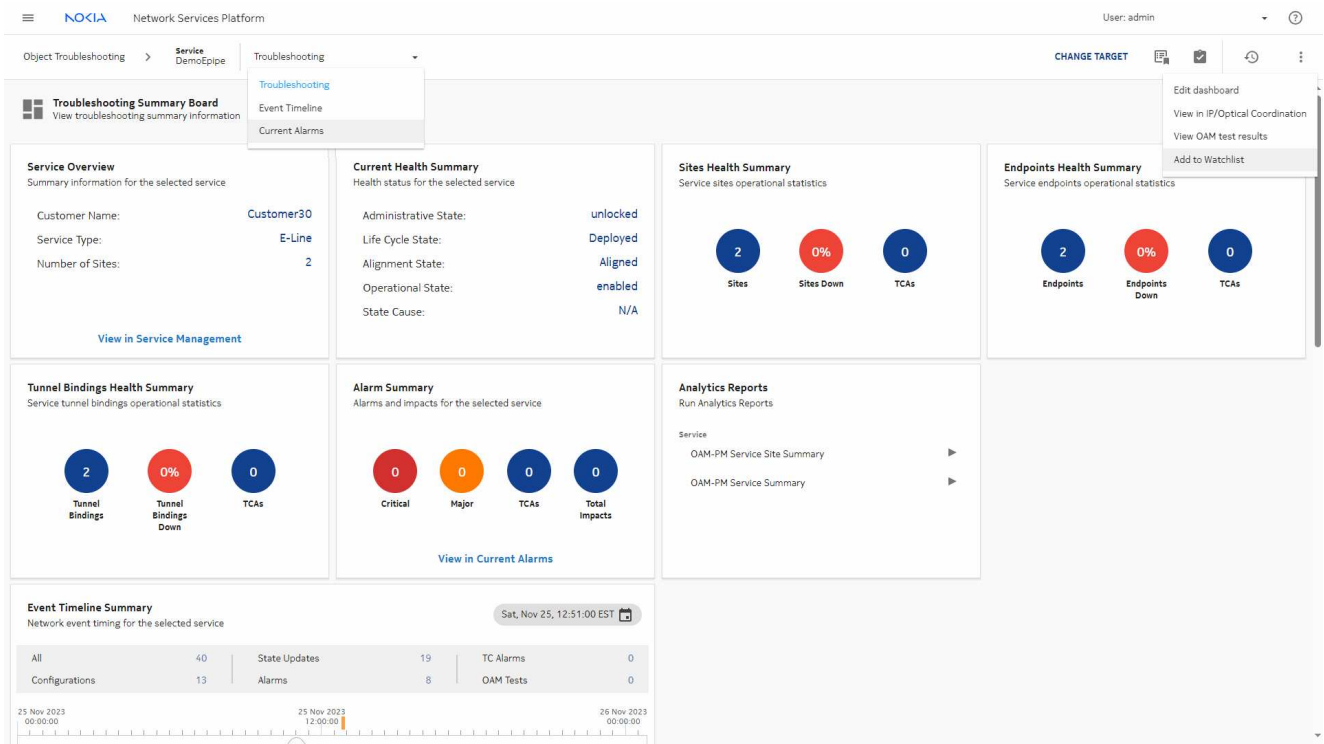


Choose **Open in Object Troubleshooting** to view the service in the Object Troubleshooting dashboard.

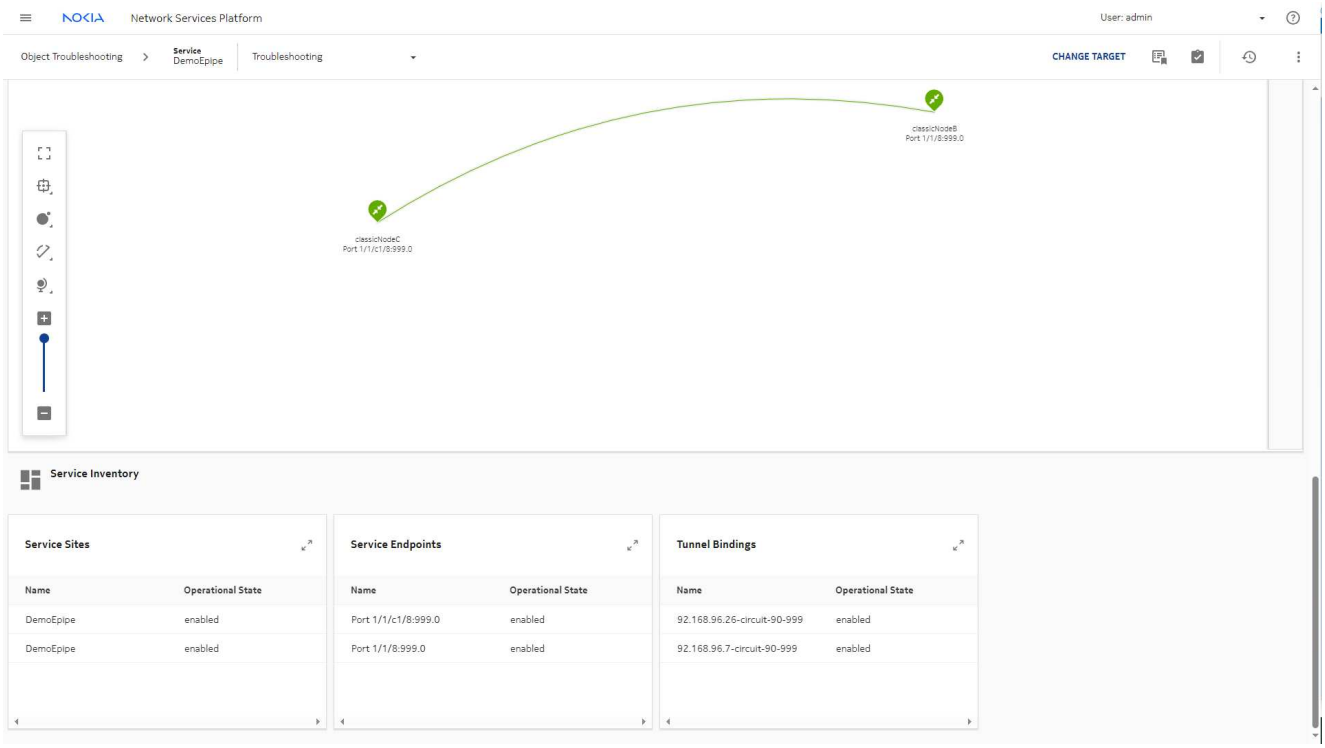
3

The Object Troubleshooting dashboard displays summaries of alarm, site, endpoint, and tunnel binding health, and if event recording has been enabled, an event timeline summary. From the view drop-down, you can navigate to the event timeline or to the Current Alarms page.

From the More menu (⋮) at the top of the page, you can add the service to the watchlist or open other detailed views. Adding the service to the watchlist allows you to easily navigate directly to it in the future.



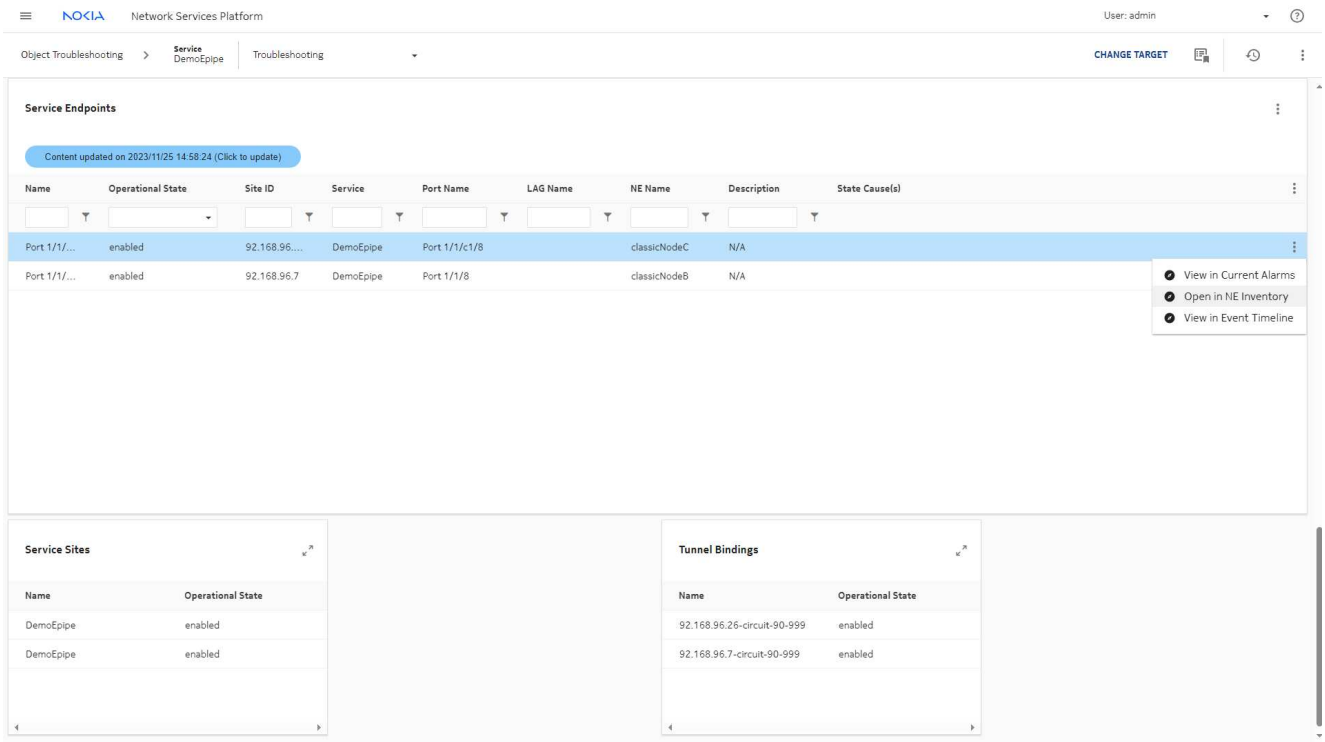
Scroll down in the view to see the Service map and Service inventory summaries.



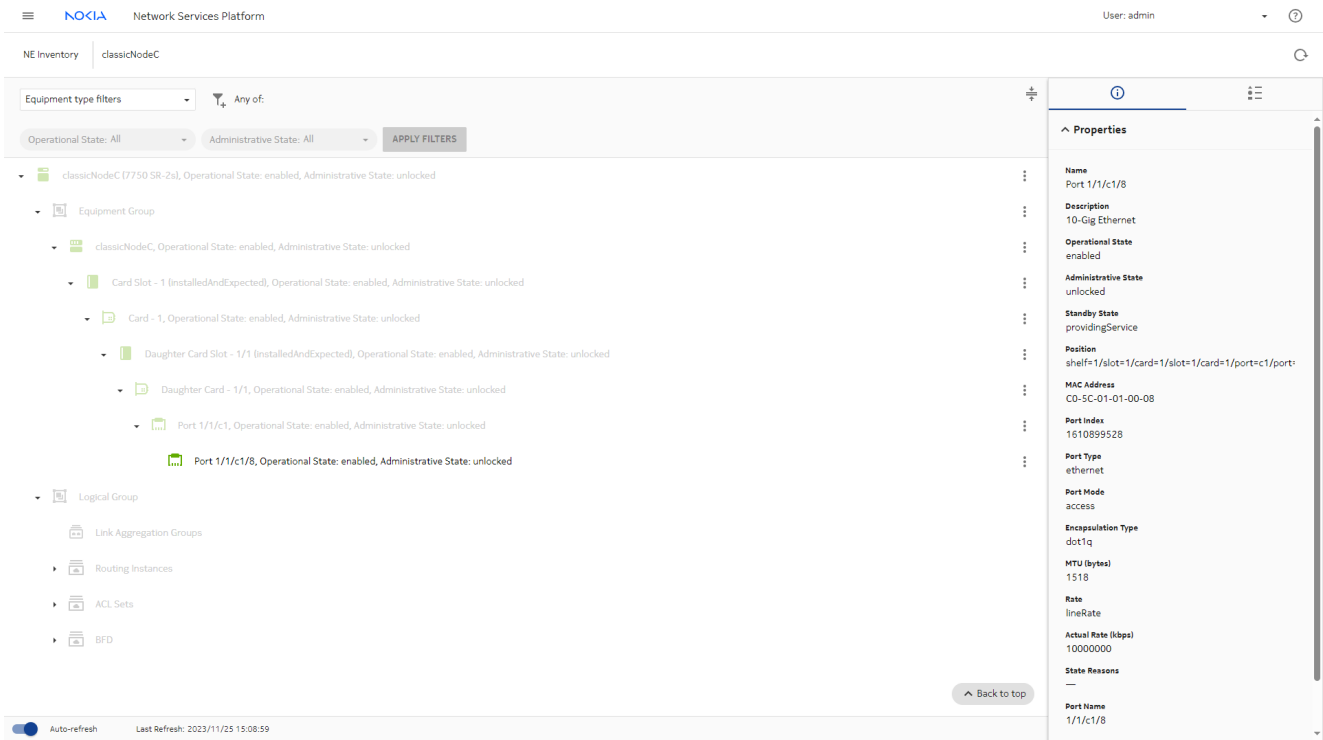
4

Click **Expand size** (⤢) on the Service Endpoint summary dashlet to see detailed information about the port associated with the endpoint.

Select an endpoint and choose Open in NE Inventory from the table row actions menu (⋮).



In the NE Inventory view, click on the port to see port details in the Info panel.



5.4.5 Initiate OAM tests from the service in the Object Troubleshooting dashboard

Returning to the Object Troubleshooting dashboard, create OAM tests to verify that the new service was provisioned and activated properly. On-demand testing verifies that traffic is flowing. After we have confirmed traffic, we can run proactive tests.

1

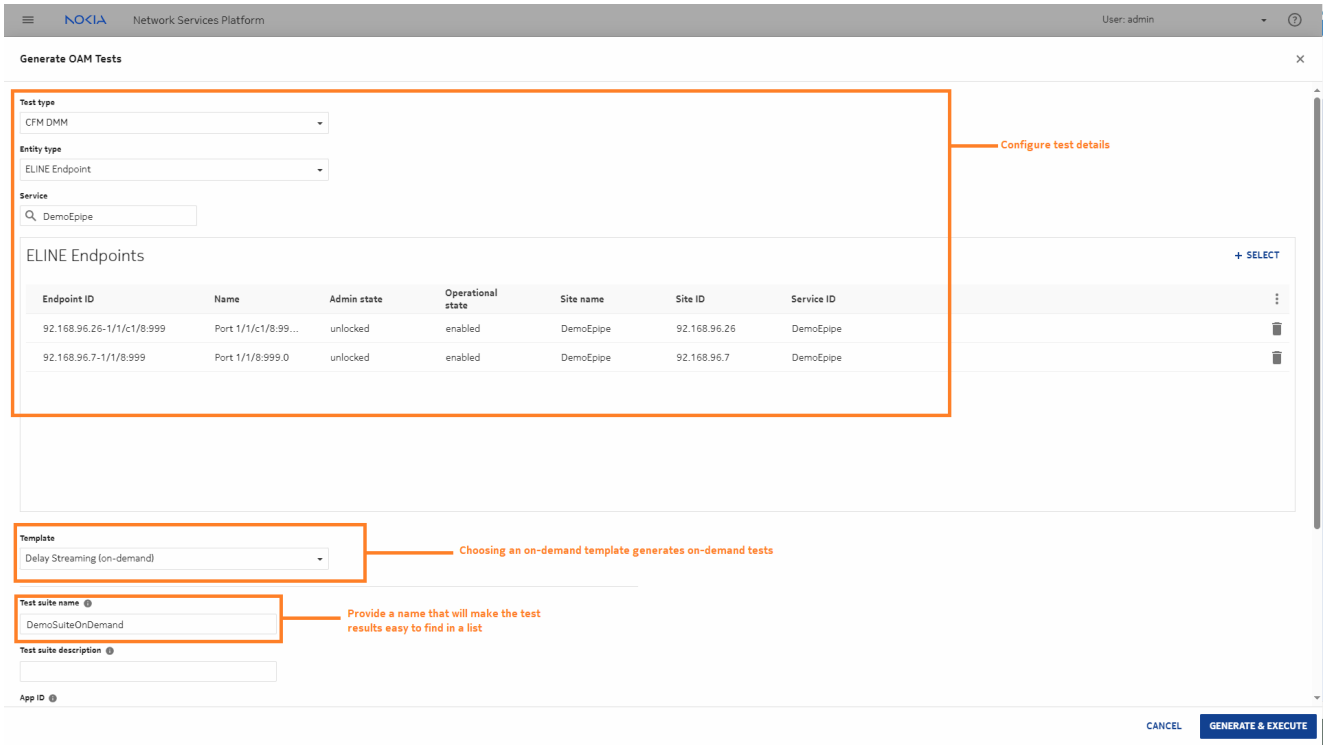
From the Object Troubleshooting dashboard, choose **Create OAM Test Suite**( ).

2

In the form that opens, configure the test parameters:

1. Choose the test type and select both service endpoints.
2. Choose an on-demand template from the **Template** drop-down.
3. Enter a name for the group of tests. Choose a name that will make the tests easy to tell apart from others in a test results page.

Click **GENERATE & EXECUTE**.



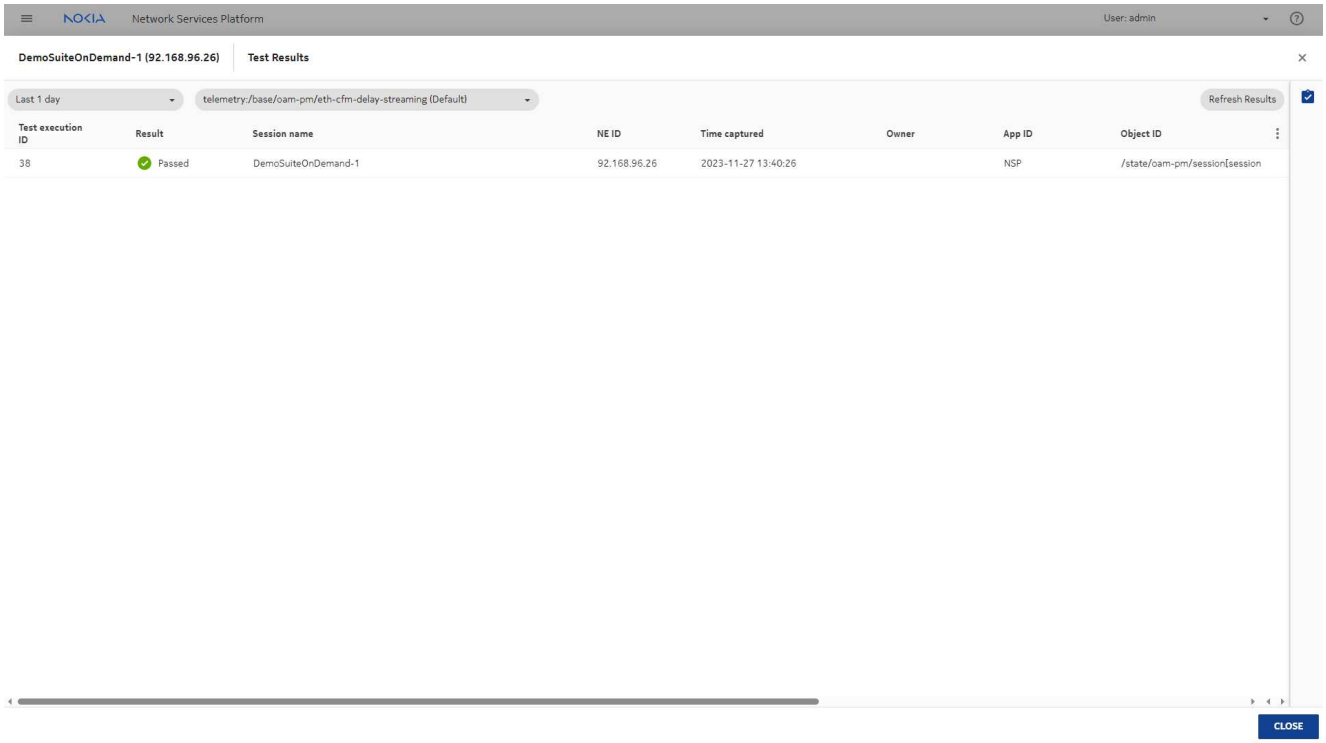
The tests are executed.

3

When test generation is completed, choose **View OAM test results** from the More menu (⋮) in the **Object Troubleshooting** dashboard.

The **Data Collection and Analysis Management**, **Tests** page opens, filtered to show the tests on the service. Select an on-demand test and choose **View Results** from the table row actions menu (⋮).

The on-demand test has passed, verifying that traffic is flowing.



5.4.6 View port details and utilization data in real time

From the NE inventory view, you can launch a utilization chart to view raw utilization data and verify that traffic is moving between service endpoints. This request creates a temporary telemetry subscription, which is deleted when the utilization chart is closed.

1

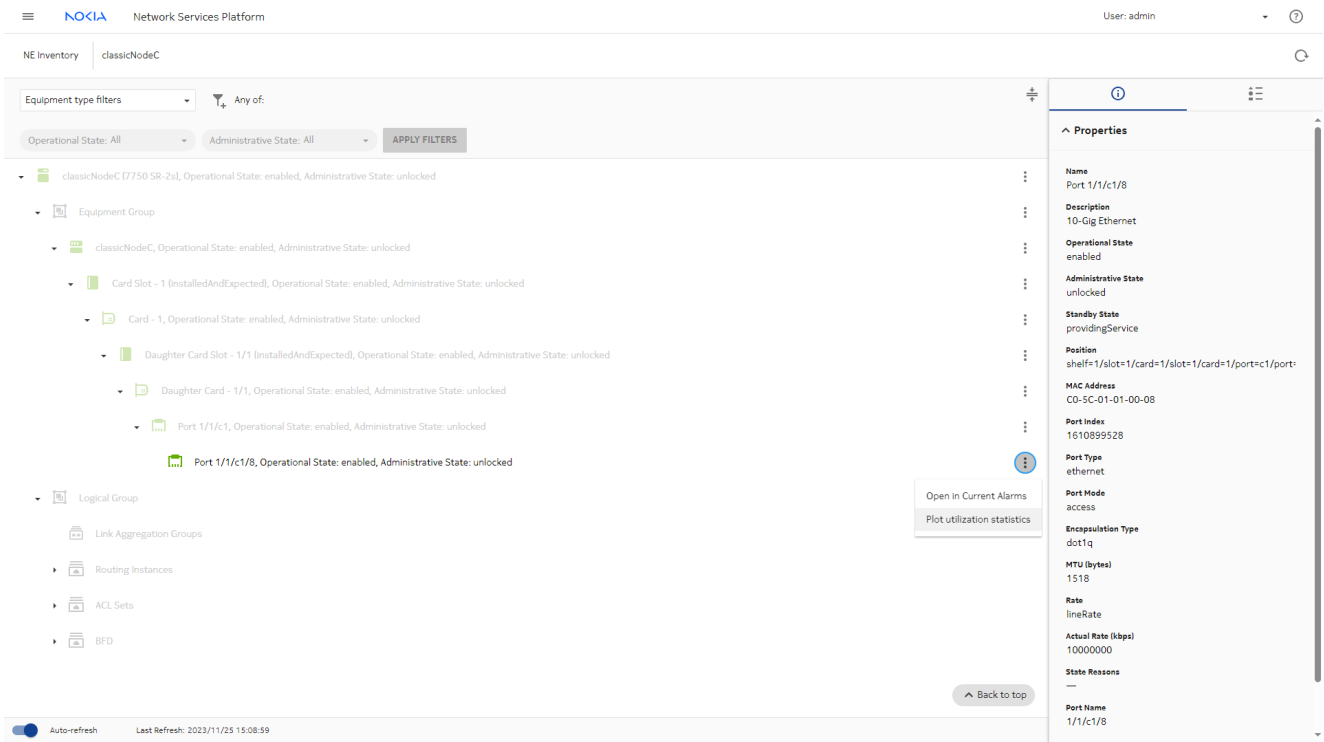
Identify the service endpoints:

1. Open the Object Troubleshooting dashboard for the service and navigate to **Service Endpoints**.
2. Select an endpoint and choose **Open in NE Inventory** from the table row actions menu (⋮).

The NE Inventory view for the endpoint NE opens.

2

In the **NE Inventory** view, click on a port. The port properties display in the **Info** panel. From the More menu for the port (⋮), choose **Plot utilization statistics**.



3

Data Collection and Analysis, **Visualizations** opens, showing the chart of the pre-configured utilization counters.

4

The creation of the chart creates a temporary subscription for the utilization counters.

The subscription is automatically deleted when you close the chart.

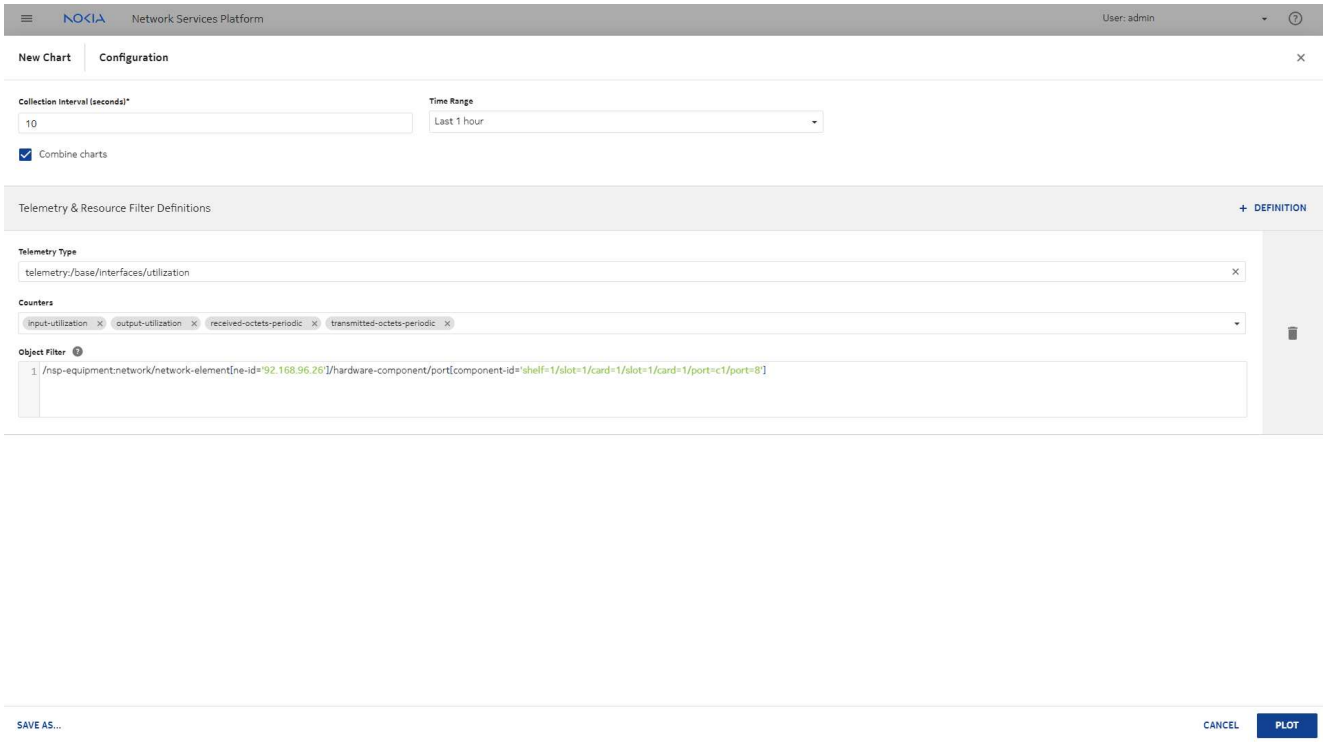
Tip: The description of the temporary subscription is **Created by telemetry data subscription**.

5

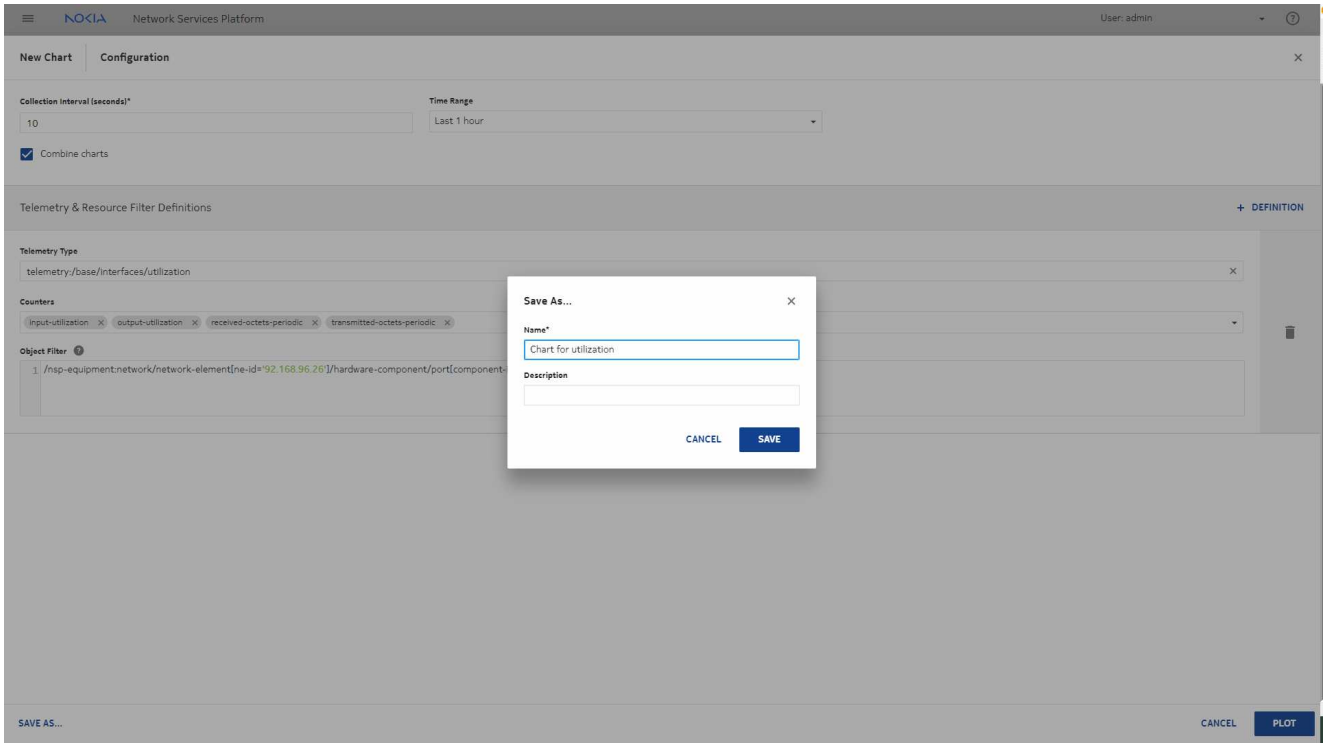
While the chart is open, you can:

a. Review the details of the pre-configured subscription by clicking **Configure**.
Tip: From the **New Chart** , **Configuration** form, copy the **Object Filter** string. You can use this string to create a permanent subscription.

b. Edit the chart configuration, for example, to show different counters.



c. Save the chart to make the chart available from **Data Collection and Analysis**, **Visualizations** in the future.



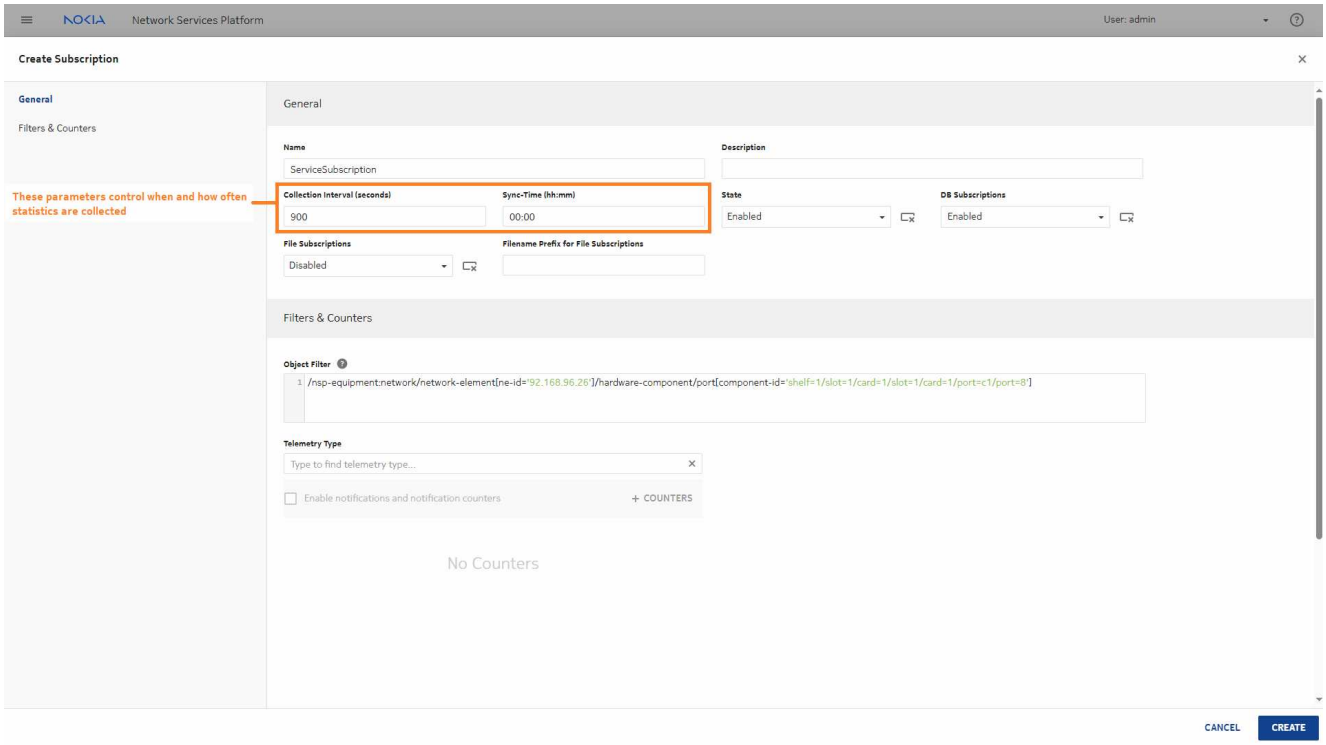
5.4.7 Create permanent telemetry subscriptions for the service endpoints

Creating a telemetry subscription is an optional step, used for monitoring performance over time. A telemetry subscription allows you to configure statistics collection, for example, utilization statistics for a service, and to run the collection at any time, for example, for use in SLA management. Statistics can also be used to generate Analytics reports. To learn how to create a subscription, and for information about aggregation and retention for use in reporting, see the *NSP Data Collection and Analysis Guide*.

1

Perform the subscription creation procedure to create subscriptions for the service SAPs. See the *NSP Data Collection and Analysis Guide* for more information.

Use the object filter string you copied from the temporary subscription in Stage 5.



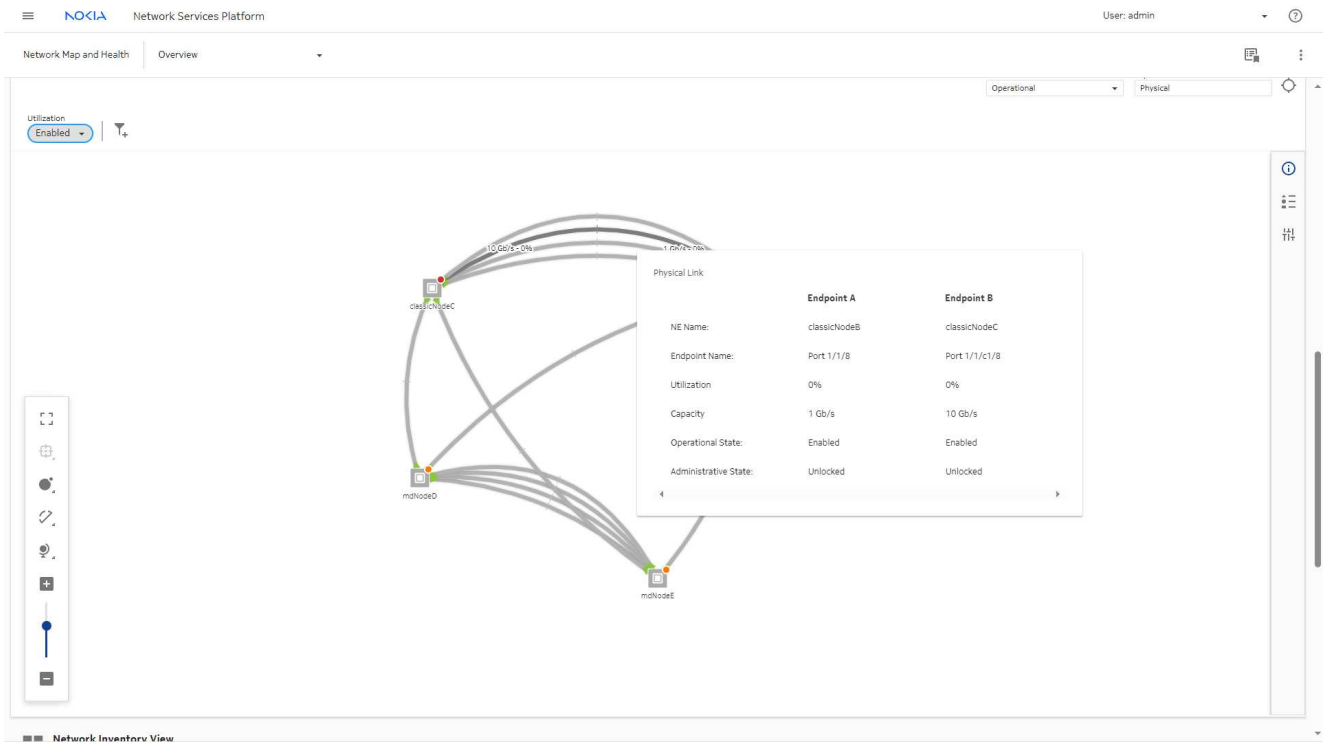
5.4.8 View utilization statistics from the Network Map and Health dashboard

1

In the Network Map and Health dashboard, navigate to the network map. Choose **Enabled** from the **Utilization** drop-down.

2

Hover over a link in the network map to show utilization information.



A subscription is automatically created for the ports associated with the endpoints for NEs present on the Network Map and Health dashboard utilization map.

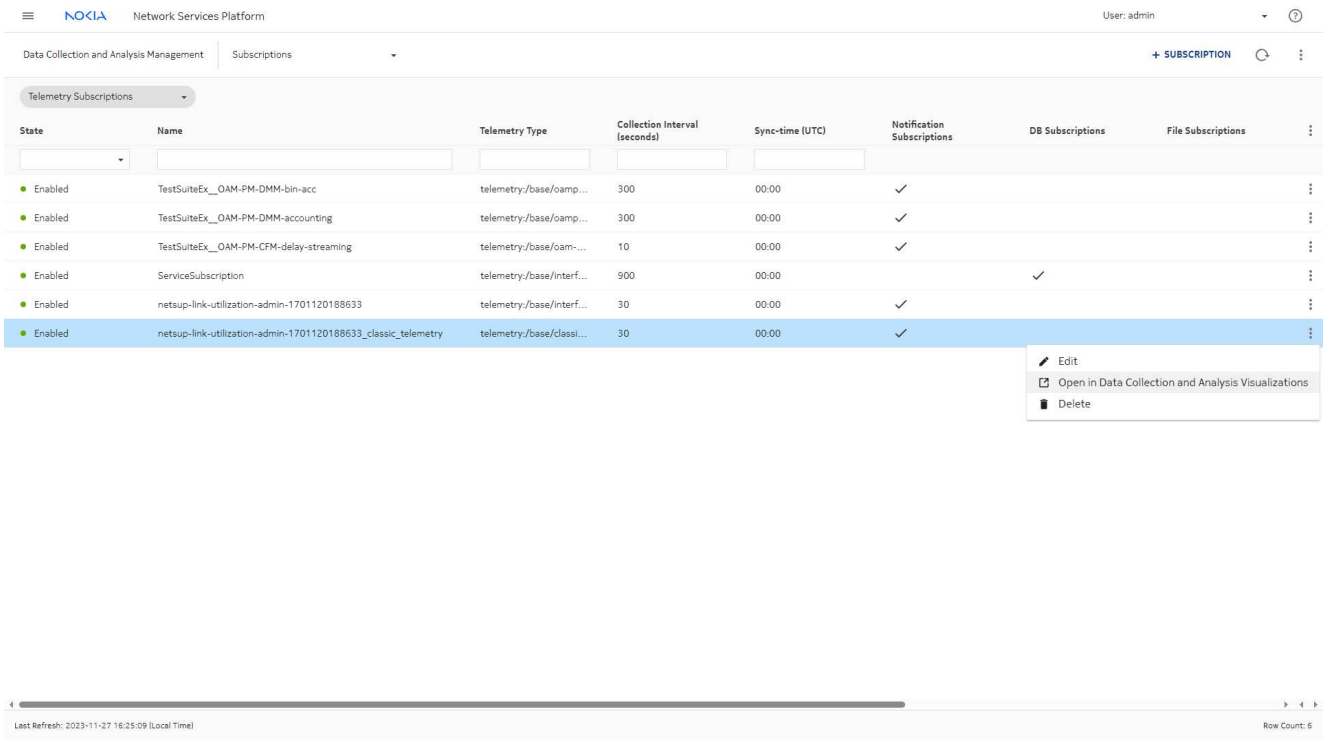
3

Open **Data Collection and Analysis**, **Management**. Edit the temporary subscription as needed.

To chart a subscription, select the subscription and choose **Open in Data Collection and Analysis Visualizations** from the table row actions menu (⋮)

Note: Two subscriptions are automatically generated, for two telemetry types: `base/classic-utilization/utilization` and `base/interfaces/utilization`. The interfaces telemetry type must be used for charting.

Tip: The name of each subscription starts with `netsup-`.



5.5 LSP Throughput with Forecast reporting scenario

5.5.1 Purpose

The LSP Throughput with Forecast (NSP) report provides the throughput trend for an LSP. The report can generate a forecast for daily and monthly granularities.

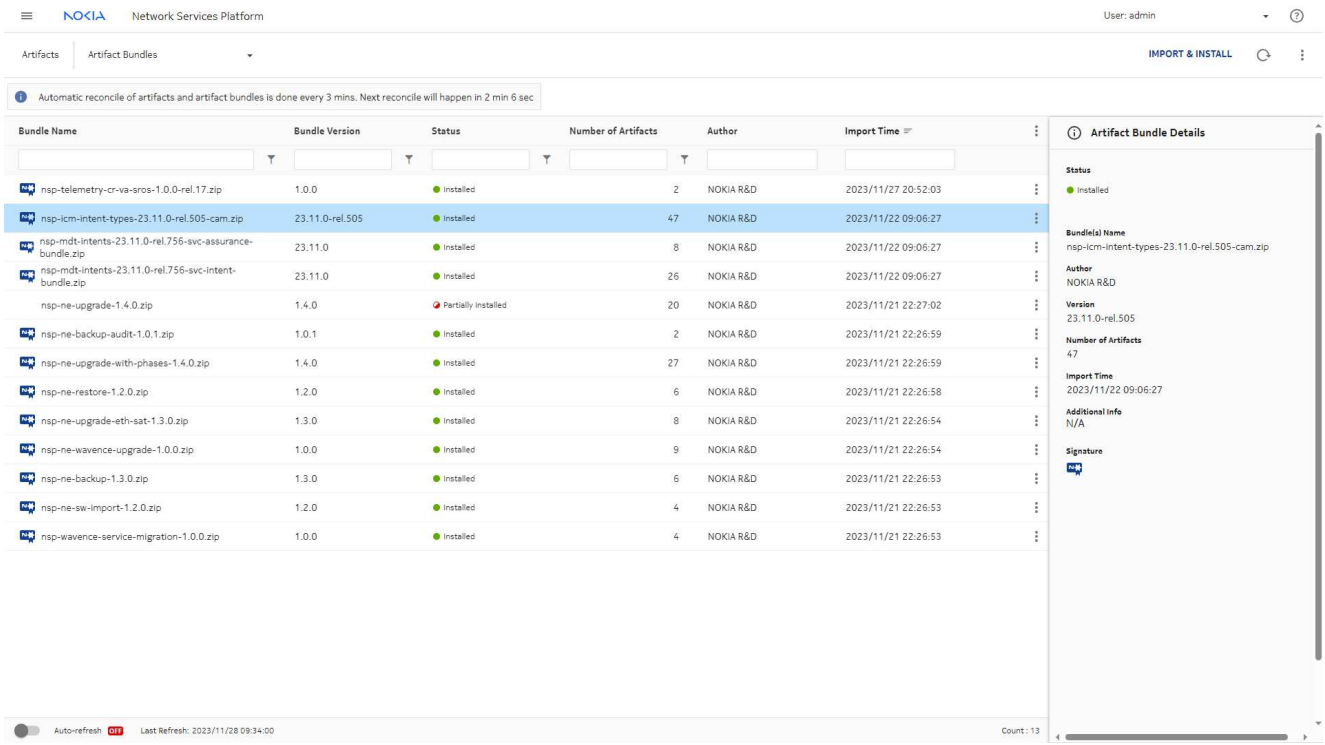
This process shows how to set up a service for LSP Throughput with Forecast reporting in Analytics.

5.5.2 Confirm that prerequisites for service provisioning are completed

1

Two intent type bundles are required for provisioning our service, and for setting up QoS and telemetry: icm-intent-types, and mdt-intents.

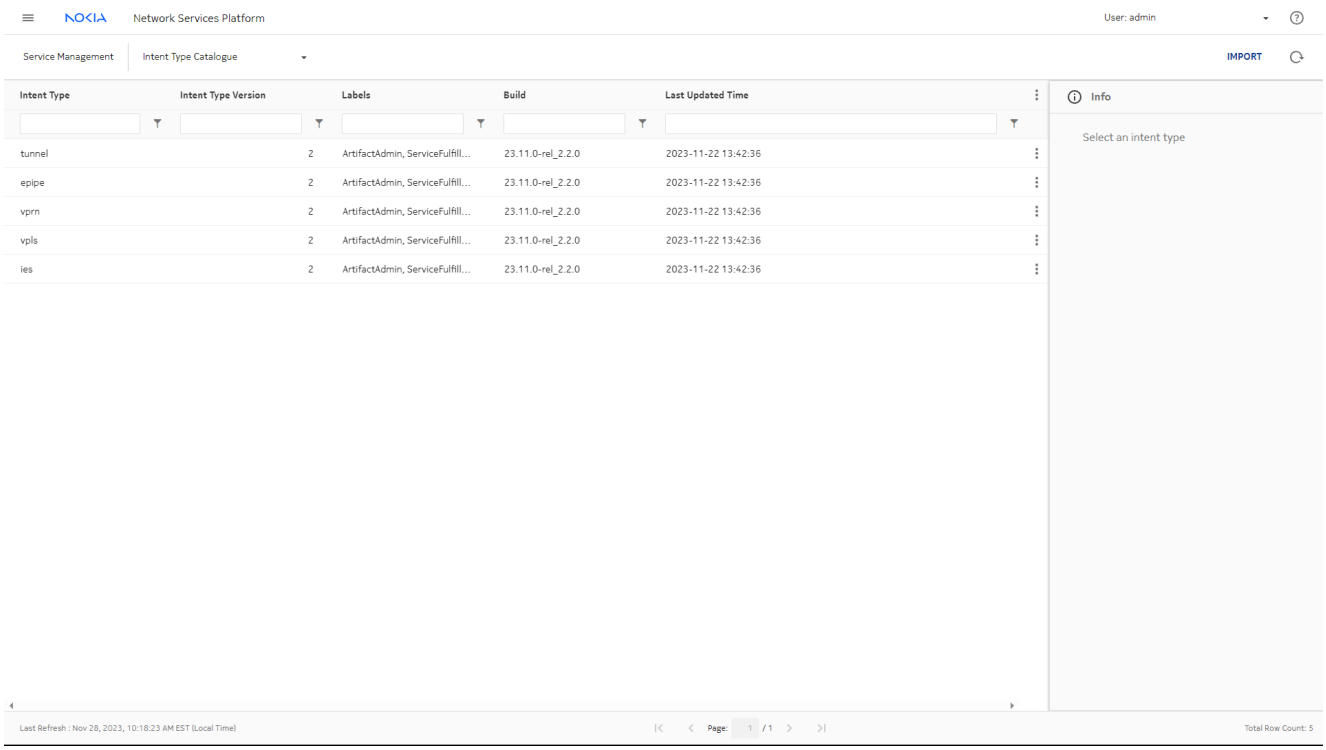
Checking the list in the **Artifacts**, **Artifact Bundles** view shows that both bundles are in Installed status.



2

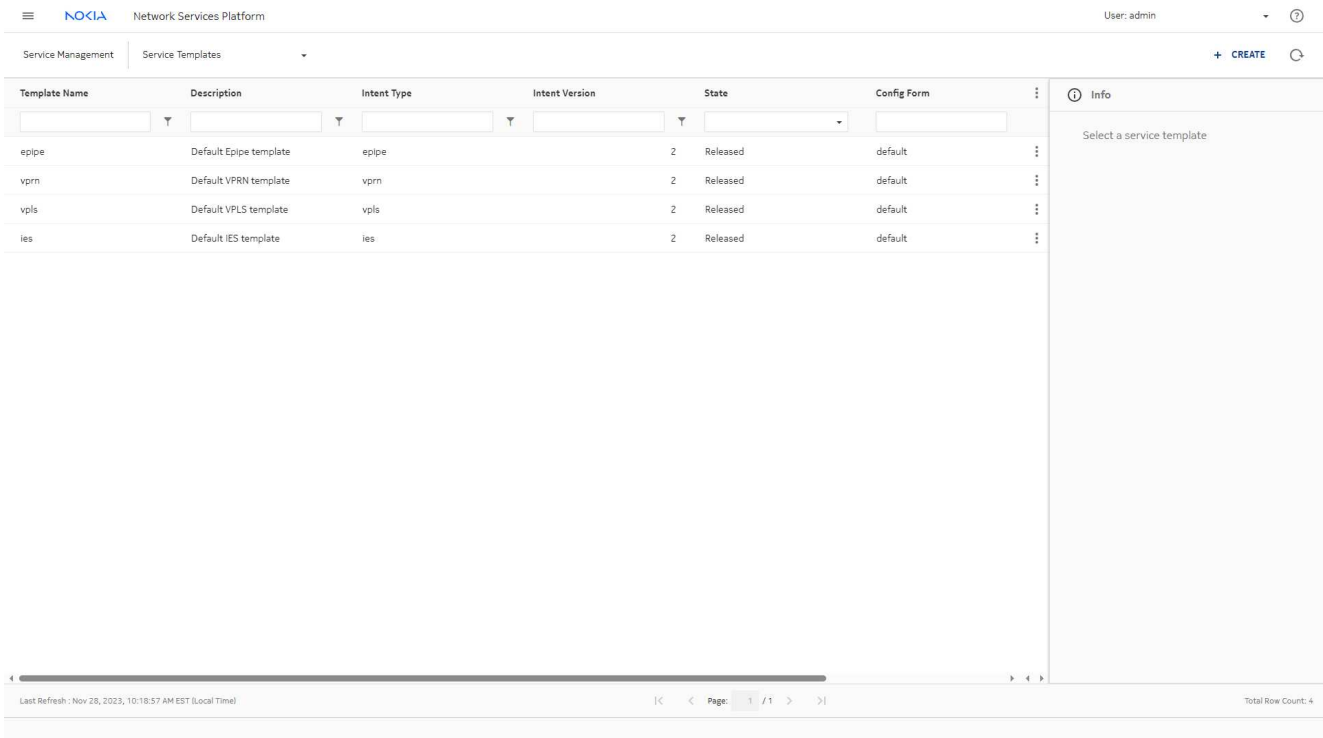
NSP installs the intent types to Network Intents, from which they can be imported to Service Management.

The **Service Management, Intent Type Catalogue** view shows that the intent types have been imported and are available for use in service management.



3

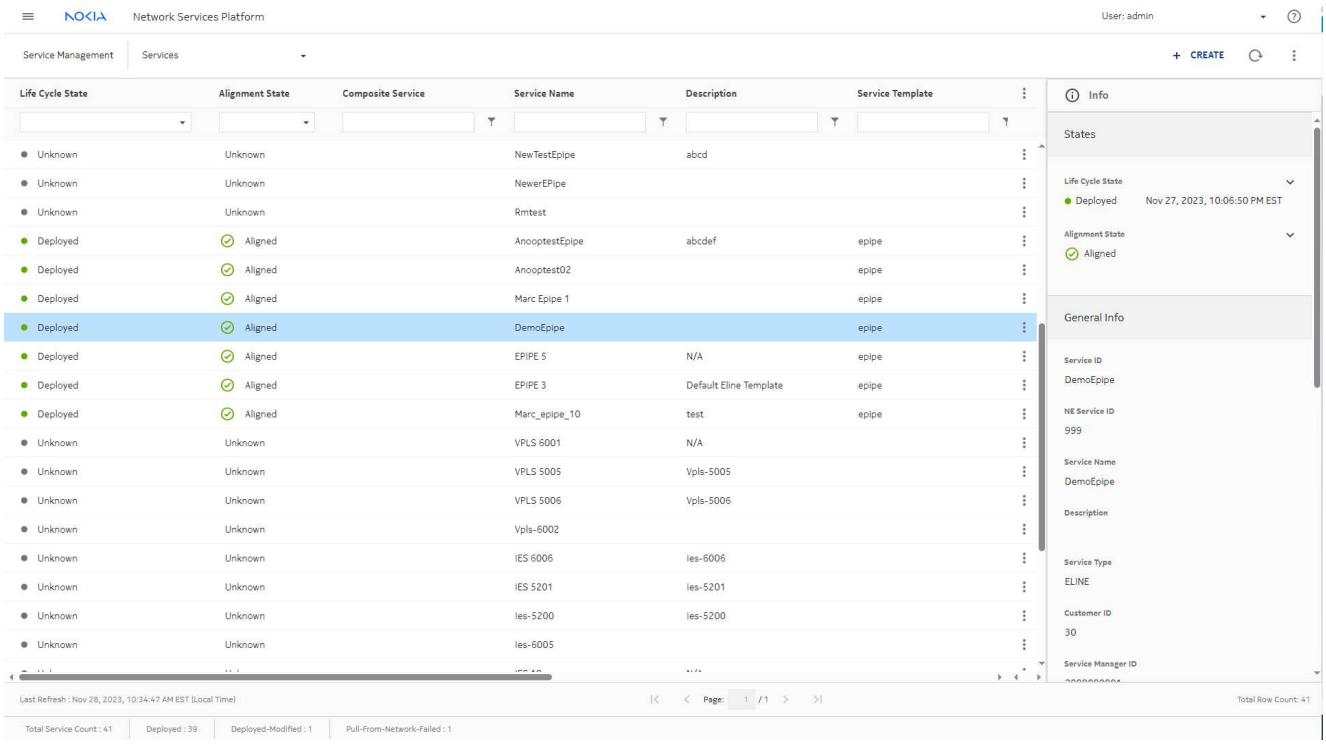
Switching to the **Service Management, Service Templates** view shows that the intent types have been used to create templates for various service types.



5.5.3 Verify the service parameters

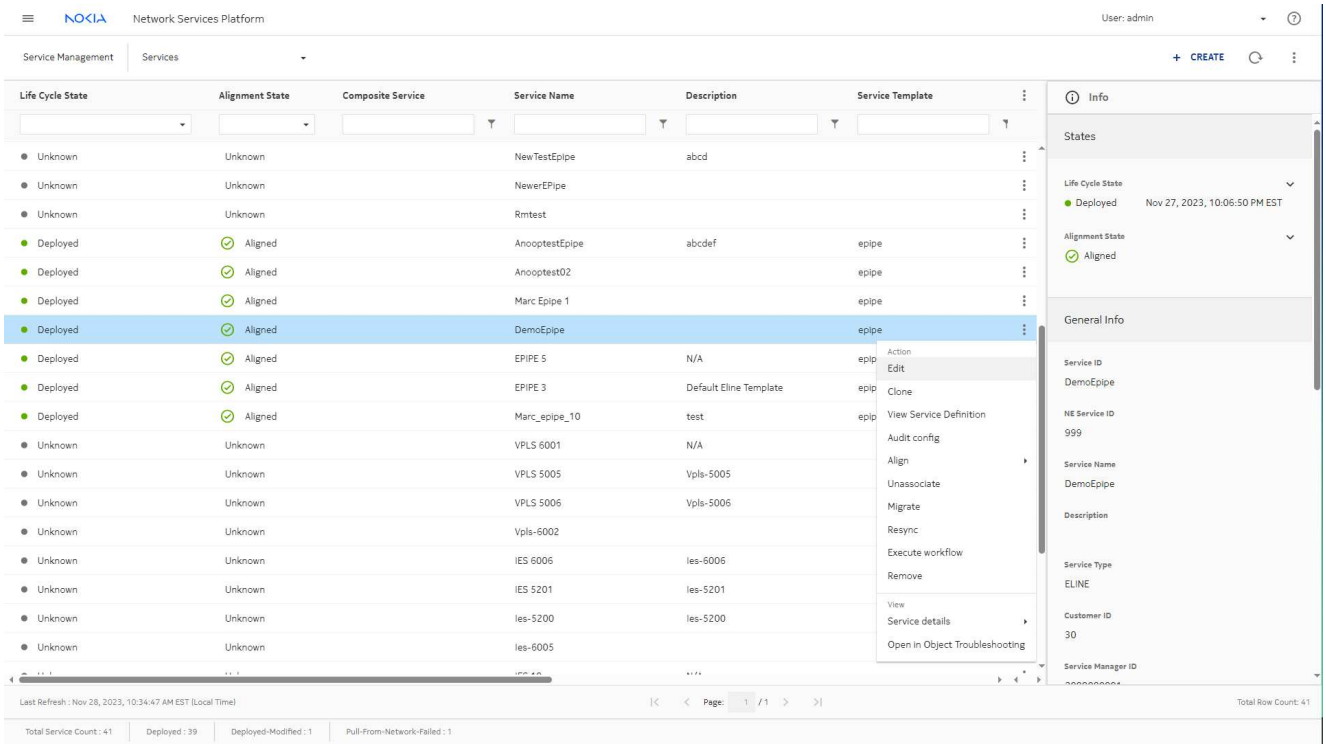
1

From the **Service Management, Services** view, we can see the provisioned services.



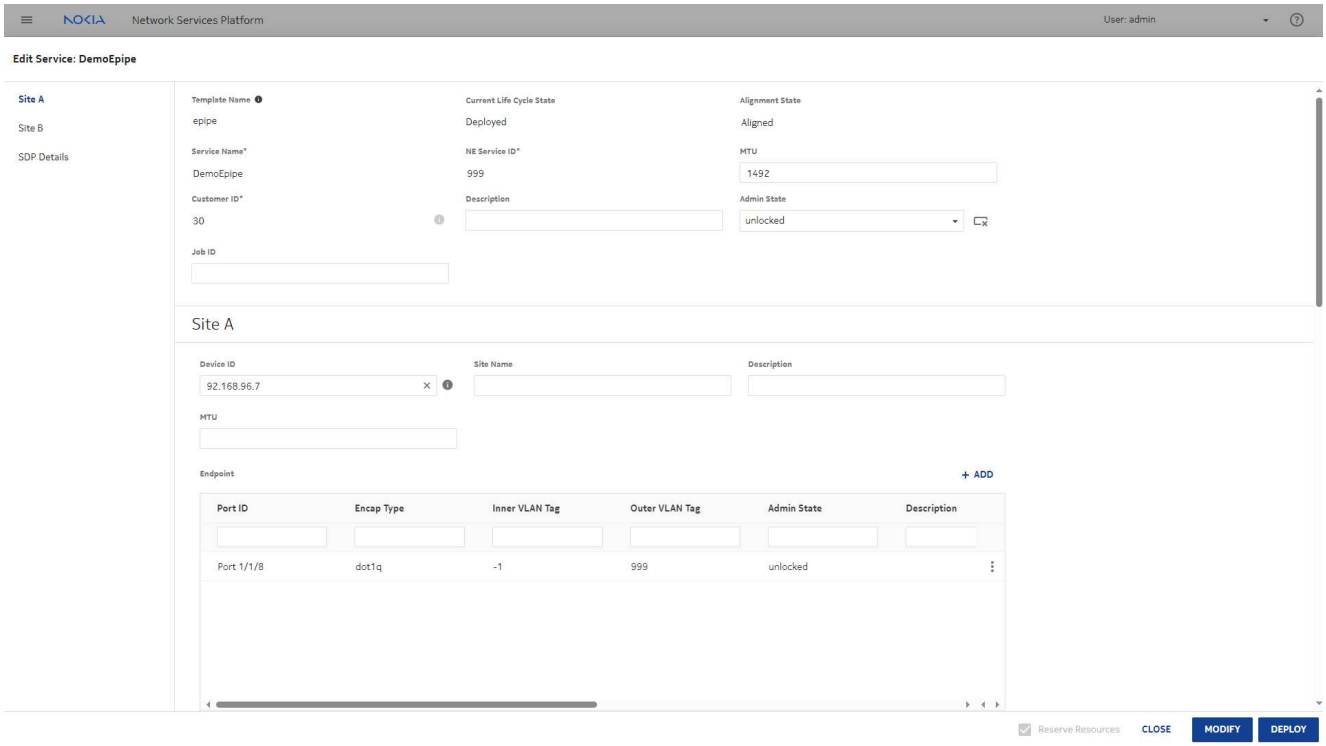
2

Opening the Edit form for a service will let us verify that everything we'll need is in place. Select the service and select Edit from the Table row actions menu.



3

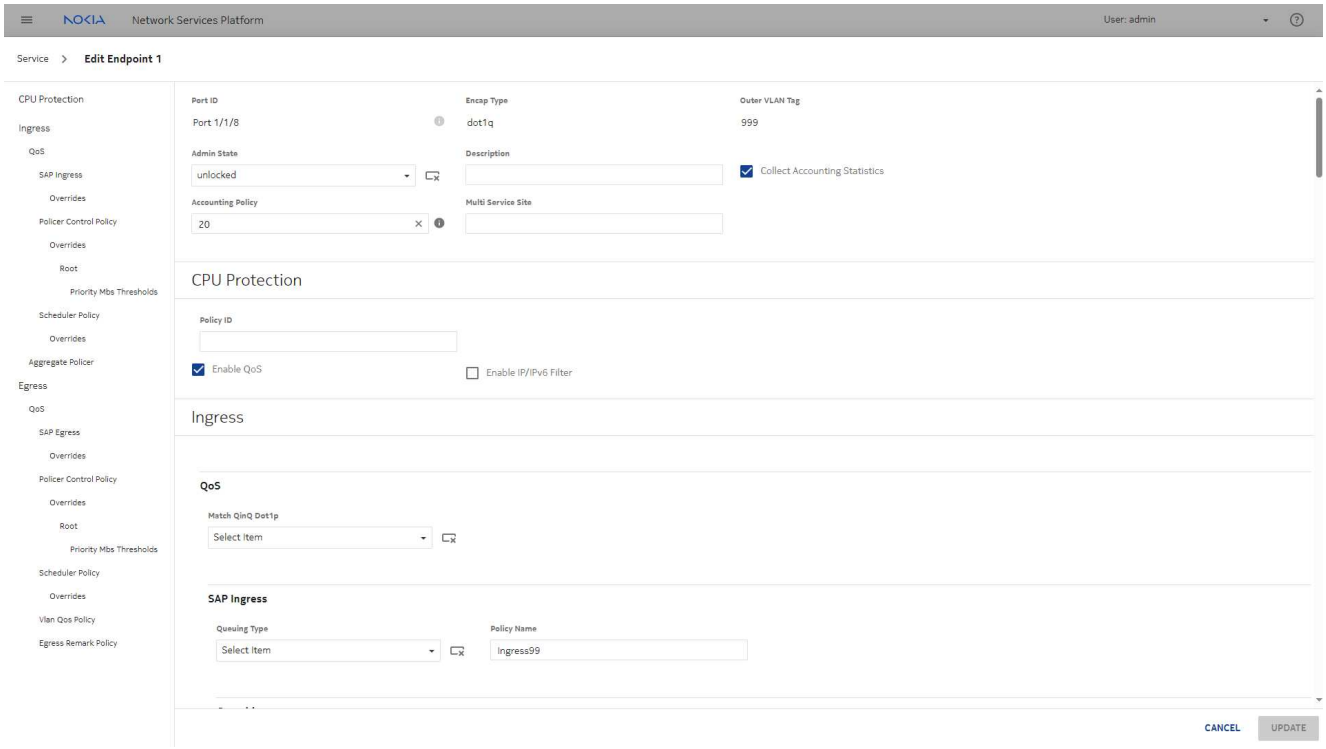
The Edit service form shows the basic service parameters such as service name and customer ID, and the service endpoints.



4

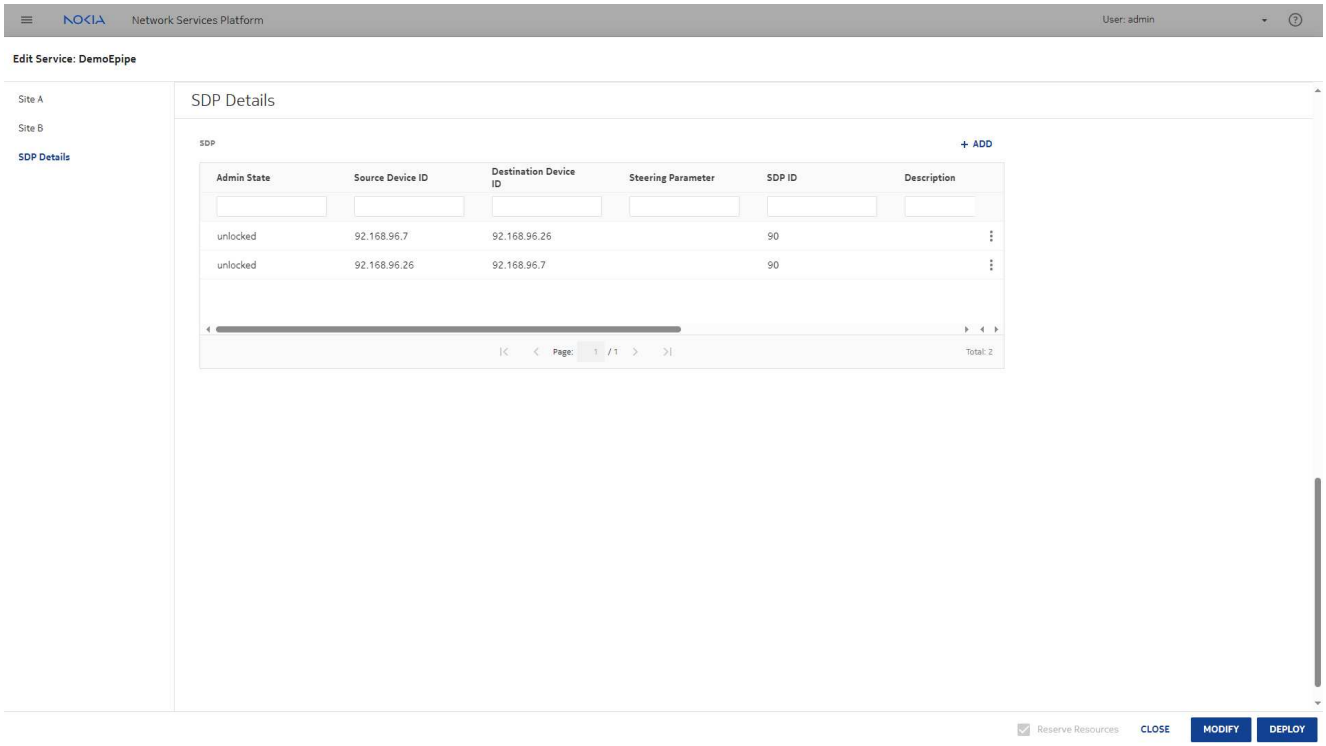
Site A of the service is on node B. Select the endpoint and choose Edit to verify the endpoint parameters.

In the Edit Endpoint form, we can see the ingress and egress QoS policies applied, and any overrides that have been added.



5

Returning to the Edit Service form, we can see the SDP details, the service destination points. An SDP has been added to the service for each direction.



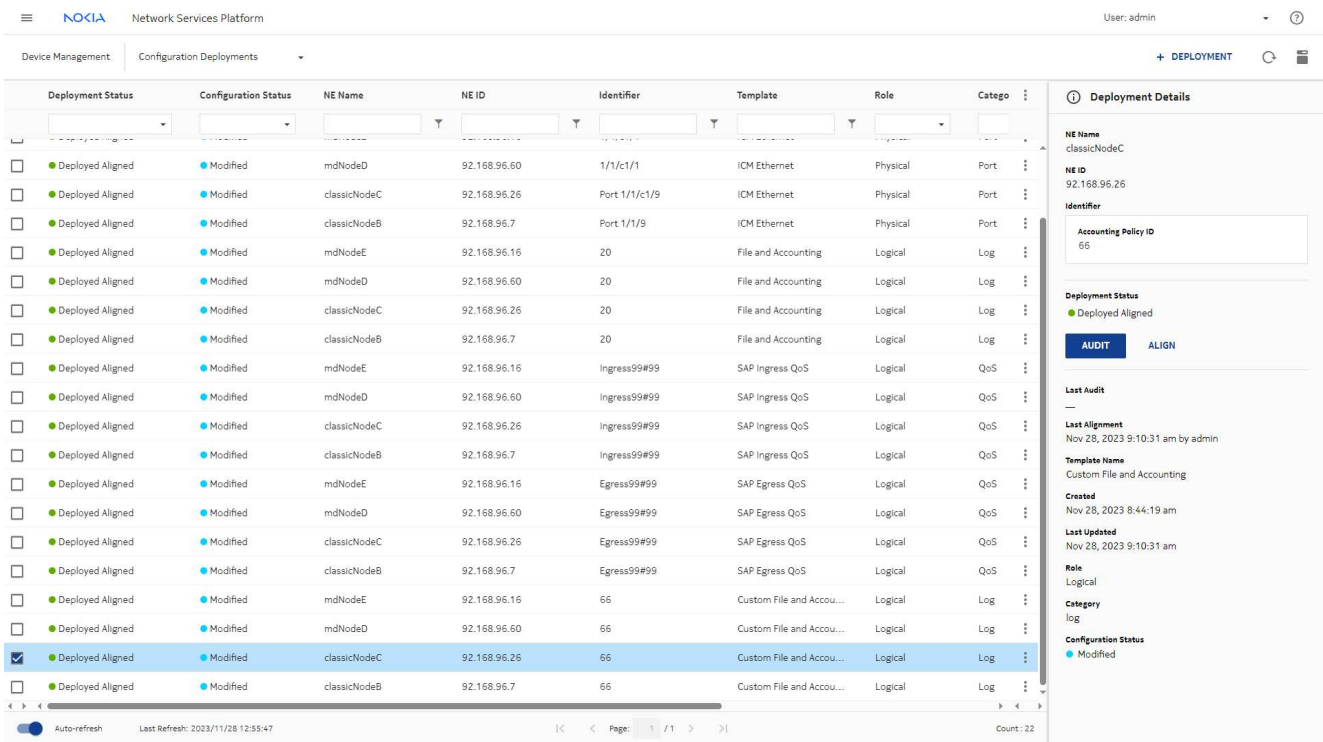
Each SDP uses an LSP, and it's this LSP that will provide the throughput telemetry data for our report.

5.5.4 Verify accounting policy configuration

1

To collect statistics on an NE, a file and accounting policy must be configured on the NE. This can be done by deploying a template in the **Device Management**, **Configuration Deployments** view.

In the Configuration Deployments list, we can see that a template called Custom File and Accounting has been deployed on the NE and the Deployment Status is Deployed Aligned.

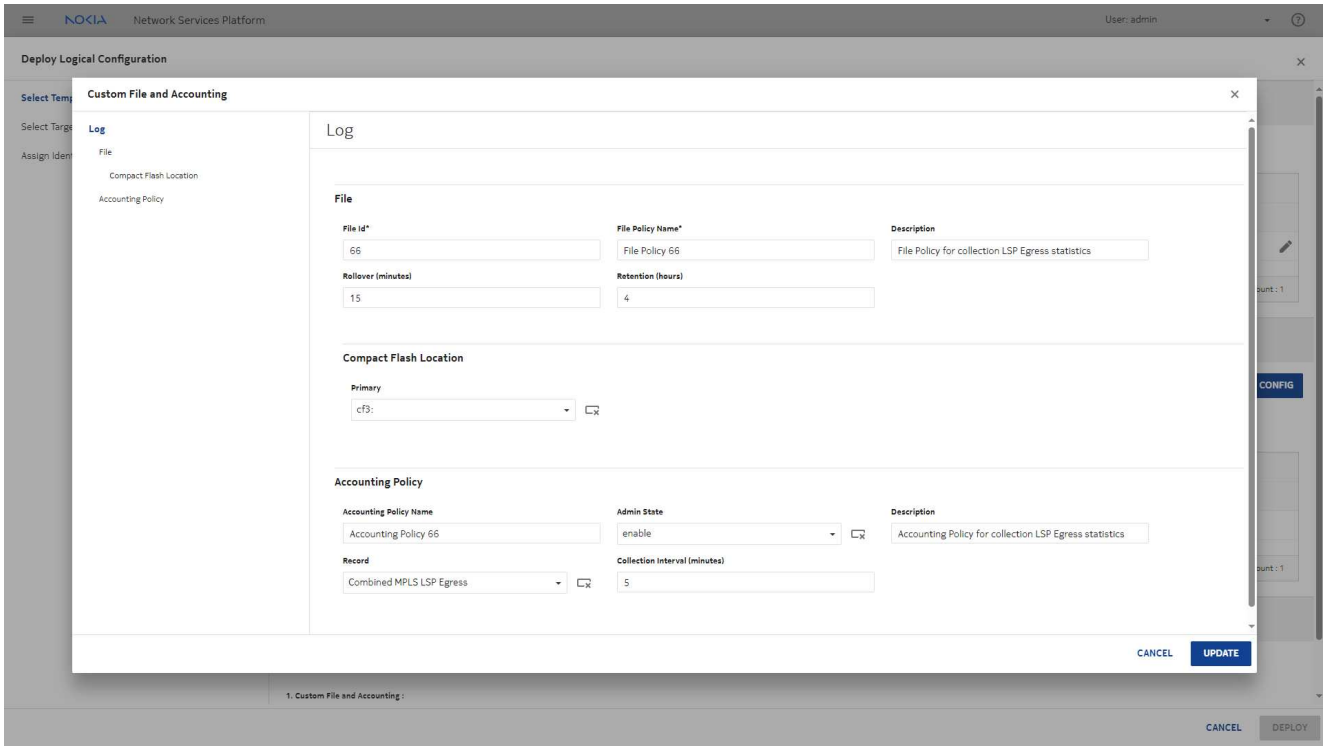


2

We can view the template details to see policy details:

1. Select the deployment and choose View/Edit from the Table row actions menu.
2. In the form that opens, click **VIEW/EDIT TEMPLATE CONFIG**.

The template information shows the rollover duration, or how long a statistics collection file remains open before a new file is started, the retention period for the file, and the compact flash location where the file is stored. Accounting policy details show that the policy applied is number 66, and it will be collecting Combined MPLS LSP Egress statistics.



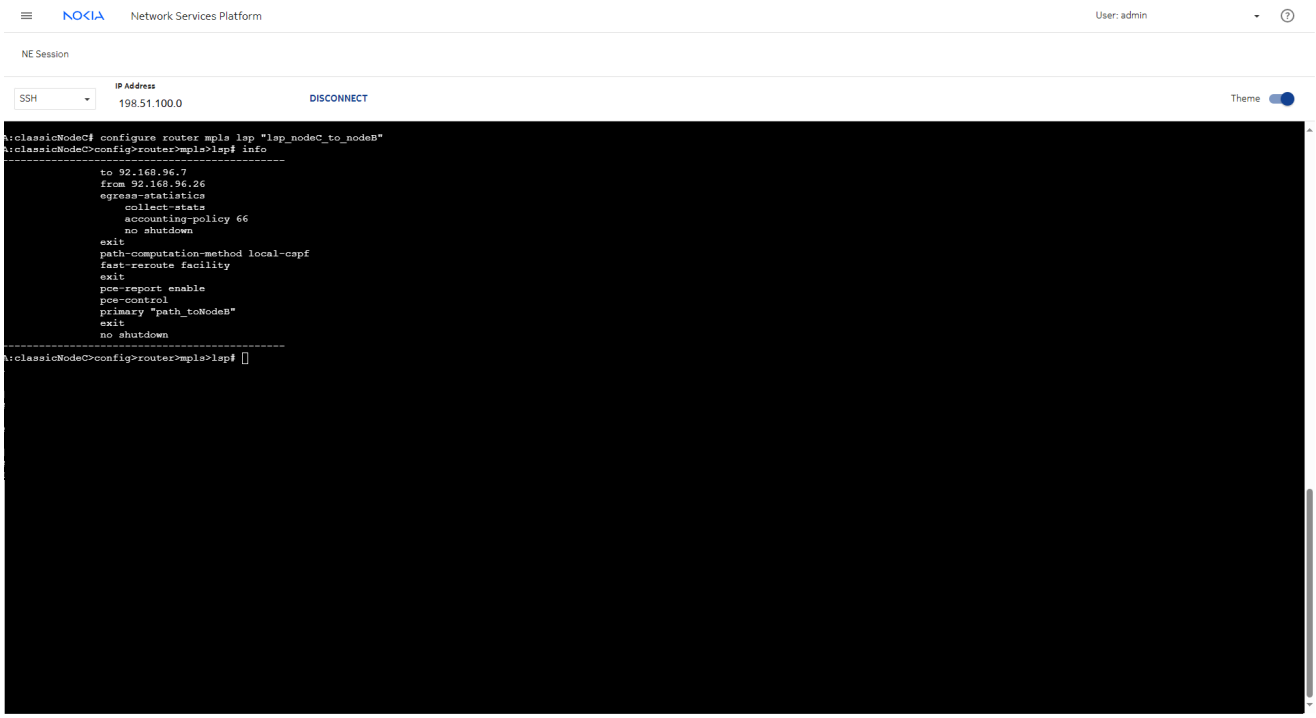
5.5.5 Verify the LSP parameters

1

LSPs must be configured on the NE. Opening an NE session will show us the configuration of the LSP in use by the SDP. It's called lsp_NodeC_to_nodeB.

We can see that an accounting policy is in place on the LSP, and collection of egress statistics is enabled. These are required for any LSPs we want to monitor for LSP Throughput reporting.

The account policy ID for this LSP is 66.



5.5.6 Verify statistics collection configuration

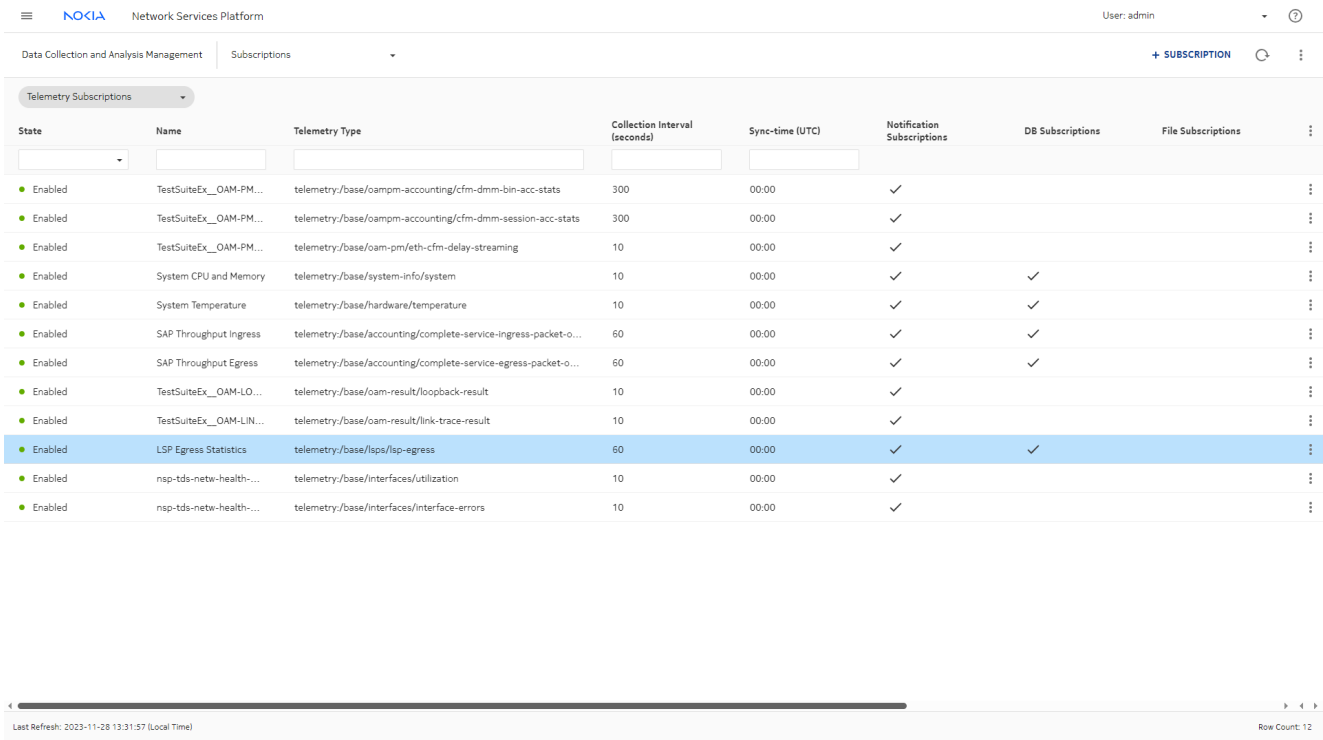
Now that we have verified that the service and LSP are configured, we can confirm that statistics collection has been set up.

1

In the **Data Collection and Analysis Management**, **Subscriptions** view, we can see that there is a subscription called LSP Egress Statistics.

The telemetry type is base/lsps/lsp-egress. The collection interval is 60 s, meaning that every minute the NSP will collect the statistics from the node.

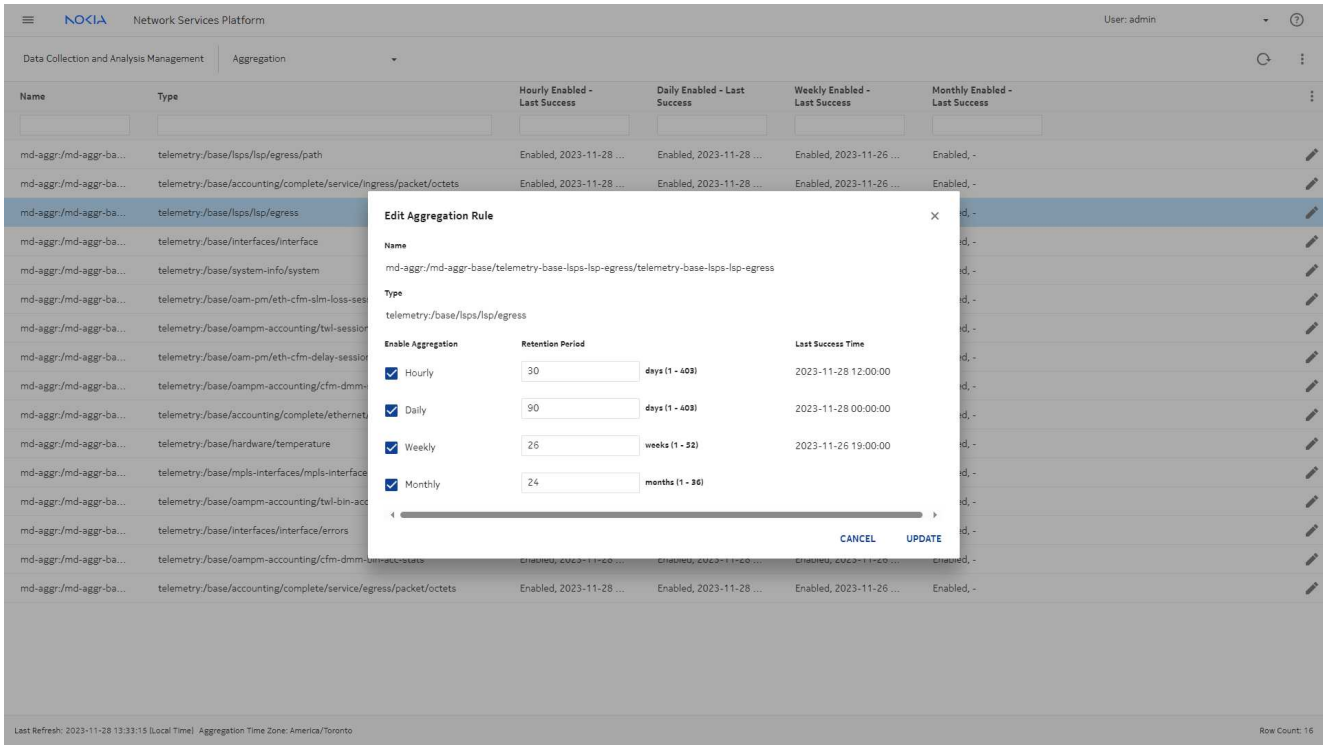
Most importantly, database subscriptions are enabled. Data is stored in the NSP auxiliary database and is available to Analytics.



2

The report we need creates forecasts based on aggregated data. Switching to the **Data Collection and Analysis Management**, **Aggregation** view, we'll take a look at the aggregation settings for the telemetry type. Select the telemetry type and click Edit.

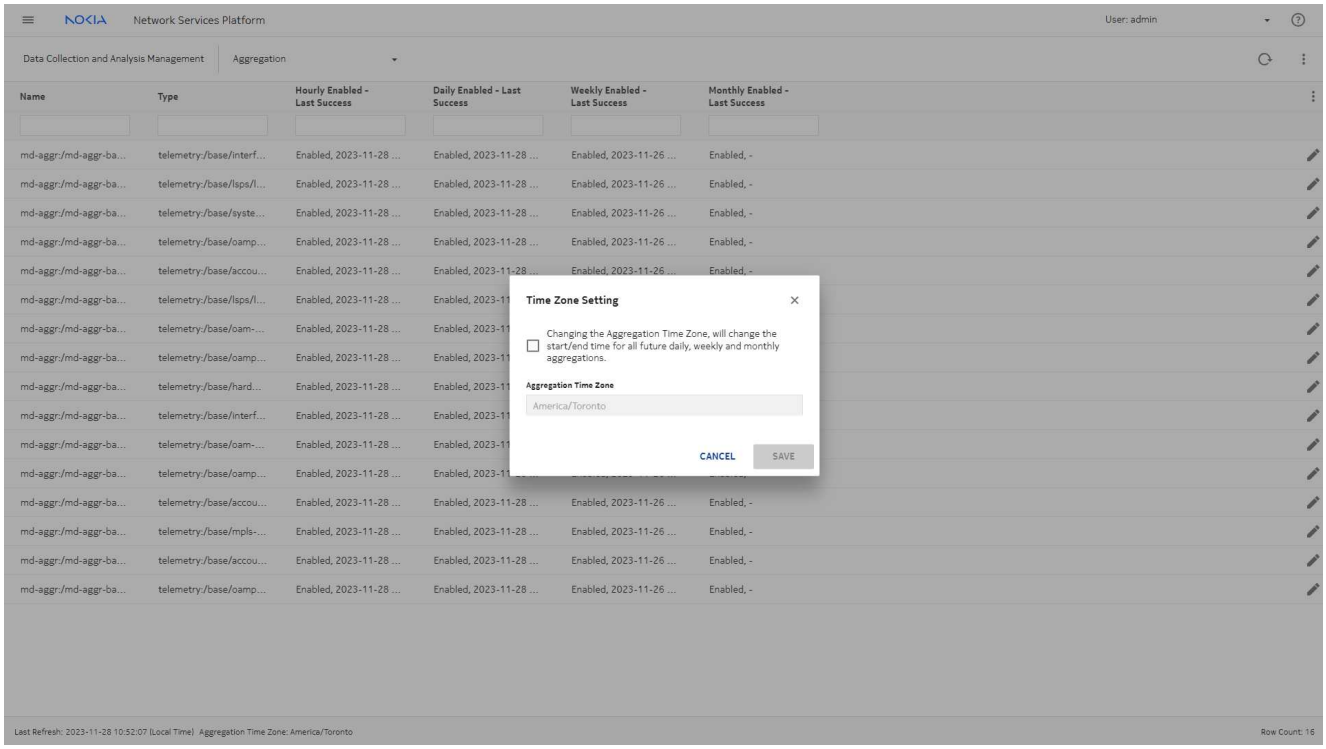
Here we see that all aggregation types are enabled, and the retention period is set for each. The Last Success Time can also be used to verify that the subscriptions are working. For example, the last success time for daily aggregation should not be longer than a day ago.



3

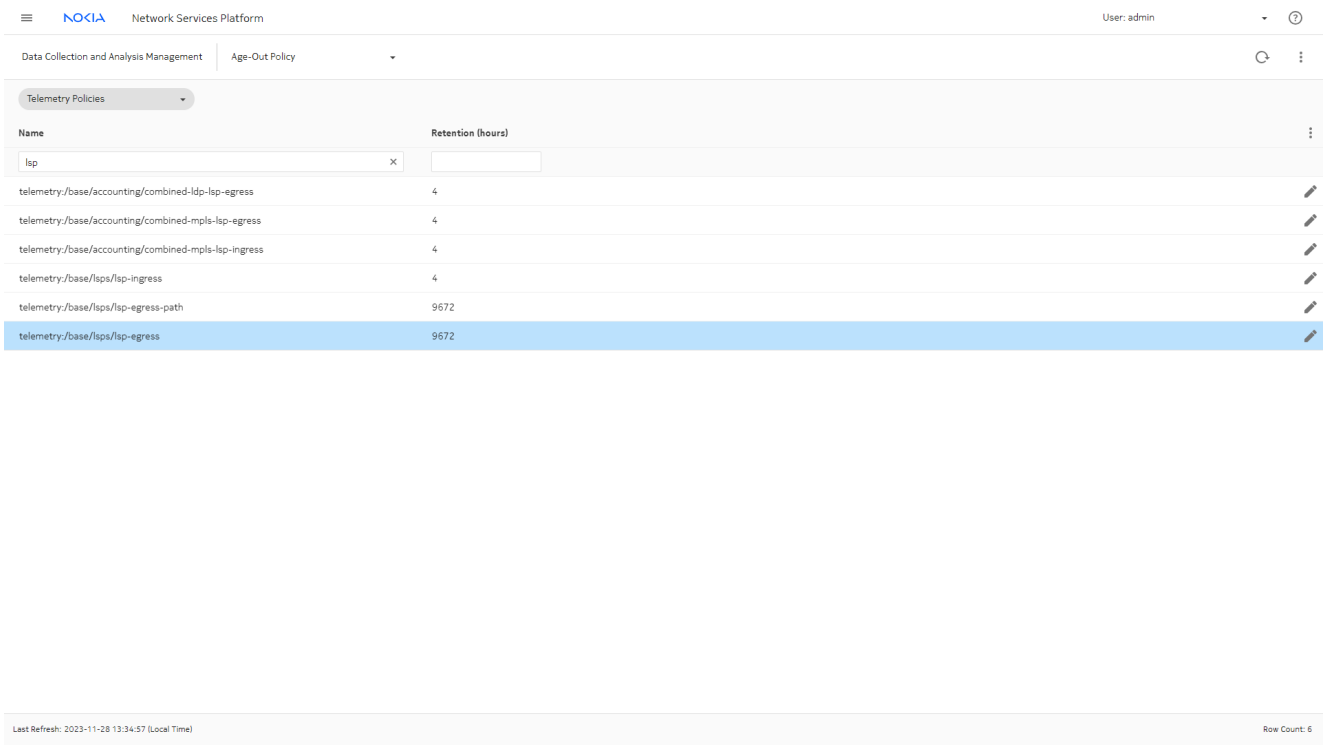
We also need to confirm that the aggregation time zone has been set correctly. If the aggregation time zone doesn't match the reporting time zone, Analytics will show an error when we try to generate an aggregated report. Click on the More Actions menu at the top of the page and select **Time Zone Setting**.

The time zone has been set to local time.



4

To generate a report using daily or monthly data, we need to ensure we have an appropriate retention policy for the telemetry type. Switching to the **Data Collection and Analysis Management**, **Age-Out Policy** view, we can see that the retention policy for the telemetry type has been set to the maximum.

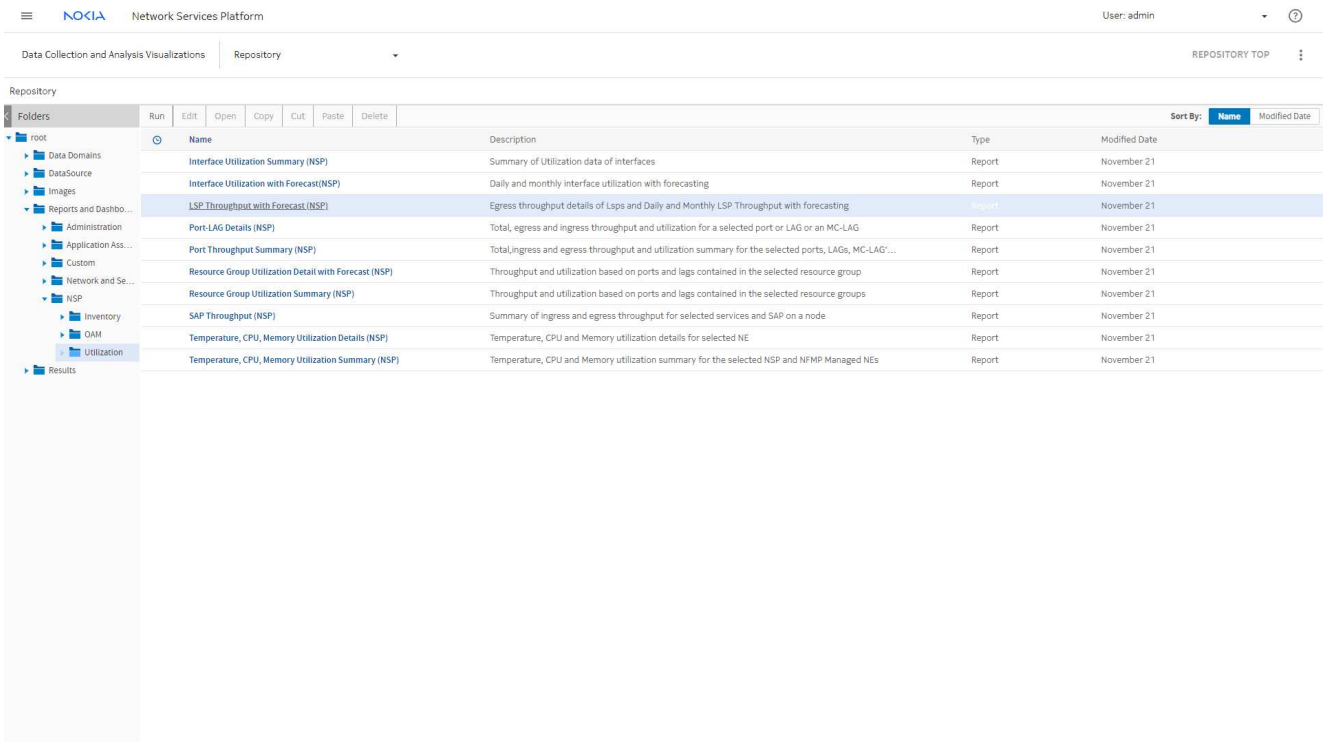


5.5.7 Generate the report in Analytics

Now that we've confirmed that all the prerequisites are in place, we can run the report.

1

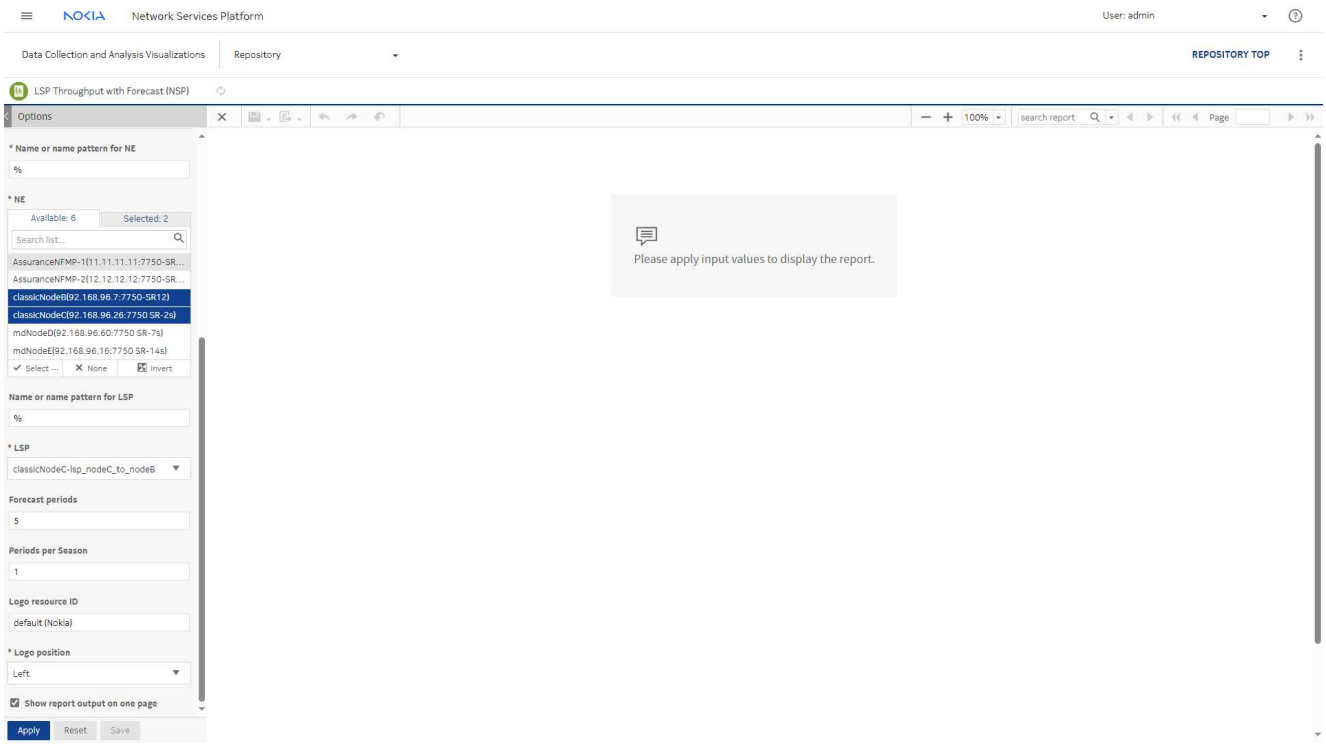
In the Analytics repository, the report we need is under Reports and Dashboards, NSP, Utilization. Navigate through the folders and choose LSP Throughput with Forecast (NSP).



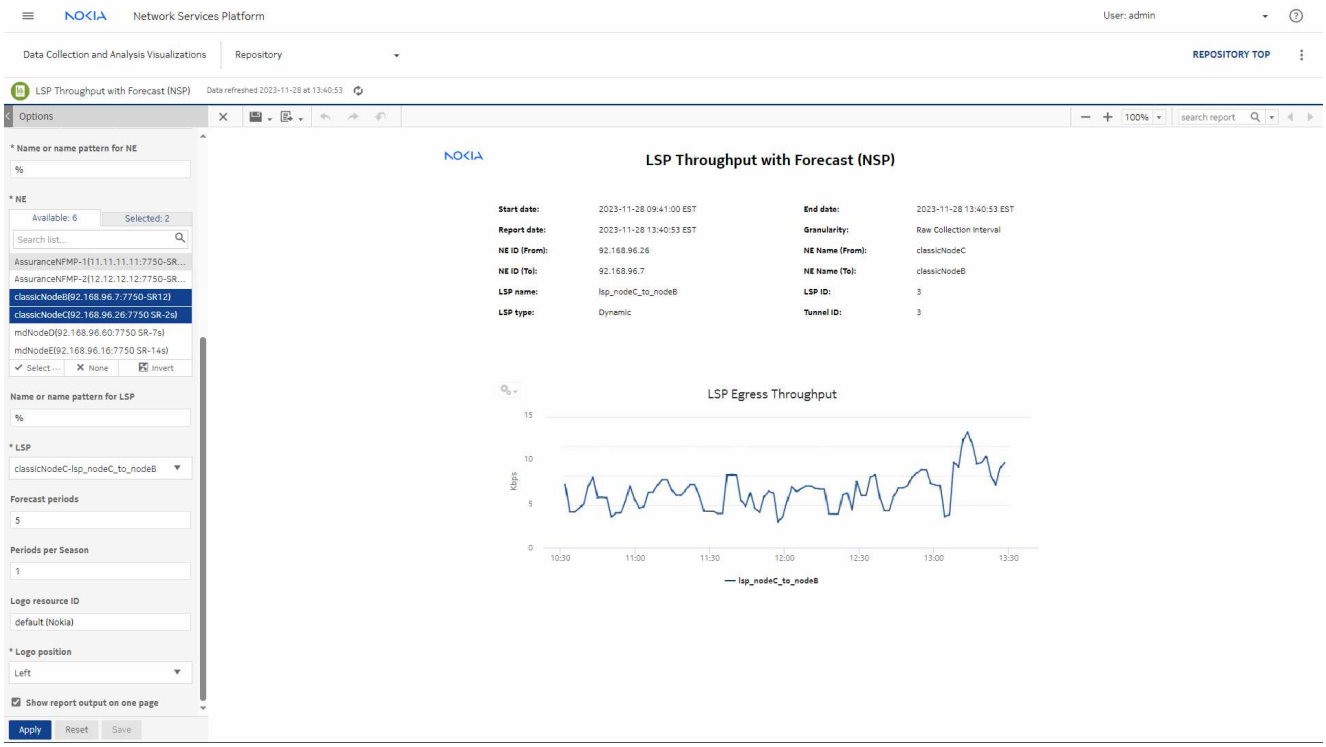
2

We'll start with a raw data report.

1. Select all the NE types.
2. In the NE list, choose NEs that host the service endpoints.
3. In the LSP field, choose the LSP between the two NEs.
4. Select the Show report output on one page check box.
5. Click Apply.



The report shows the raw LSP utilization data.



3

Next, we'll re-run the report on daily aggregated data. When you run this report with daily or monthly aggregation, a forecast is provided.

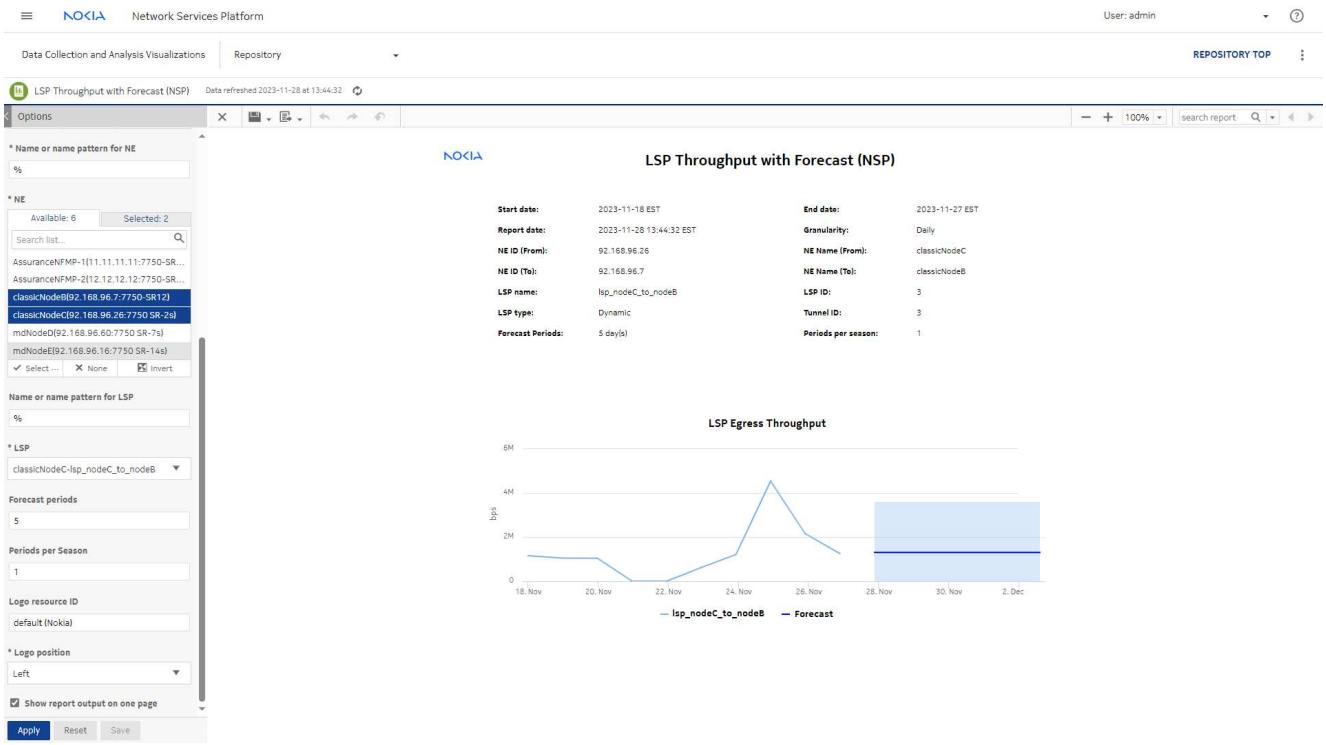
We'll set the report range to 10 days, the forecast periods to 5 and the periods per season to 1.

Periods per season refers to the number of aggregations you want to track to see a repeating pattern. For example, to see a weekly pattern with daily aggregation, you would set Periods per season to 7. Setting this to one means we expect traffic to be similar from one day to the next.

To generate a forecast, you must provide at least two seasons of data, although more may be required if the input data is not linear. For example, if you choose a periods per season value of 7 and the granularity is daily, you must use a report range of at least 14 days.

4

View the report.



This report shows the 10 days of collected data and 5 days of forecasting based on that data. The blank space on the graph indicates that data hasn't been aggregated yet for the current date.

After the current date is the forecasted data. The shading shows the upper and lower range of the predicted throughput, and the line shows the expected throughput value for the next five days.

5.6 SAP Throughput reporting scenario

5.6.1 Purpose

The SAP Throughput (NSP) report shows throughput by a specified service and SAPs. The SAP Throughput (NSP) report includes throughput data for NEs managed by the NFM-P only, MDM (model-driven) only, or NFM-P+MDM-mediated NEs. The default display is a set of time series graphs, showing ingress, egress and total throughput.

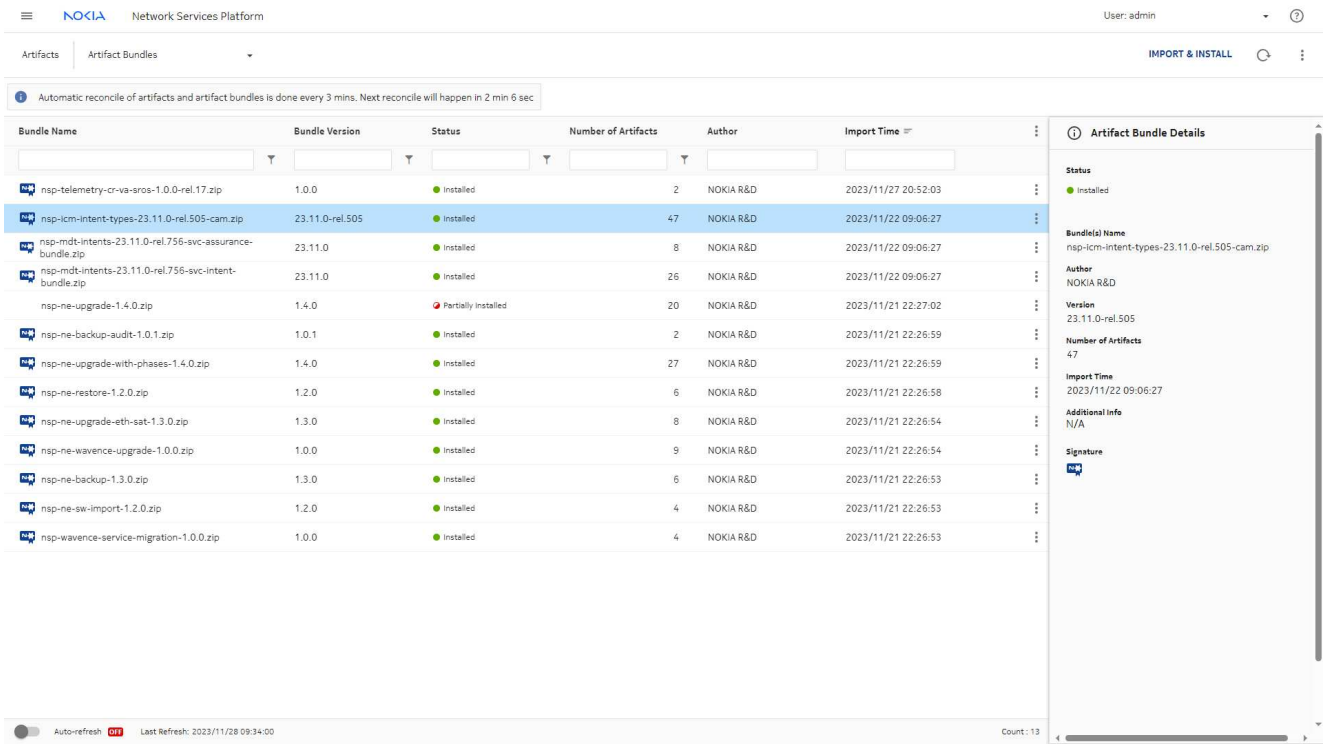
This process shows how to set up a service for SAP Throughput reporting in Analytics.

5.6.2 Confirm that prerequisites for service provisioning are completed

1

Two intent type bundles are required for provisioning our service, and for setting up QoS and telemetry: icm-intent-types, and mdt-intents.

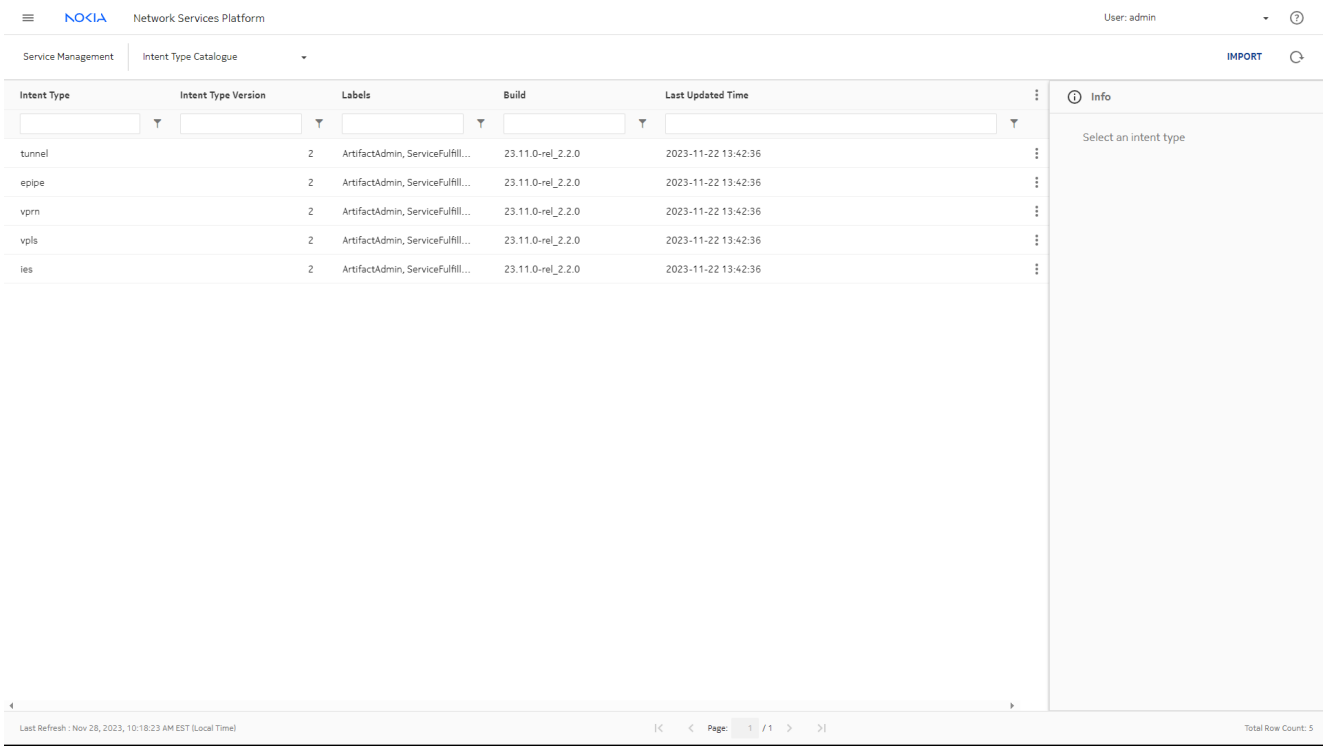
Checking the **Artifacts**, **Artifact Bundles** view shows that both bundles are in Installed status.



2

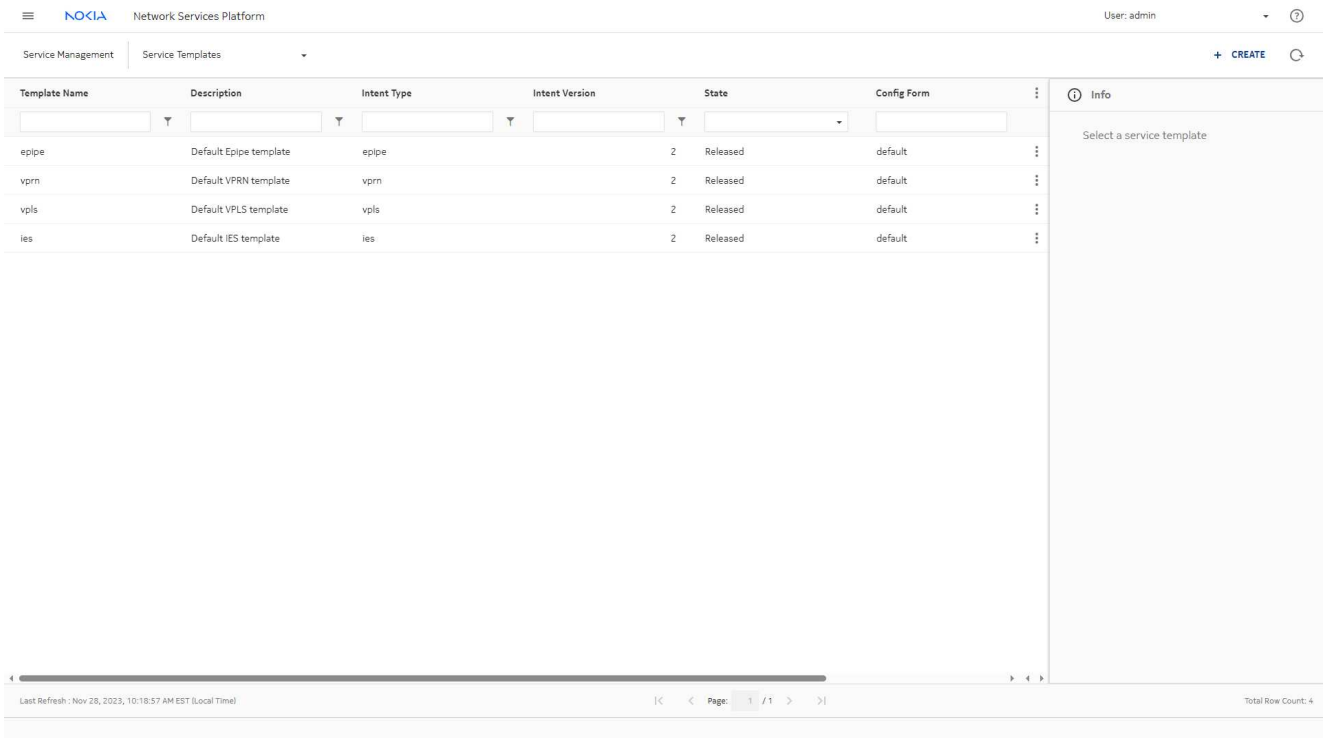
NSP installs the intent types to Network Intents, from which they can be imported to Service Management.

Checking the **Service Management**, **Intent Type Catalogue** view shows that the intent types have been imported and are available for use in Service Management.



3

Switching to the **Service Management**, **Service Templates** view shows that the intent types have been used to create templates for various service types.

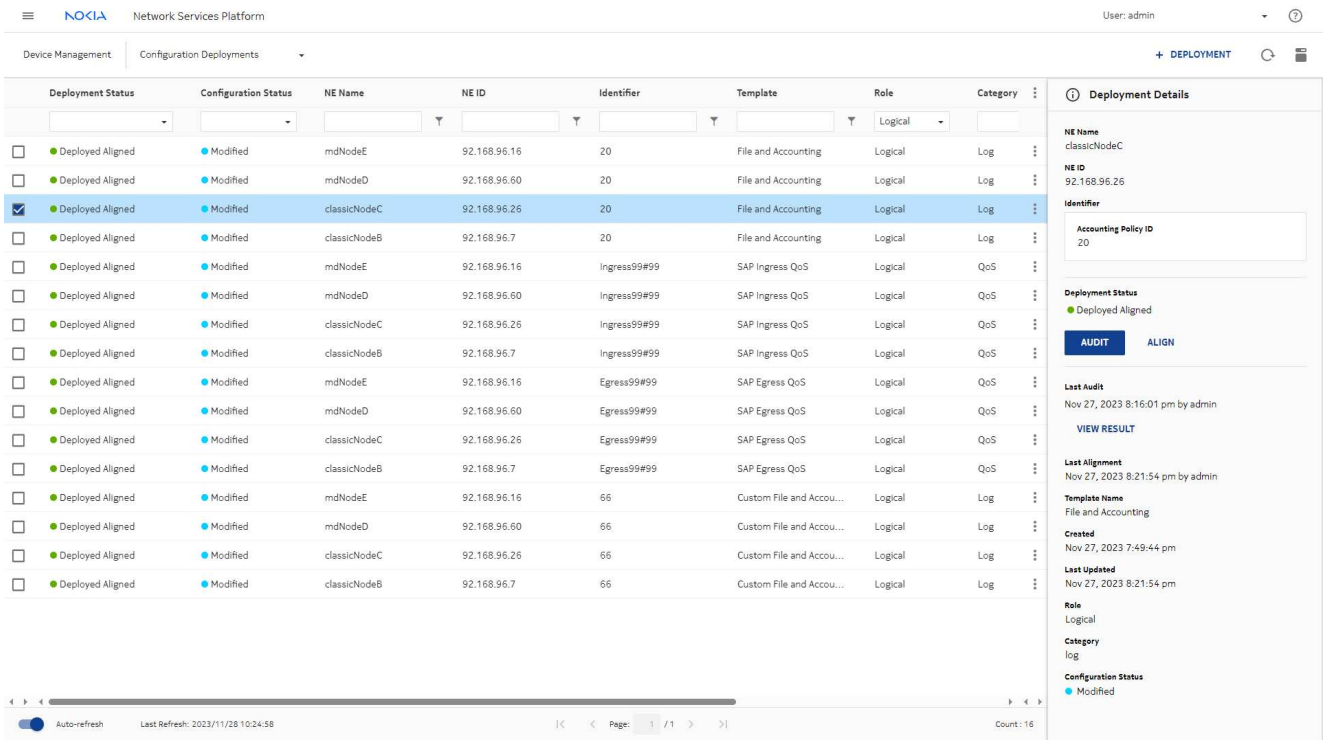


5.6.3 Verify policy configuration

1

To collect statistics on an NE, a file and accounting policy must be configured on the NE. This can be done by deploying a template in the **Device Management**, **Configuration Deployments** view.

In the Configuration Deployments list, we can see that a template called File and Accounting has been deployed on the NE and the Deployment Status is Deployed Aligned. The policy identifier is 20.



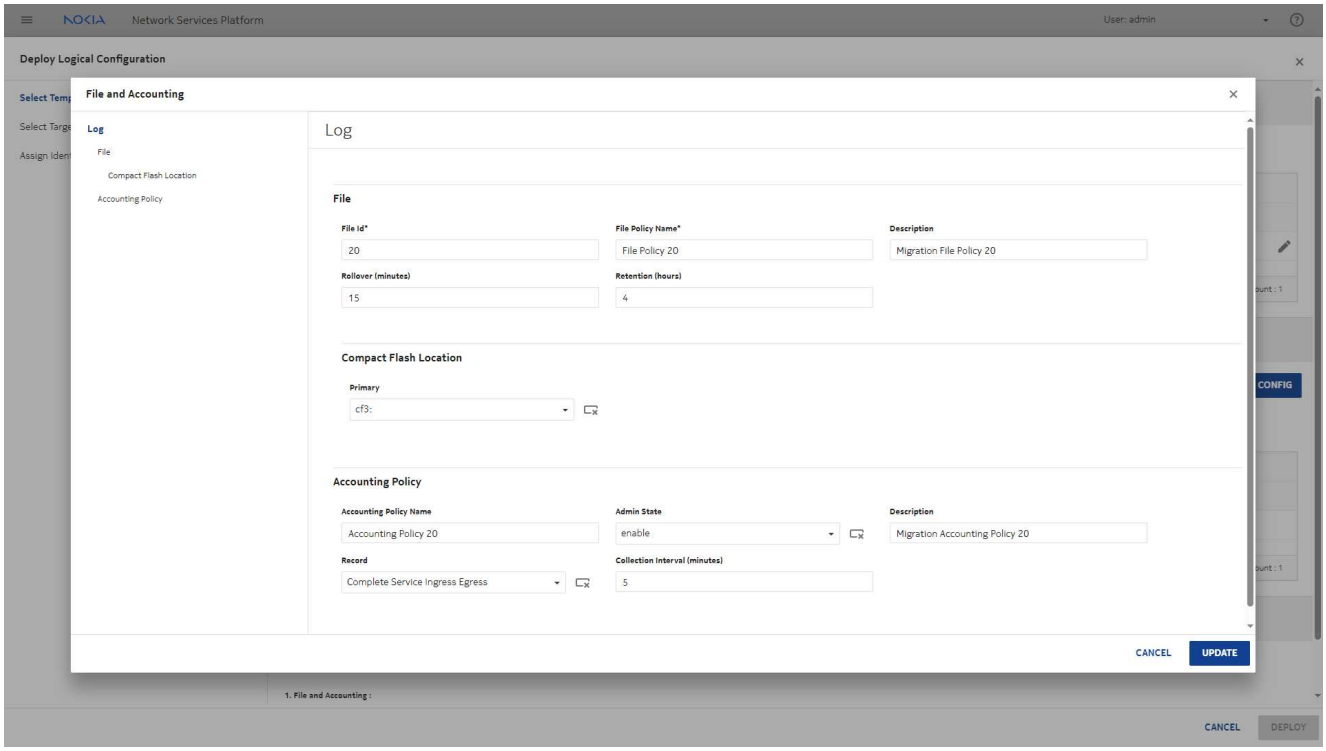
2

We can view the template details to see policy details:

1. Select the deployment and choose View/Edit from the Table row actions menu.
2. In the form that opens, click **VIEW/EDIT TEMPLATE CONFIG**.

The template information shows the rollover duration, or how long a statistics collection file remains open before a new file is started, the retention period for the file, and the compact flash location where the file is stored.

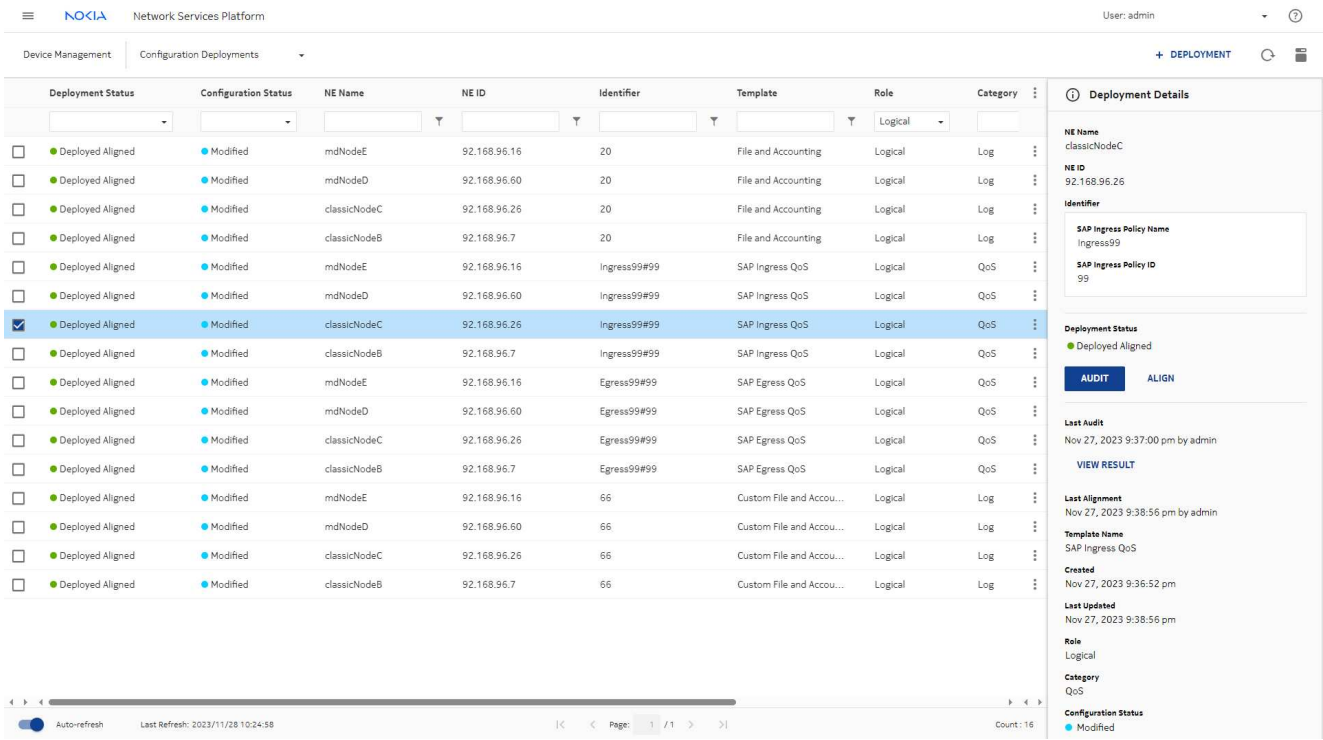
Accounting policy details show that the policy applied is number 20, and it will be collecting Complete Service Ingress Egress statistics. The collection interval is 5 min, meaning that every 5 min the NSP will collect the statistics from the node and save them to the database.



3

Additionally, there are egress and ingress QoS policies deployed, which allows traffic shaping and to prioritize certain types of traffic.

The ingress QoS policy identifier is Ingress99#99.

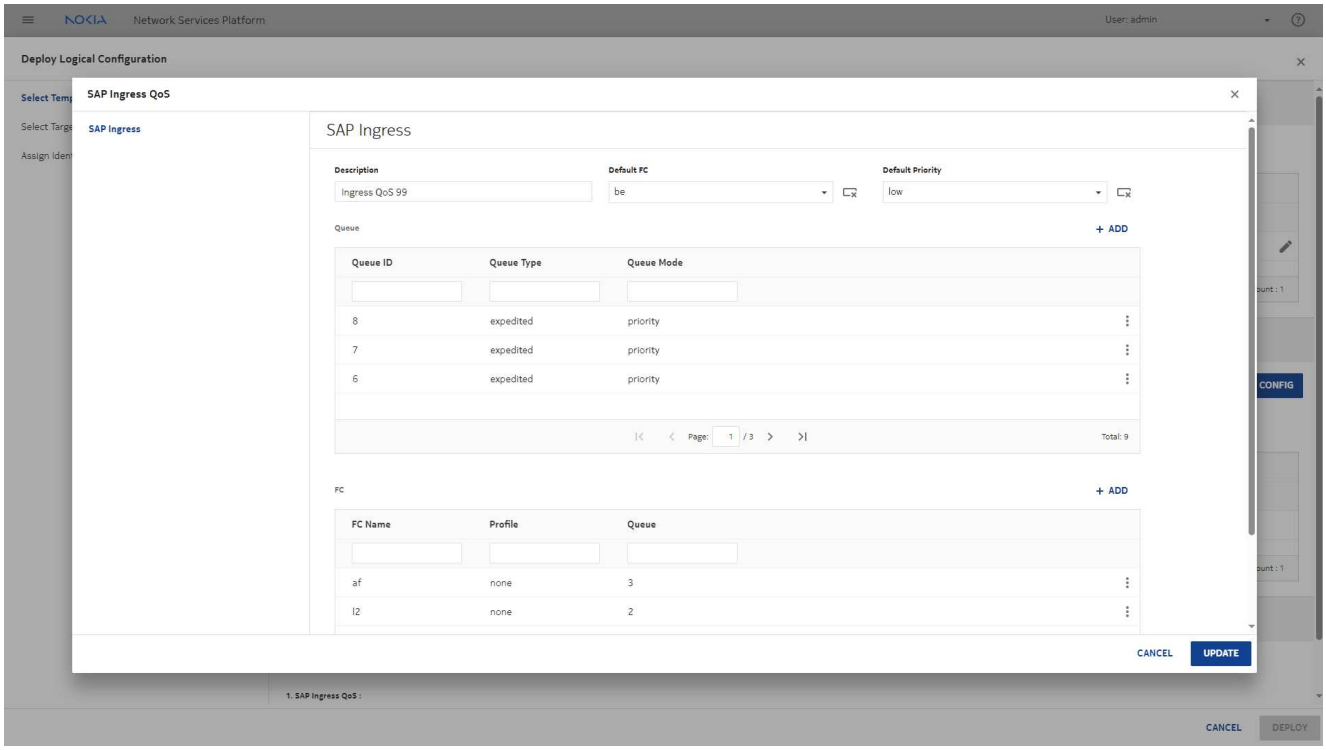


4

We'll view the ingress template details as an example:

1. Select the deployment and choose View/Edit from the Table row actions menu.
2. In the form that opens, click **VIEW/EDIT TEMPLATE CONFIG**.

There are a total of nine queues configured. The three that display on this page have been configured as expedited queues with high priority. At the bottom of the form, we can see two of the forwarding classes.

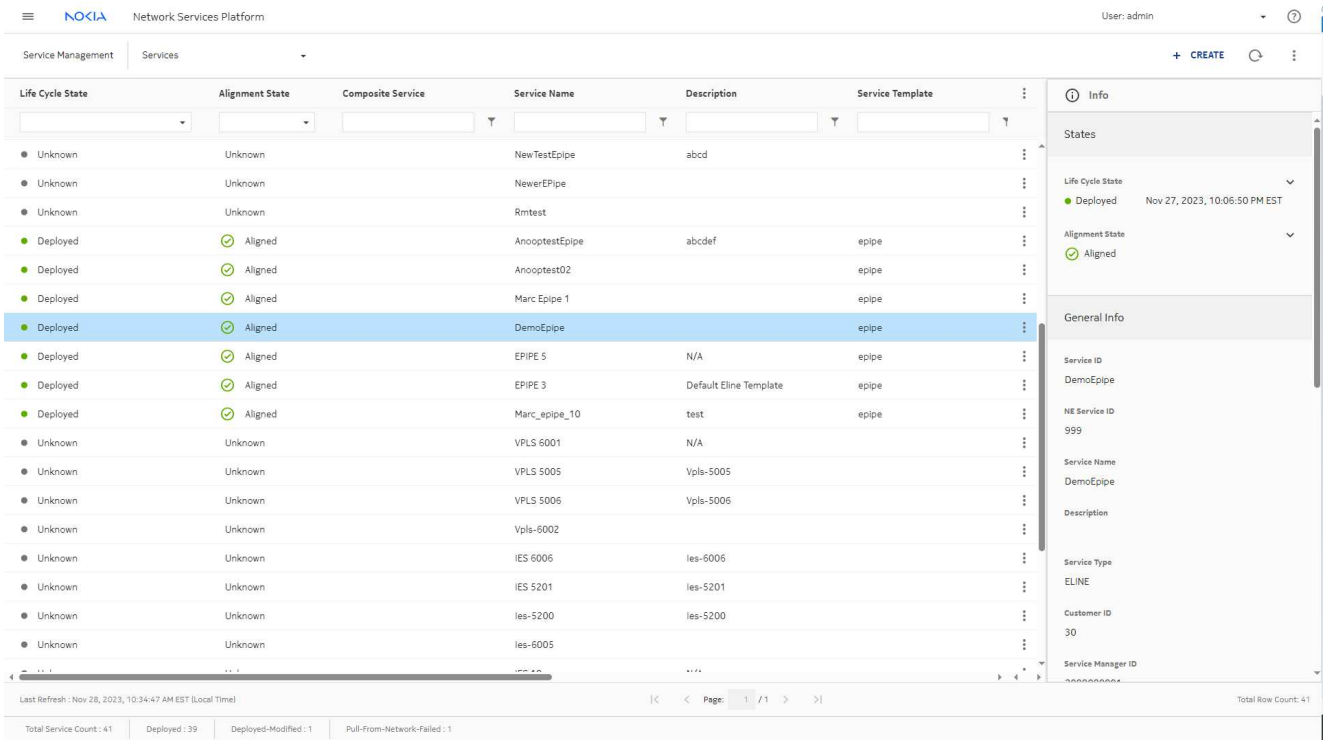


Policers have also been applied directly to the NEs.

5.6.4 Verify the service parameters

1

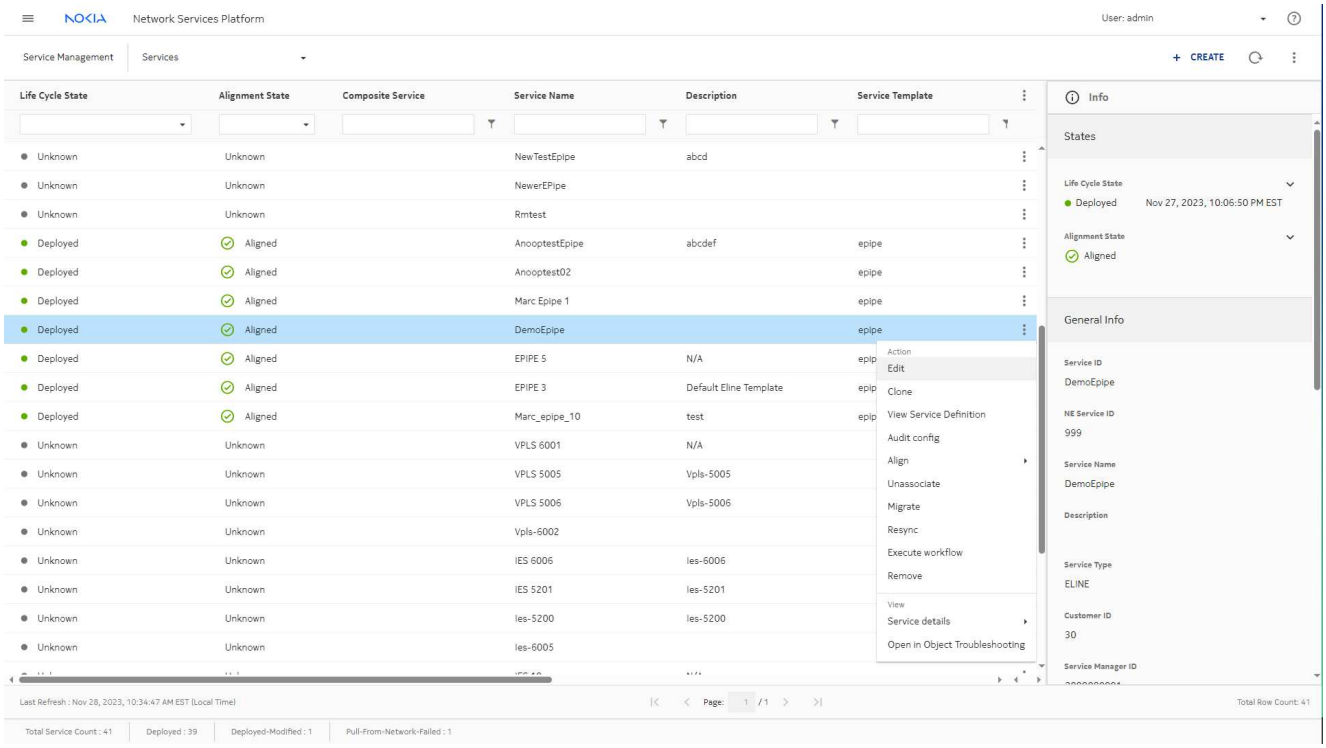
In the **Service Management**, **Services** view, we can see the provisioned services.



2

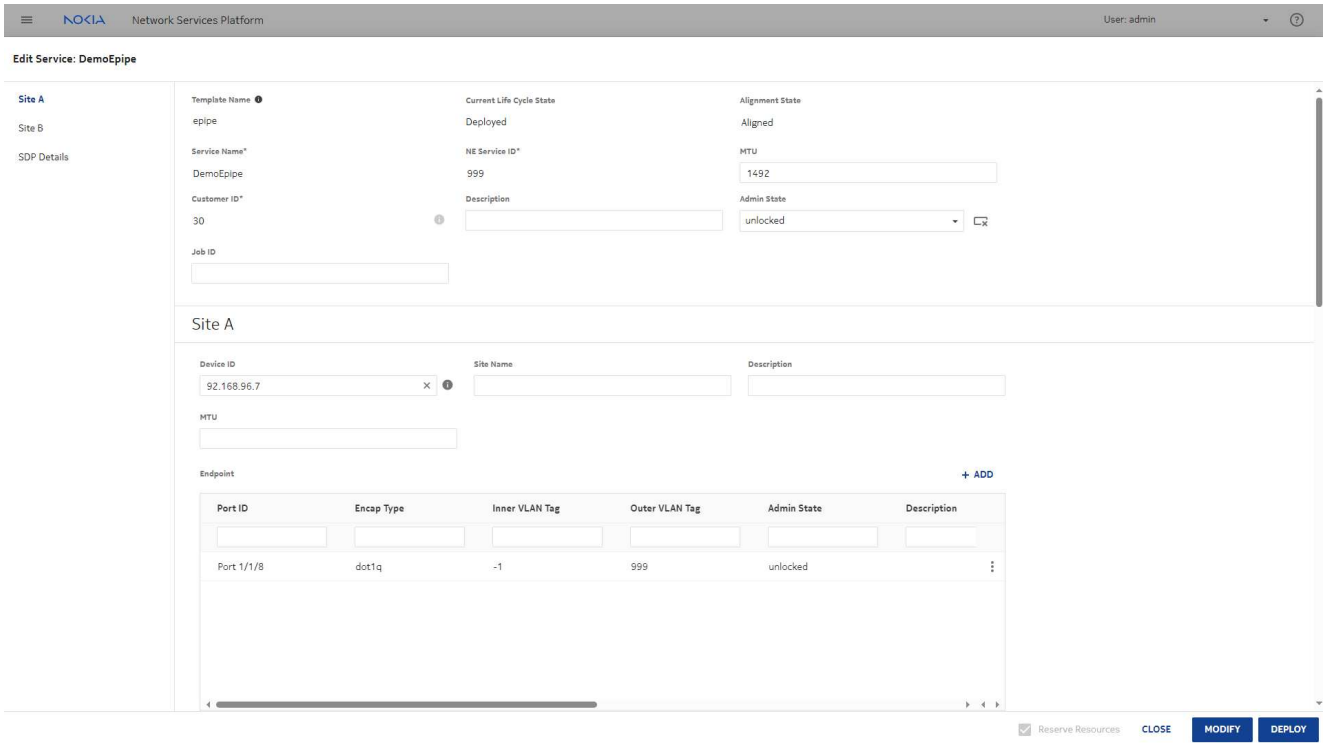
DemoEpipe is Deployed and Aligned.

Opening the Edit form for the service will let us verify that everything we'll need is in place. Select the service and select Edit from the Table Row actions menu.



3

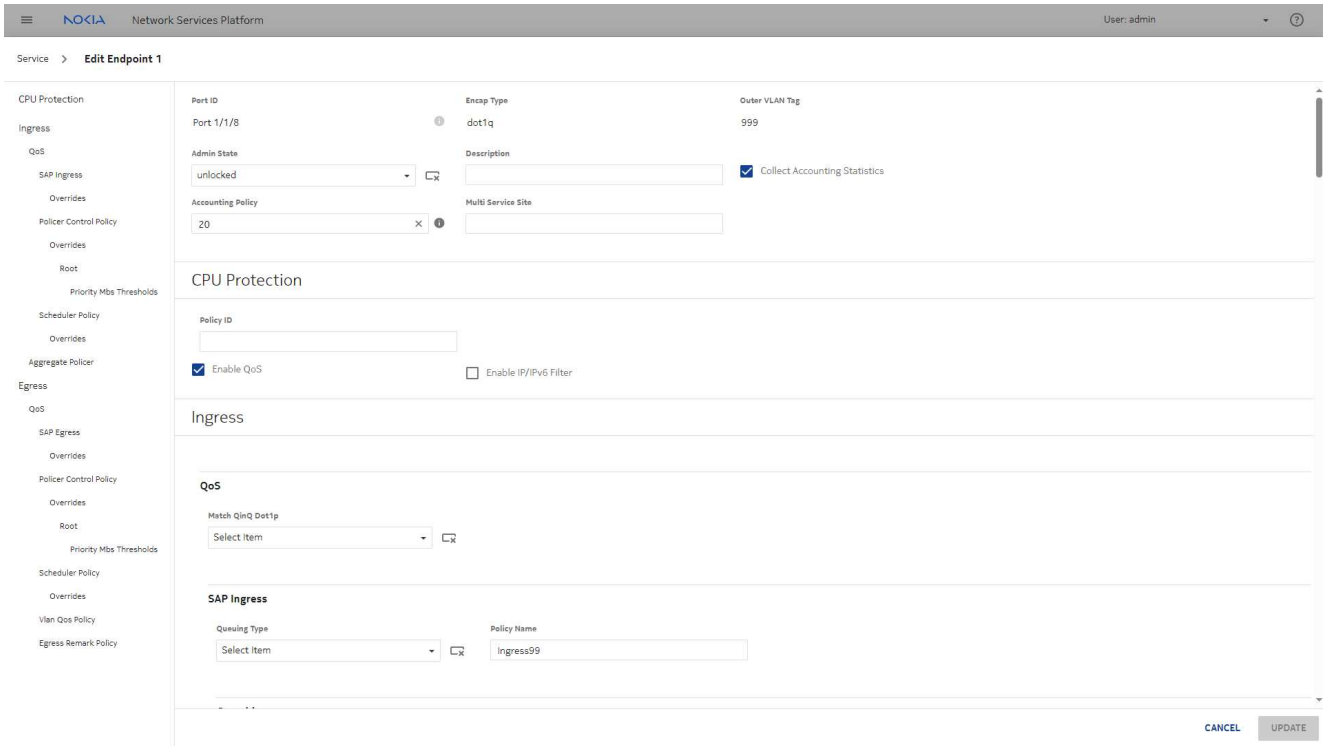
The Edit service form shows the basic service parameters such as service name and customer ID, and the service endpoints.



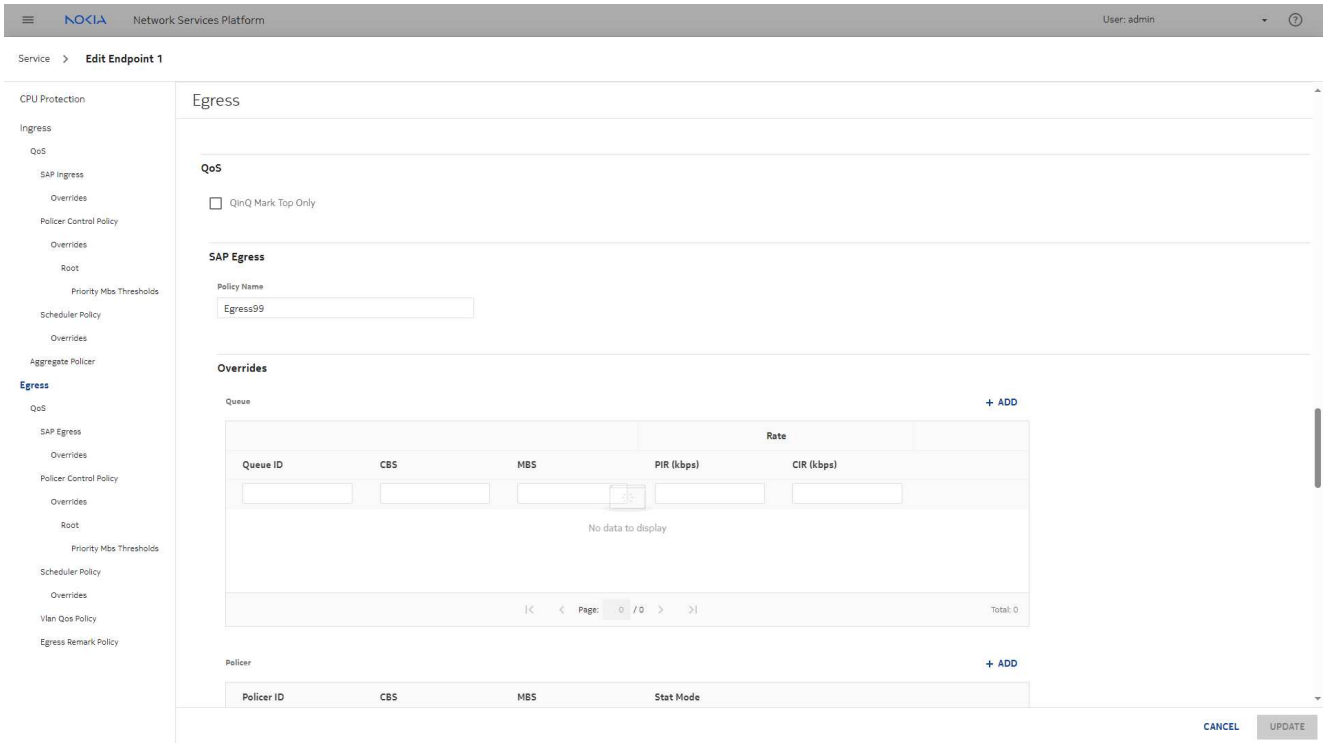
4

Site A of the service is on port 1/1/8. Select the endpoint and choose Edit to verify the endpoint parameters.

In the Edit Endpoint form, we can see that accounting statistics collection and QoS have been enabled, and the policies and overrides that have been applied. The accounting policy is 20, and the SAP Ingress policy is Ingress99: the policies we verified in the device management views.

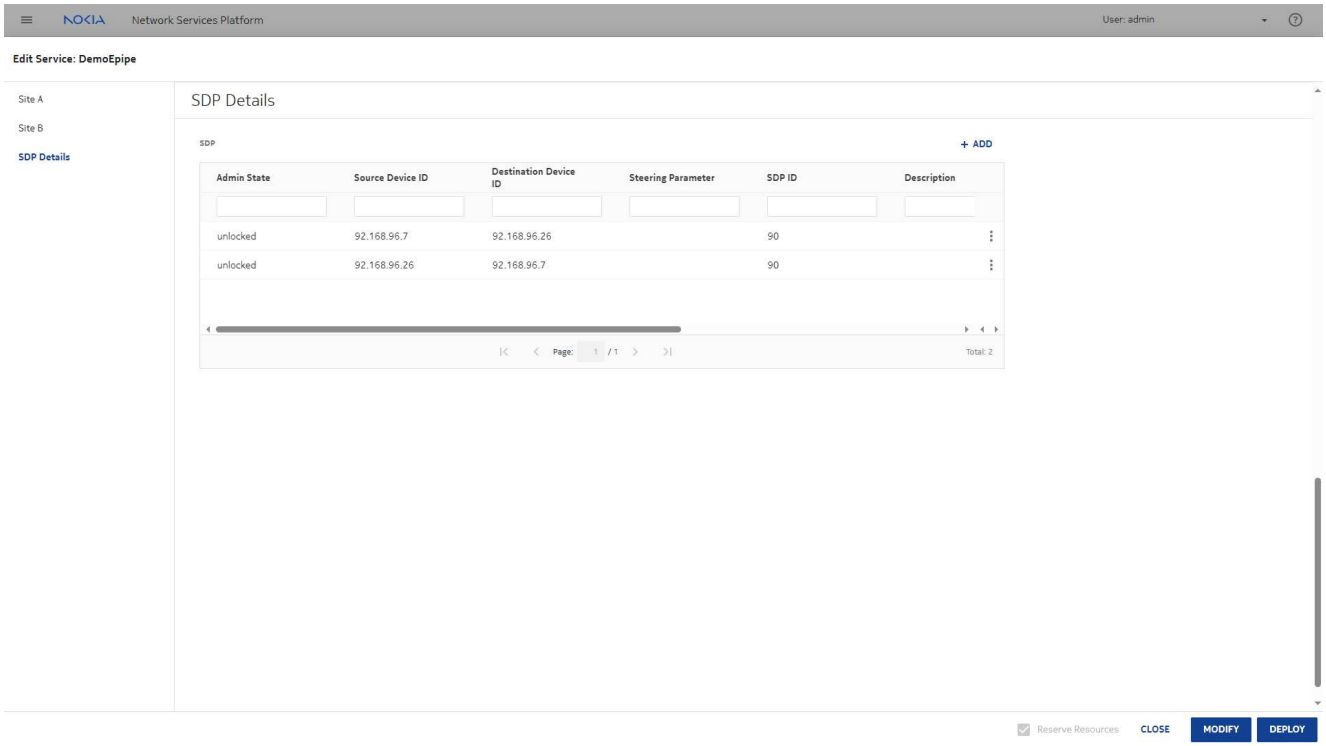


Scroll down to see the egress settings: the egress policy is Egress99.



5

Returning to the Edit Service form, we can see the SDP details, the service destination points. An SDP has been added to the service for each direction.



5.6.5 Verify statistics collection configuration

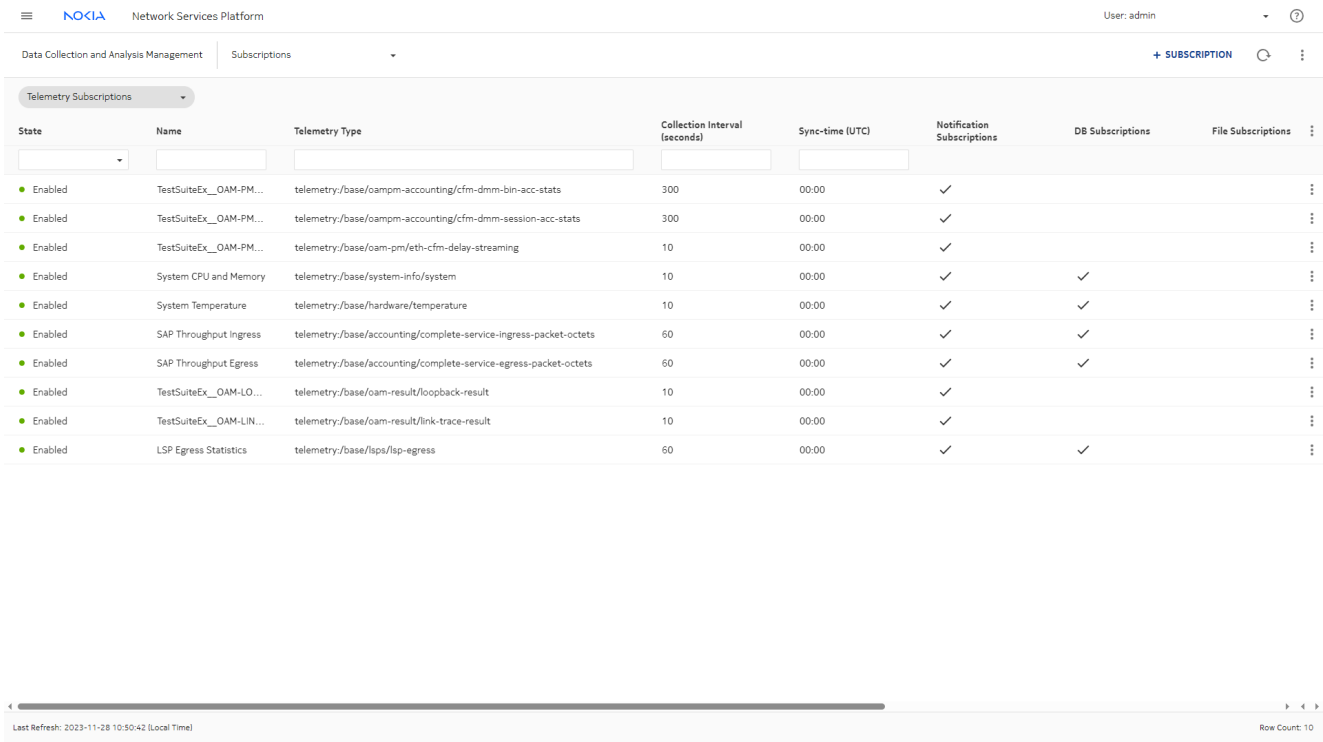
Now that we have verified that the service is configured, we can confirm that statistics collection has been set up.

1

For the report we need to generate, we need to collect statistics for two telemetry types: base/accounting/complete-service-ingress-packet-octets and base/accounting/complete-service-egress-packet-octets.

In the **Data Collection and Analysis Management**, **Subscriptions** view, we see that subscriptions have been configured and enabled for each. The collection interval is 60 s, meaning the data will be collected by NSP every minute.

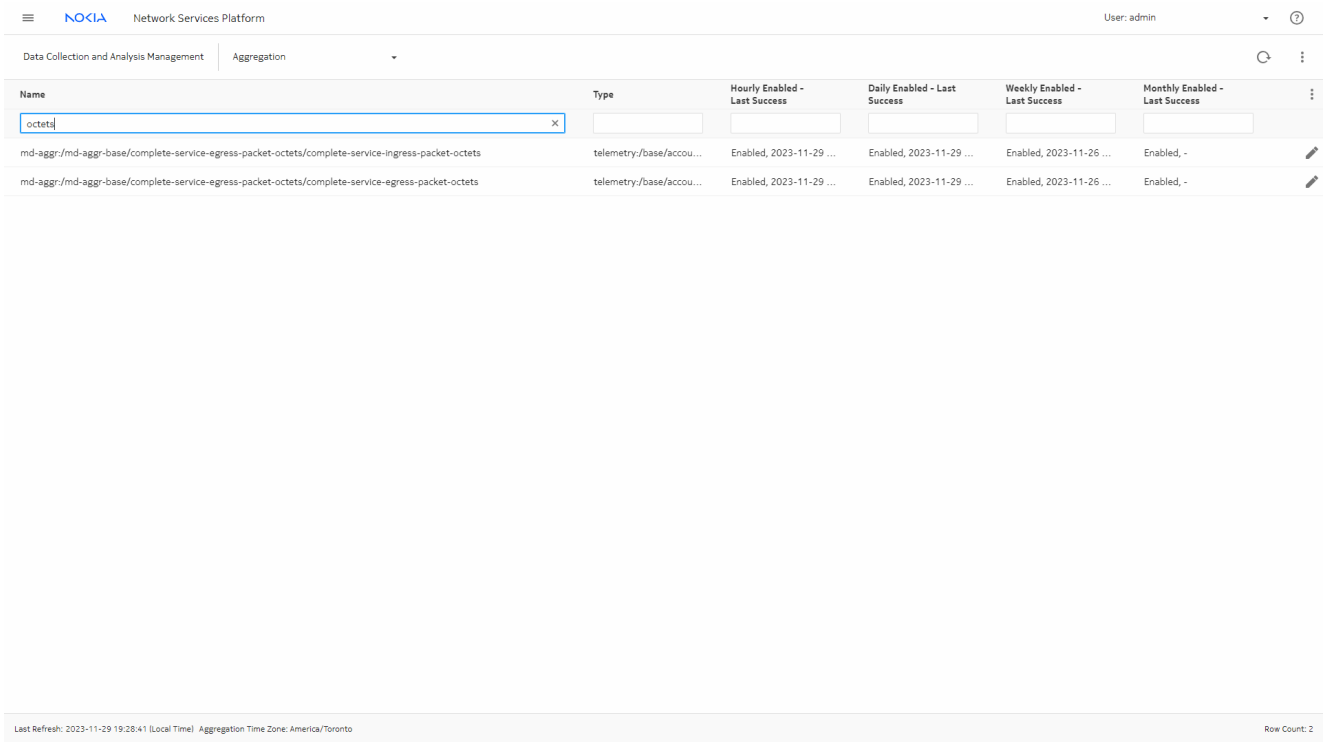
Database subscriptions are enabled: this will make the historical data available to Analytics.



2

The report we need also reports based on aggregated data. Switching to the **Data Collection and Analysis Management**, **Aggregation** view, we'll take a look at the aggregation settings for the telemetry types.

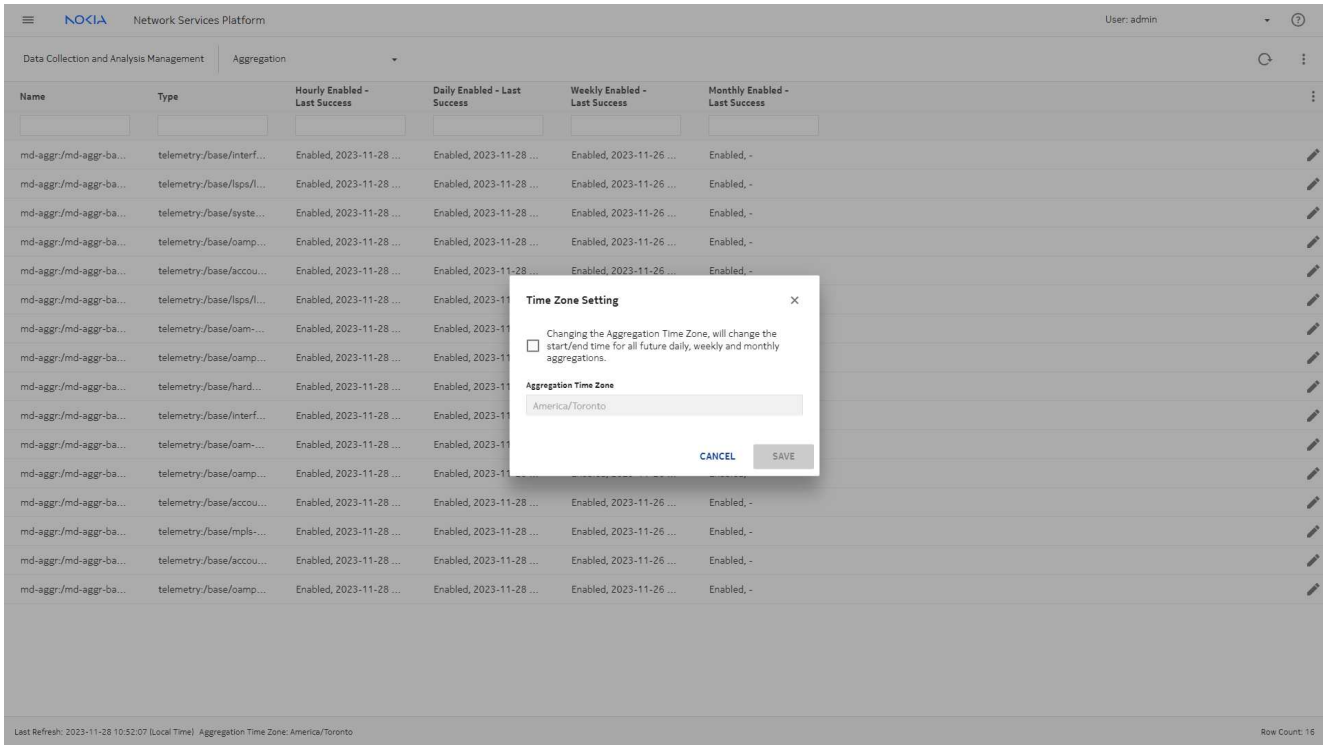
Here we see that all aggregation types are enabled for the telemetry types of interest. The Last Success Time can also be used to verify that the subscriptions are working. For example, the last success time for daily aggregation should not be longer than a day ago.



3

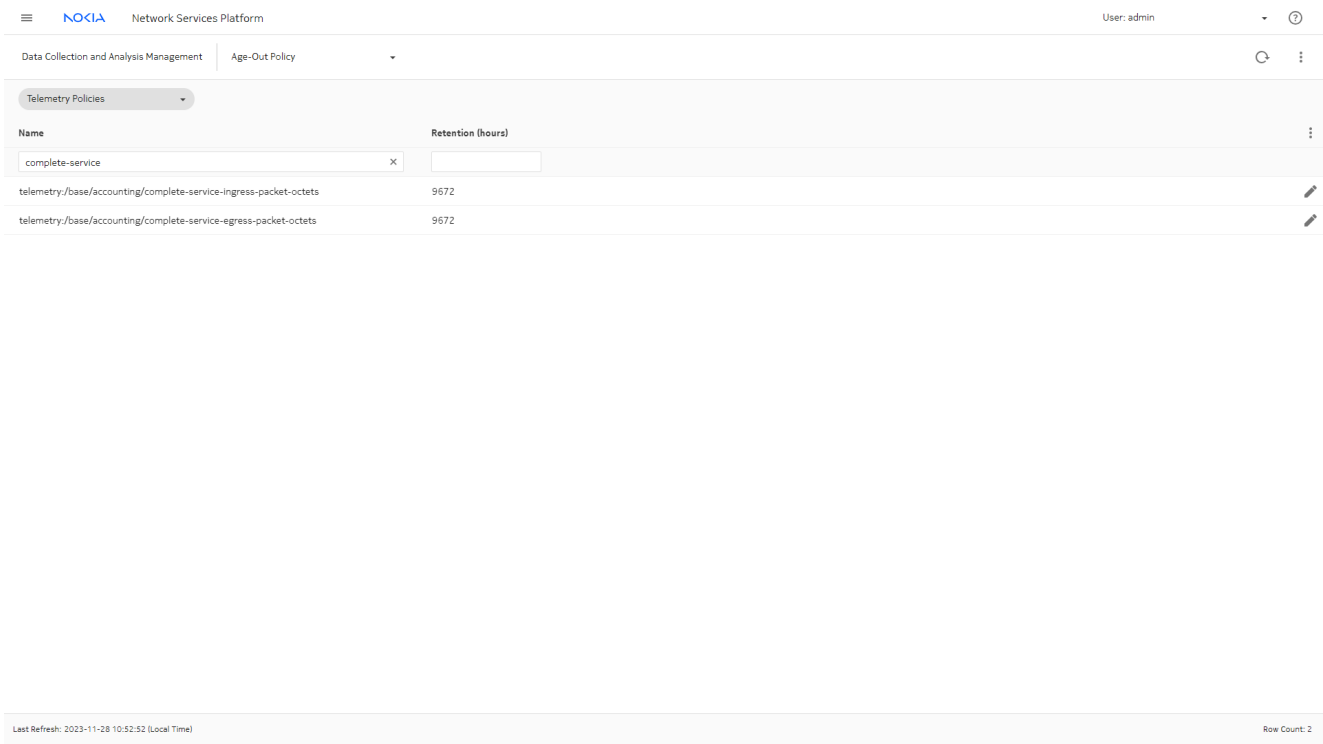
We also need to confirm that the aggregation time zone has been set correctly. If the aggregation time zone doesn't match the reporting time zone, Analytics will show an error when we try to generate an aggregated report. Click on the More menu at the top of the page and select **Time Zone Setting**.

The time zone has been set to local time.



4

To generate a report using daily or monthly data, we need to ensure we have an appropriate retention policy for the telemetry type. Switching to the Age-Out Policy list, we can see that the retention policy for the telemetry types have been set to the maximum.

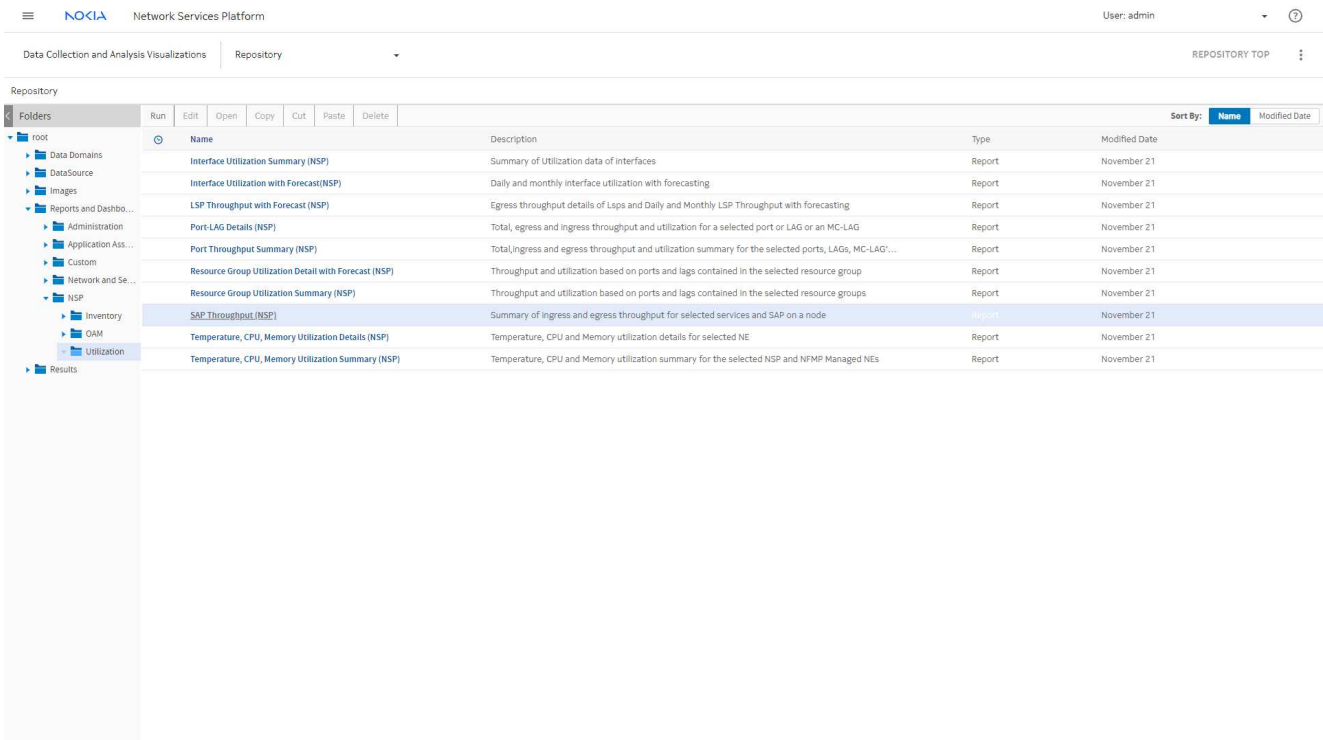


5.6.6 Generate the report in Analytics

Now that we've confirmed that all the prerequisites are in place, we can run the report.

1

In the Analytics repository, the report we need is under Reports and Dashboards, NSP, Utilization. Navigate through the folders and choose SAP Throughput (NSP).

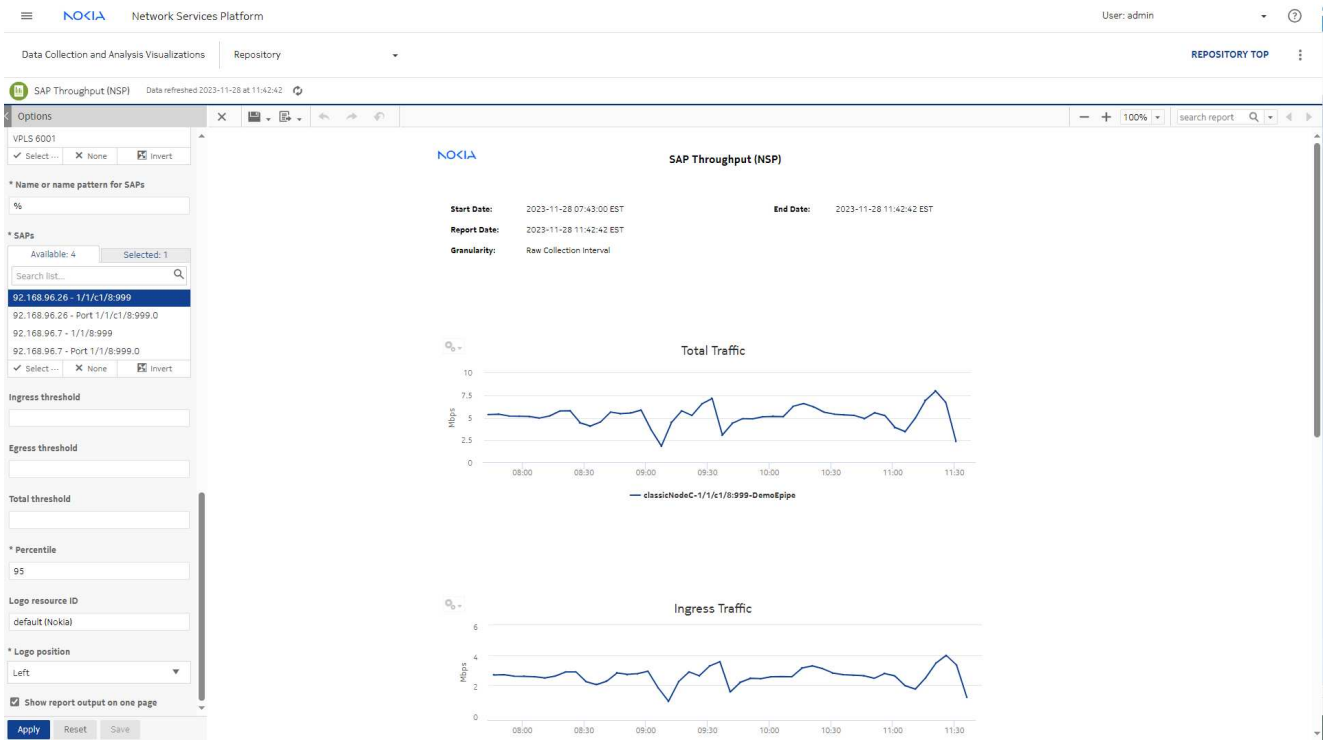


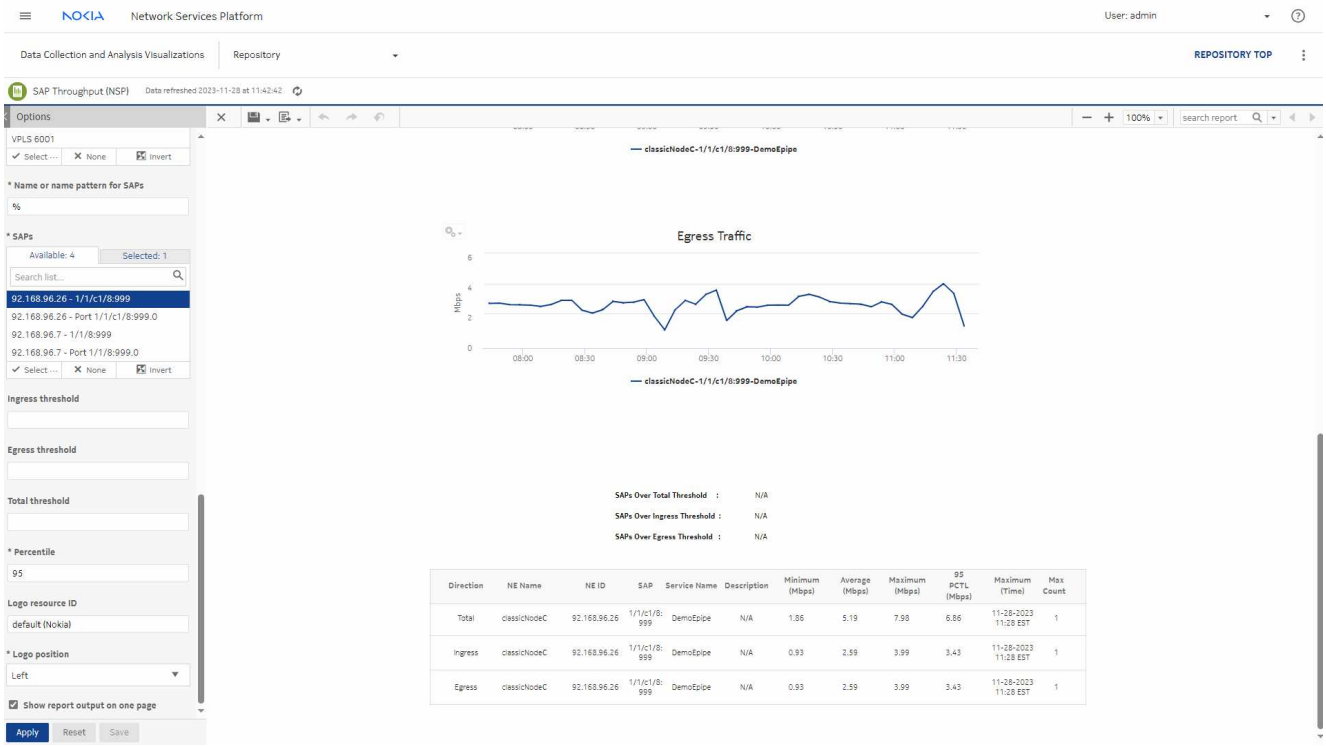
2

We'll start with a raw data report.

1. Select all the NE types.
2. In the NE list, choose NEs that host the service endpoints.
3. Choose a customer, a service, and one or more SAPs.
4. Select the Show report output on one page check box.
5. Click Apply.

The report shows the raw SAP utilization data.



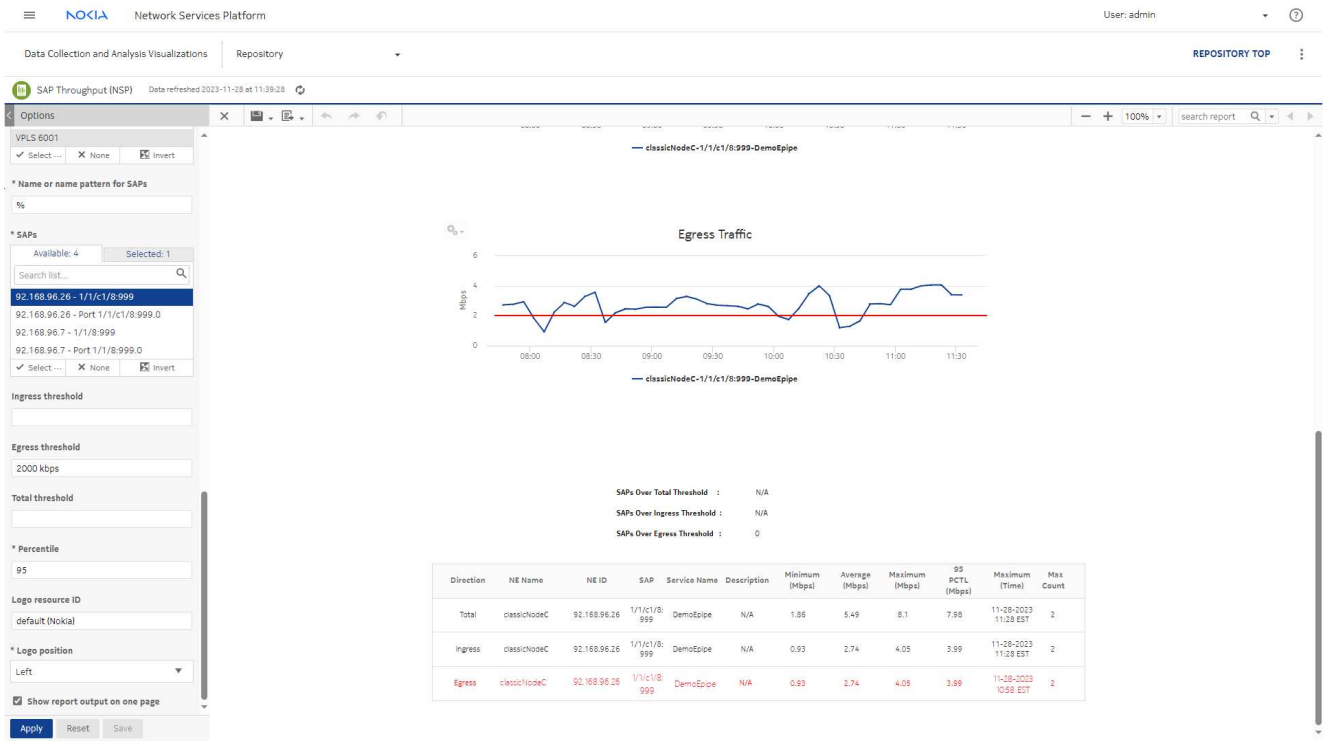


3

Next, we'll re-run the report with a threshold. A threshold helps to visualize whether traffic is exceeding expected values.

For example, we'll set an egress threshold of 2 000 kbps.

The report shows the threshold level on the graphs. If the average throughput rate exceeds the threshold, the table shows the values in red.



5.7 End-to-end NE troubleshooting scenario

5.7.1 Purpose

This process shows you how to use NSP in troubleshooting issues on NEs.

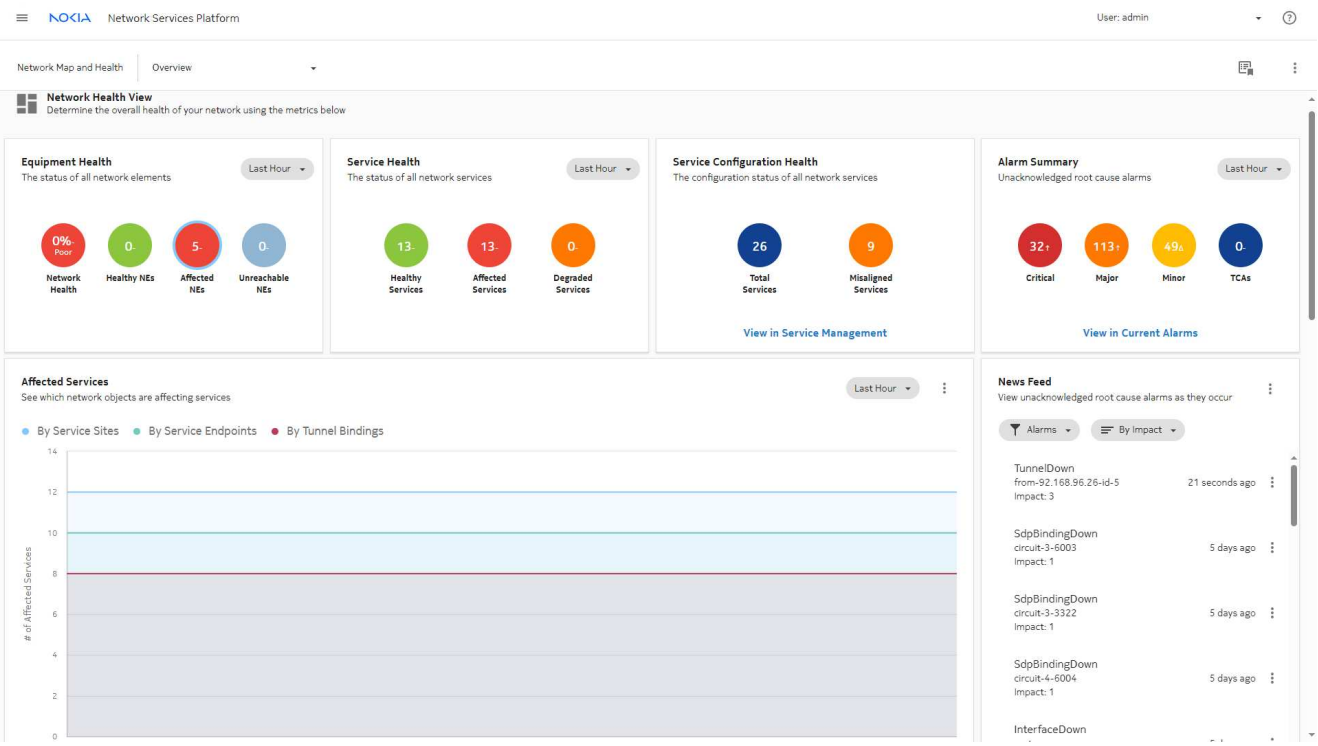
In this scenario, an NE is experiencing problems.

5.7.2 View affected equipment related resources

1

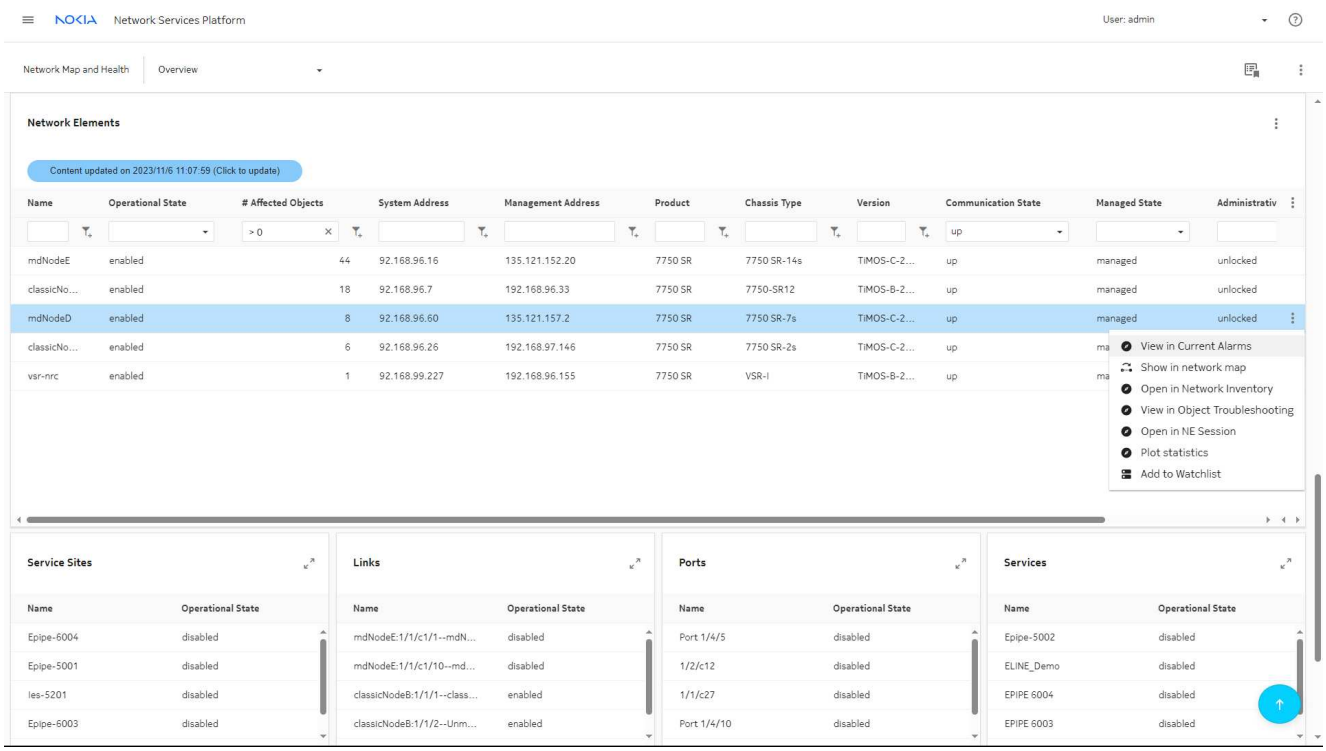
The **Equipment Health** dashlet in the **Network Map and Health** dashboard uses KPIs to show NE states.

The **Affected NEs** KPI indicates that there are NEs to look at to start investigating. Click the **Affected NEs** circle to launch the **Network Elements** data page.

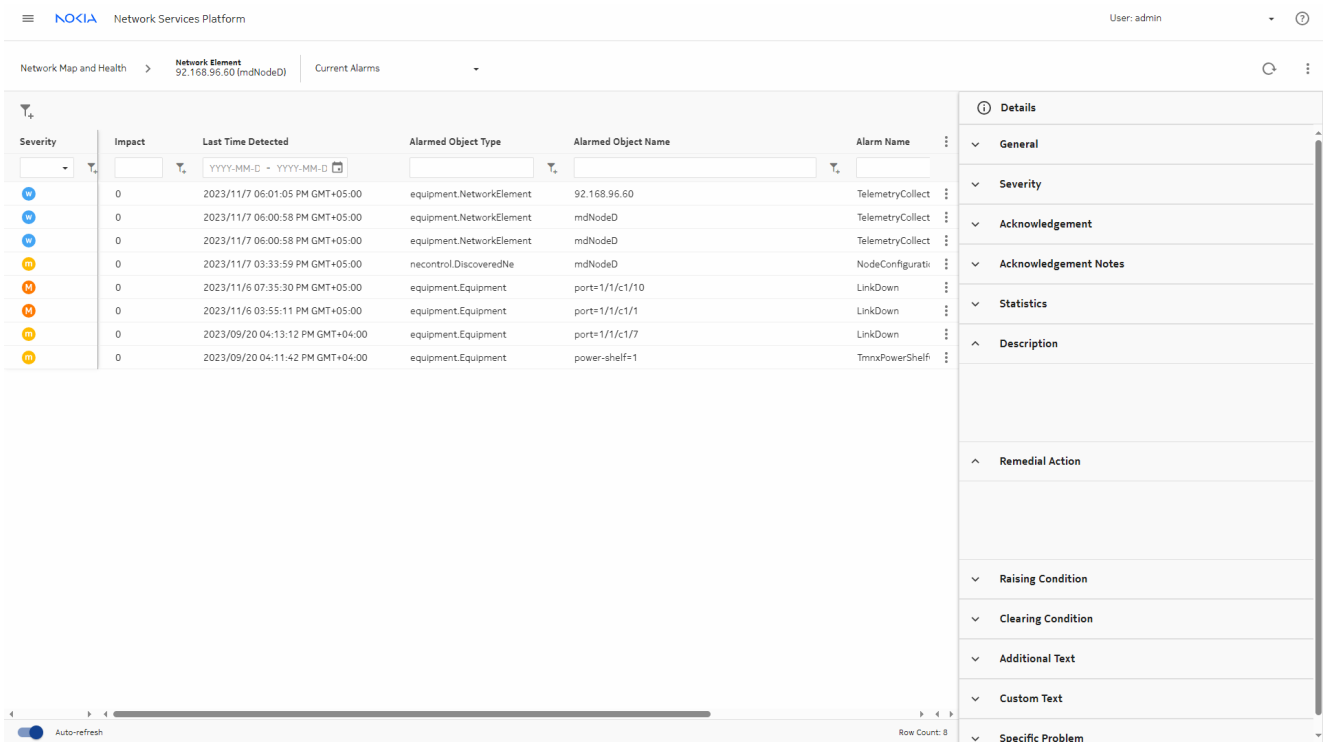


The **Network Elements** data page appears, filtered to show the list of NEs with at least one affected object. The default filter can be changed if needed, for example, to focus on NEs with more affected objects. We'll focus on the Affected Objects column for the NE we're troubleshooting.

Select the NE and click ⋮ (Table row actions), **View in Current Alarms**.



Current Alarms opens, showing a filtered list of alarms. Click on an alarm to see information in the **Details** panel, or use ⋮ (Table row actions) menu to show impacts, root cause, or open NE CLI session.

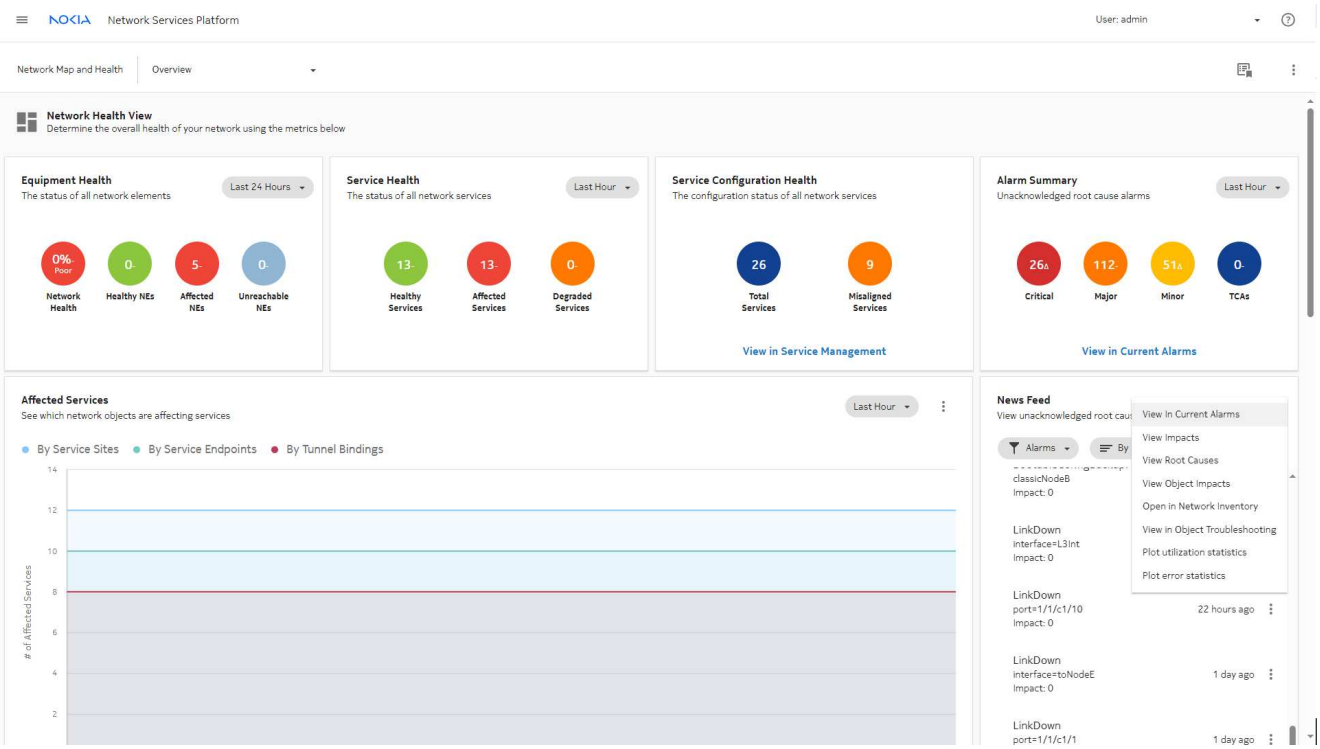


5.7.3 View the News Feed

The News Feed provides a live feed of unacknowledged root cause alarms as they occur in real time. Alarm severity and number of impacts are displayed, and cross launch is available depending on the alarm. All alarms can cross launch to Current Alarms.

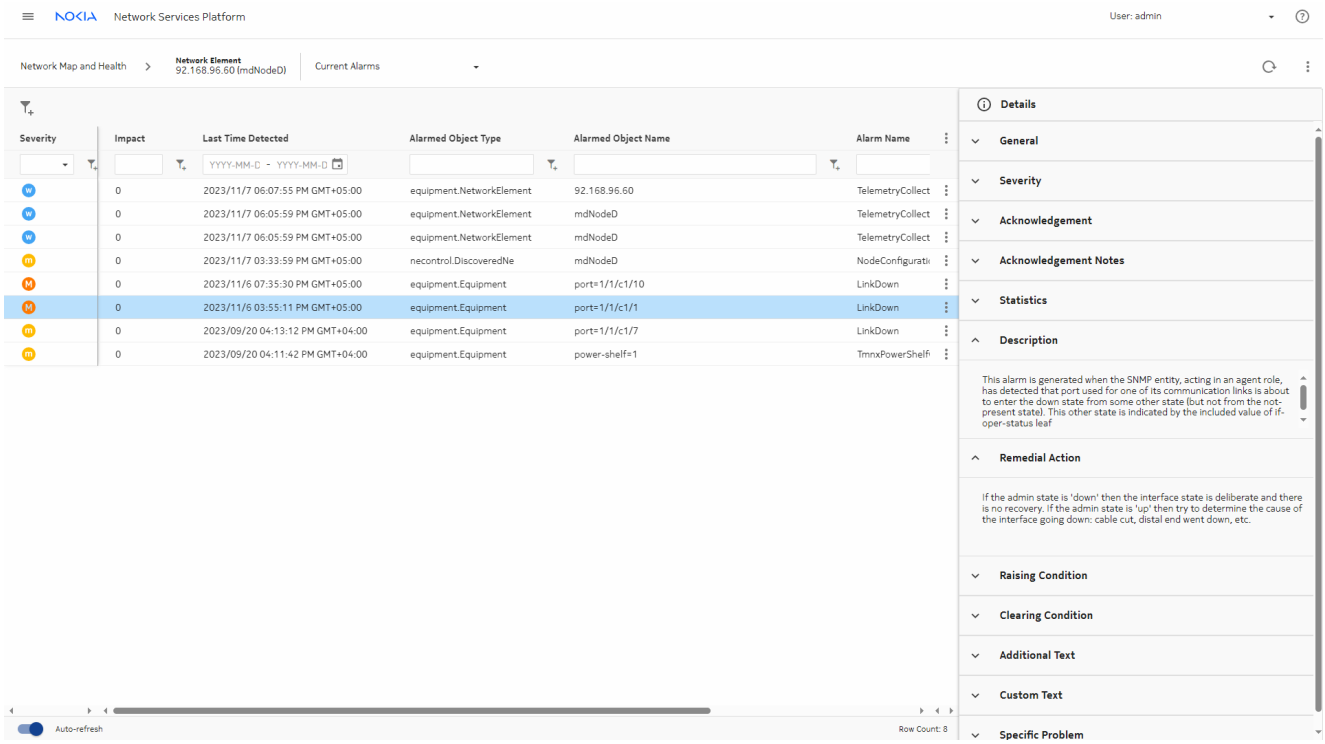
1

From the **News Feed**, select an alarm affecting the node. Click **View in Current Alarms** from the More menu.



2

Current Alarms provides details of the alarm, such as the alarm description, raising and clearing conditions, and remedial action.



3

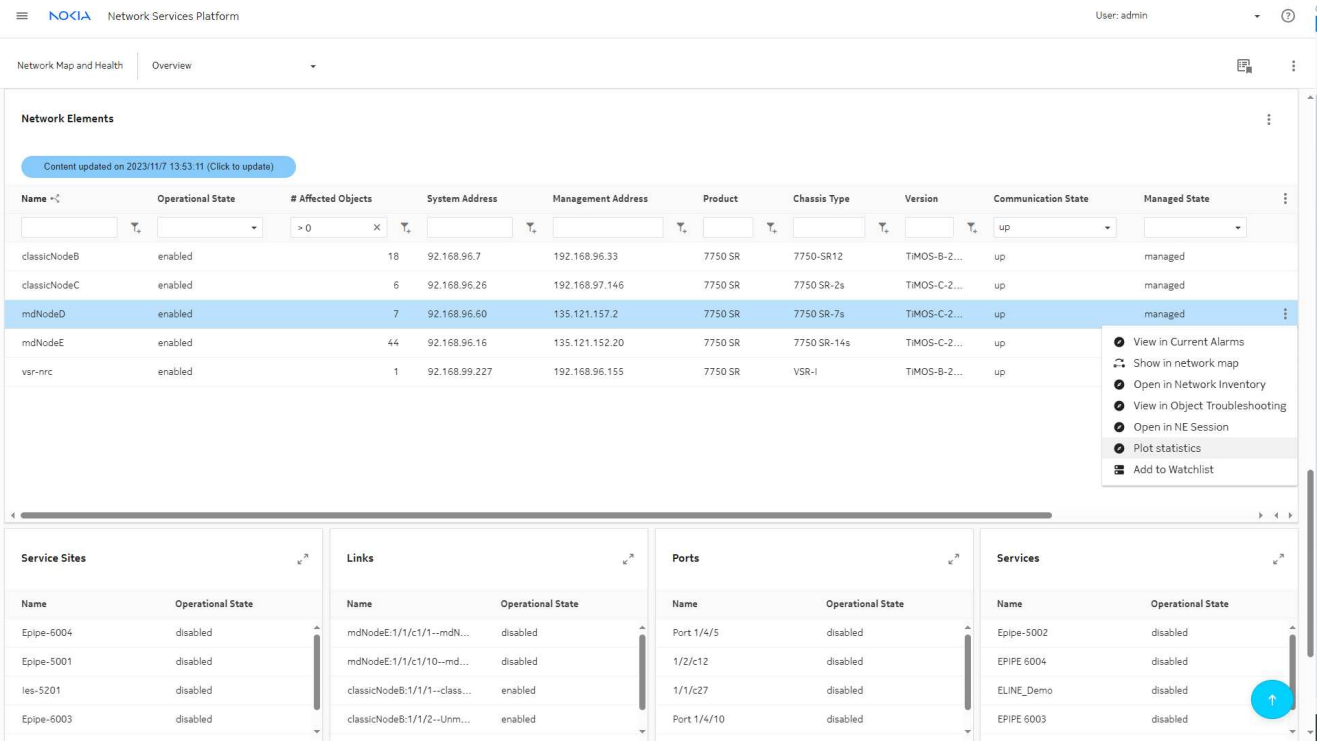
Another option is to note the NE name and switch to the **Unhealthy NEs** or **Top Problems** view, to see what other alarms are present on the NE and what other issues the NE is experiencing.

5.7.4 View the Network Map and Health dashboard map view

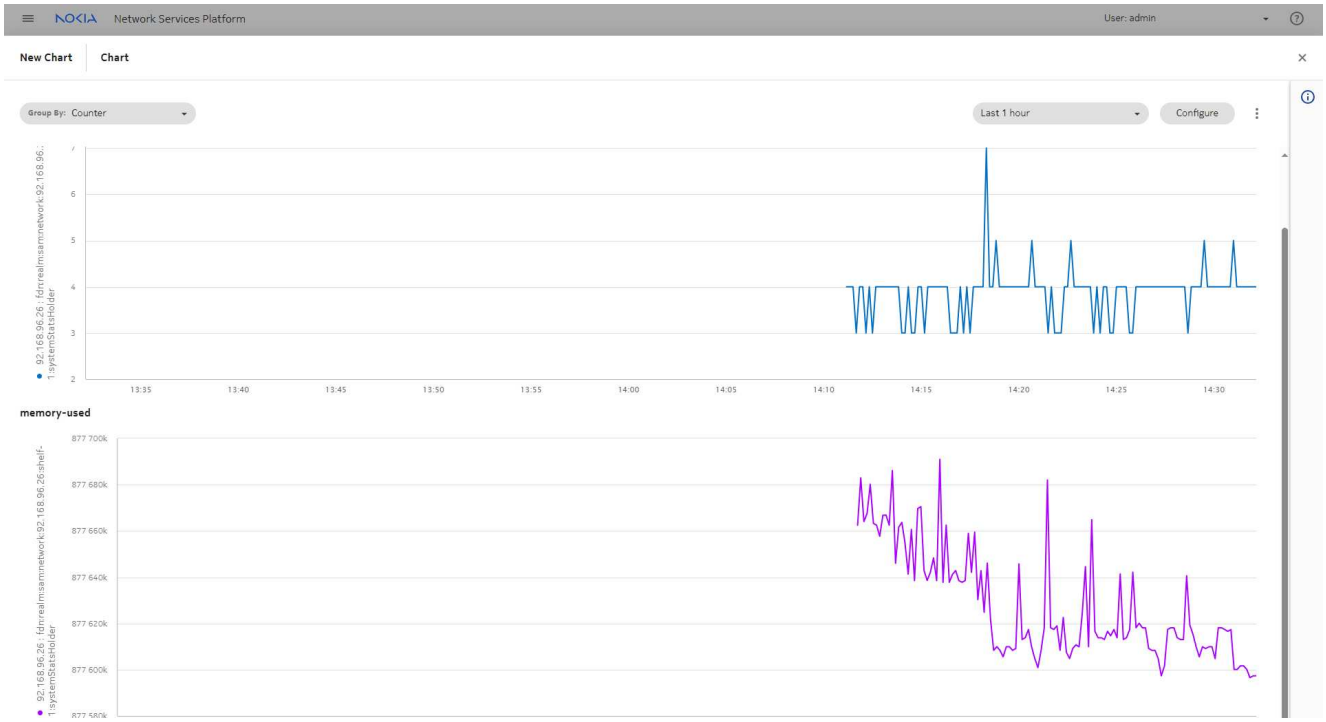
Another option on the **Network Map and Health** dashboard is the **Network Map View**. Viewing the NE in the map will show us the status of links, in case there are any port issues affecting connectivity.

1

Navigate back to the **Network Elements** data page. Click on the NE and choose **Plot statistics**.

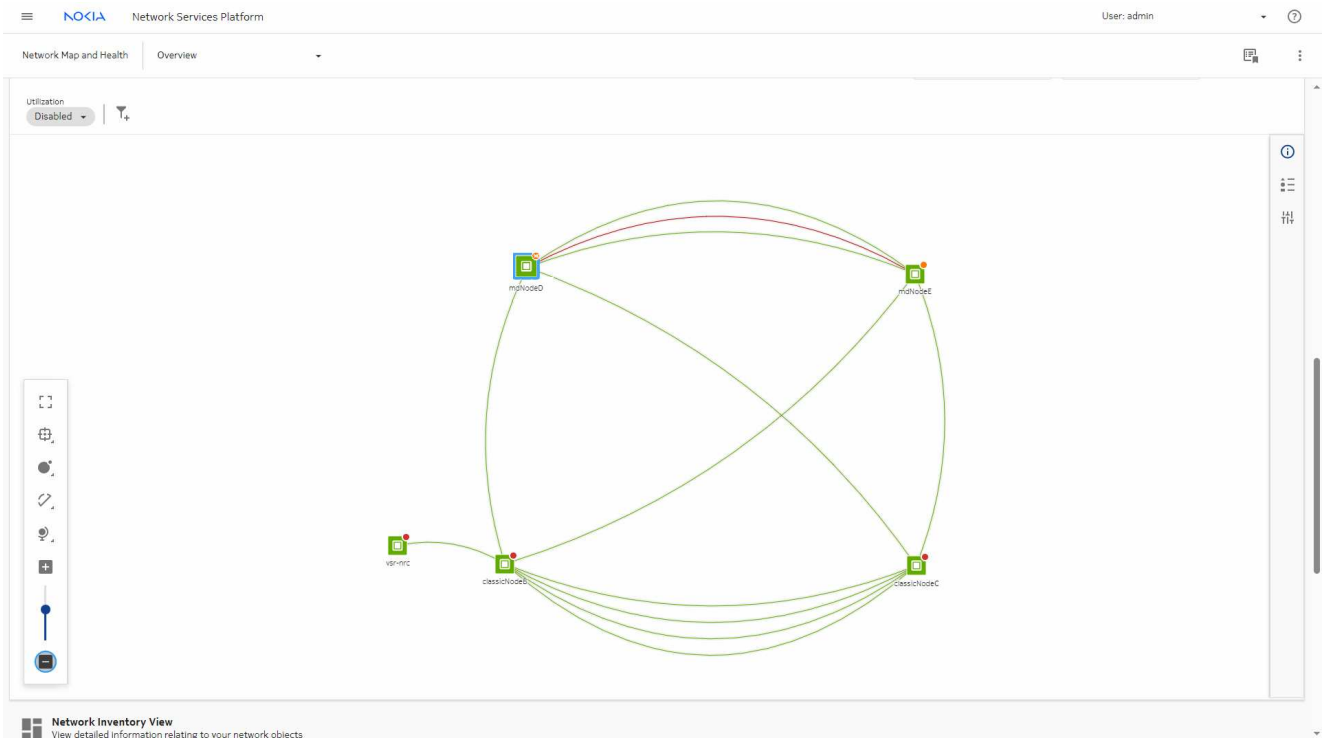


Data Collection and Analysis Visualizations launches, showing on-demand charts for memory and CPU usage for the NE.

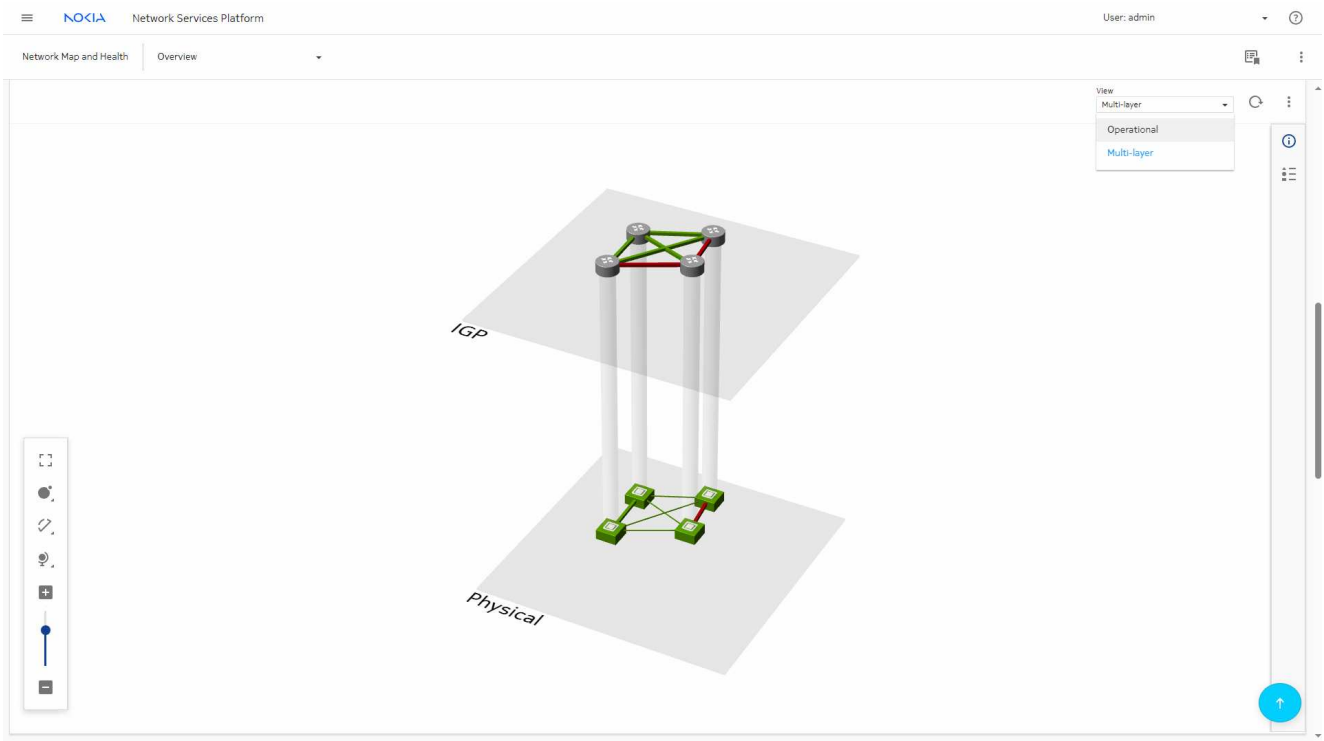


2

Back in the **Network Elements** data page, click on the NE and select **Show in network map** to open the **Network Map View** with the NE highlighted.

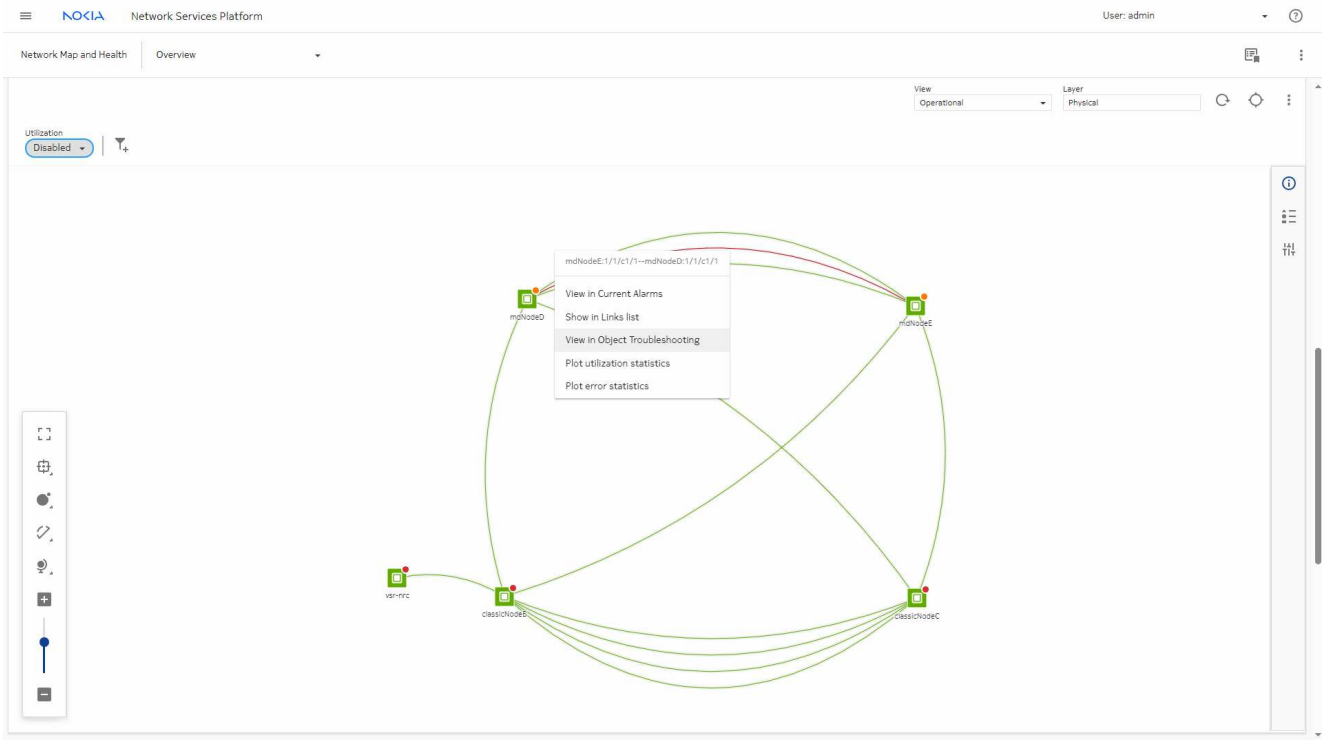


View the **Multi-layer** map to see the state of the links at the IGP layer.



Return to the Operational map and enable **Utilization** to show utilization statistics displayed on the map.

Right click on the node and select **View in Object Troubleshooting**.

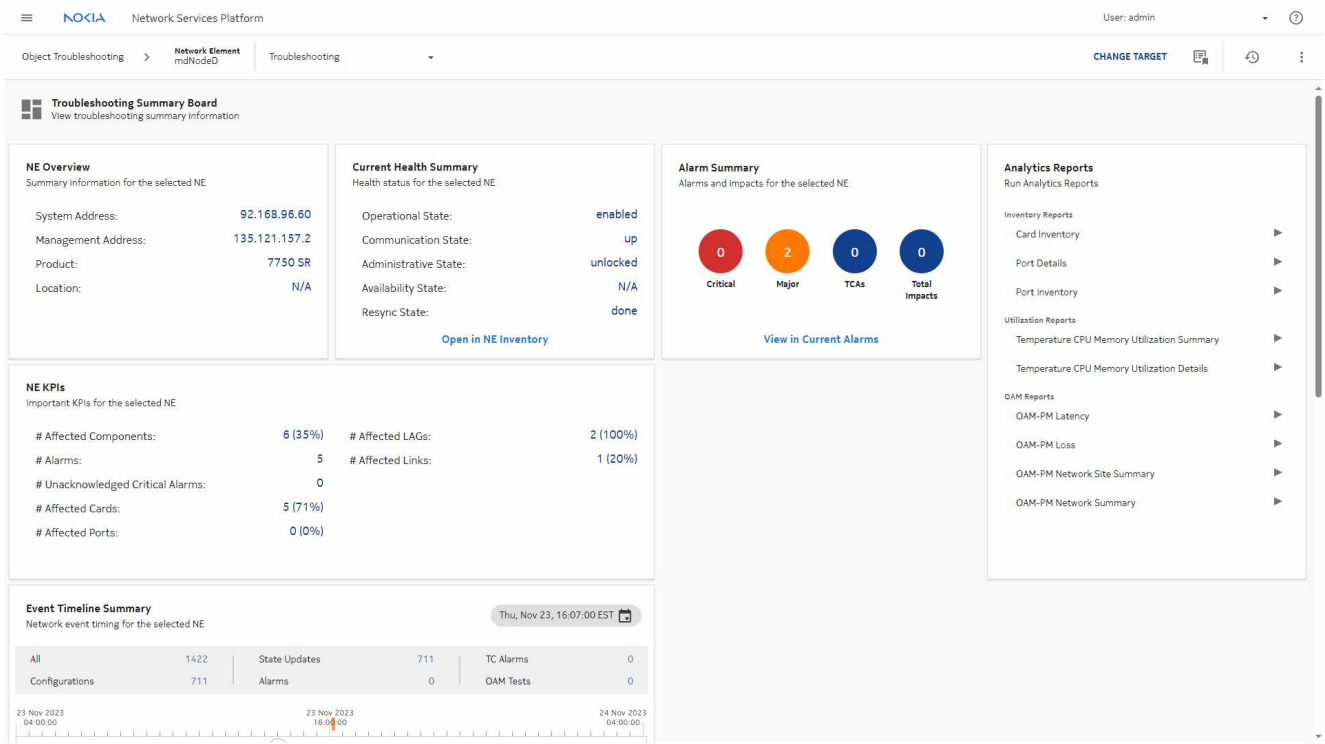


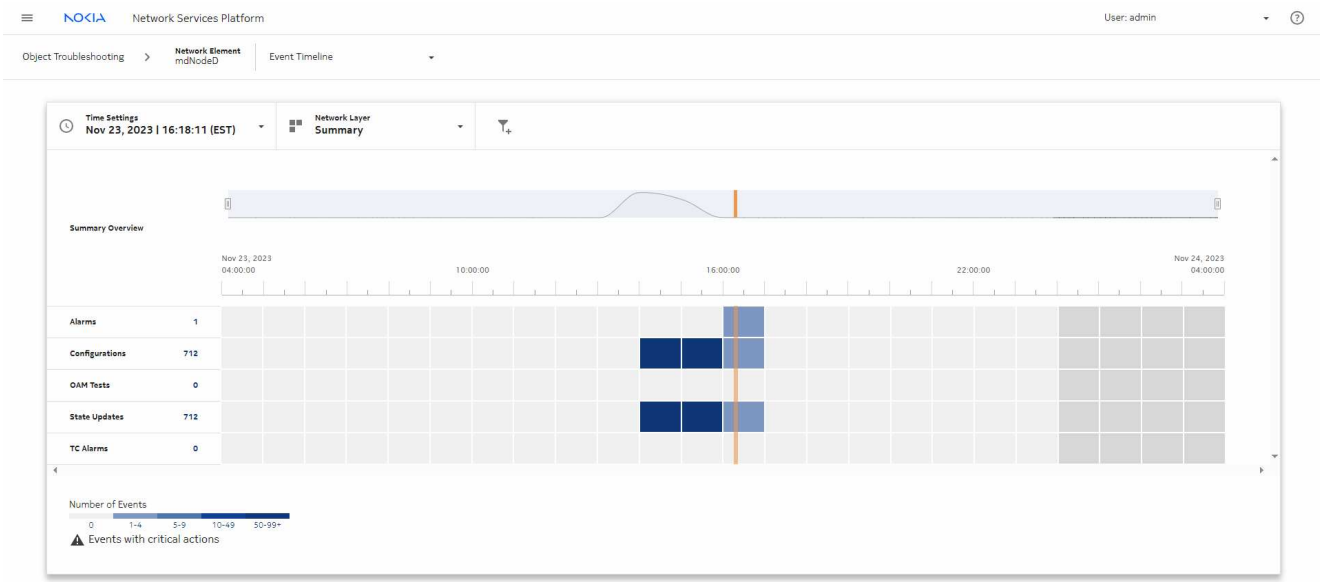
5.7.5 Check the Object Troubleshooting dashboard

1

Viewing a target in the Object Troubleshooting dashboard can help you see where to look to investigate a problem. The dashboard shows summary information for the NE, and provides a health and an alarm summary.

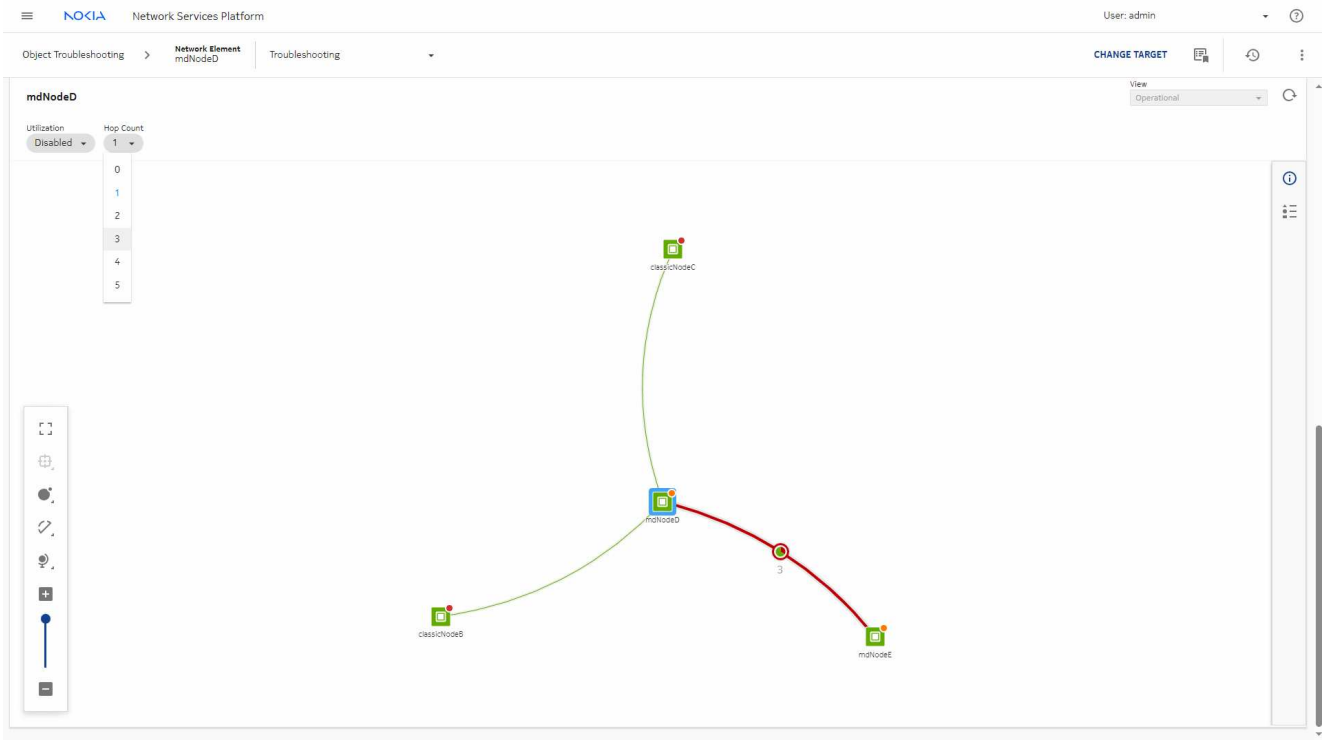
From the **Object Troubleshooting**, we can click **View in Current Alarms** to view alarms and impacts, or run **Analytics Reports**.

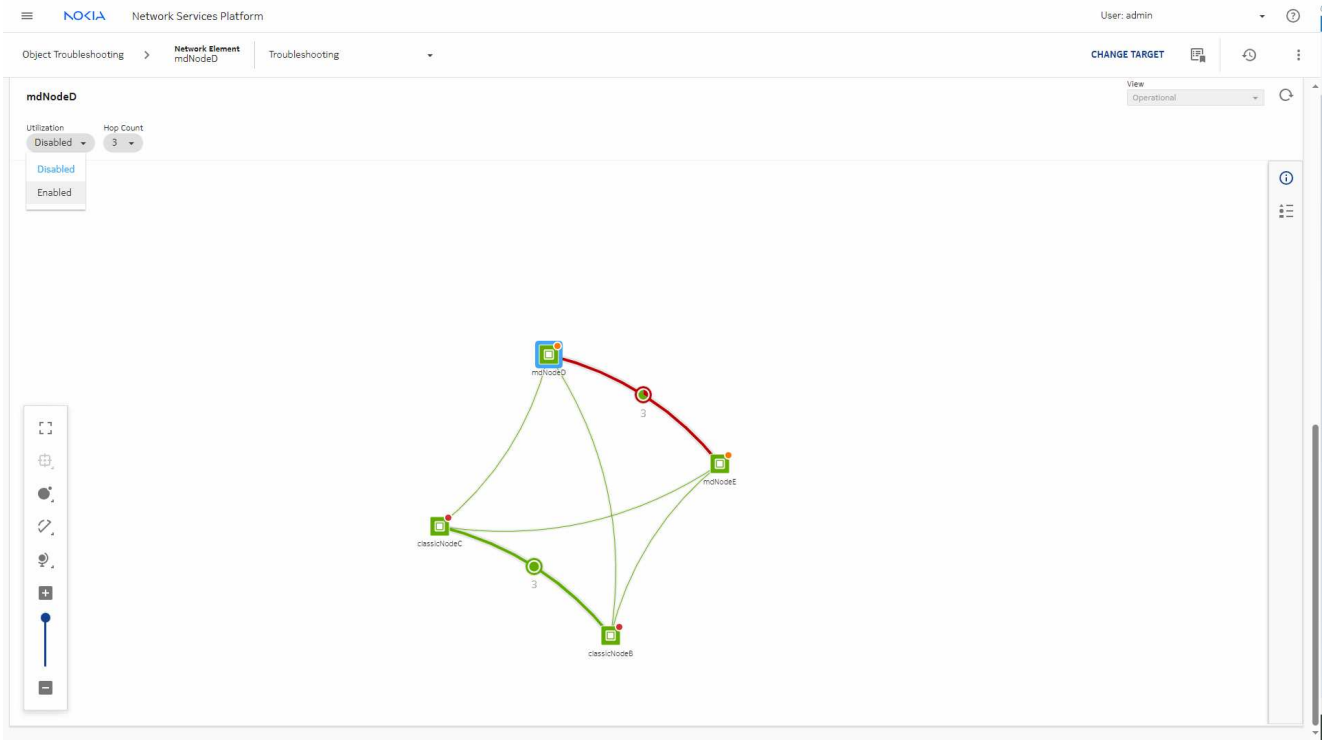




2

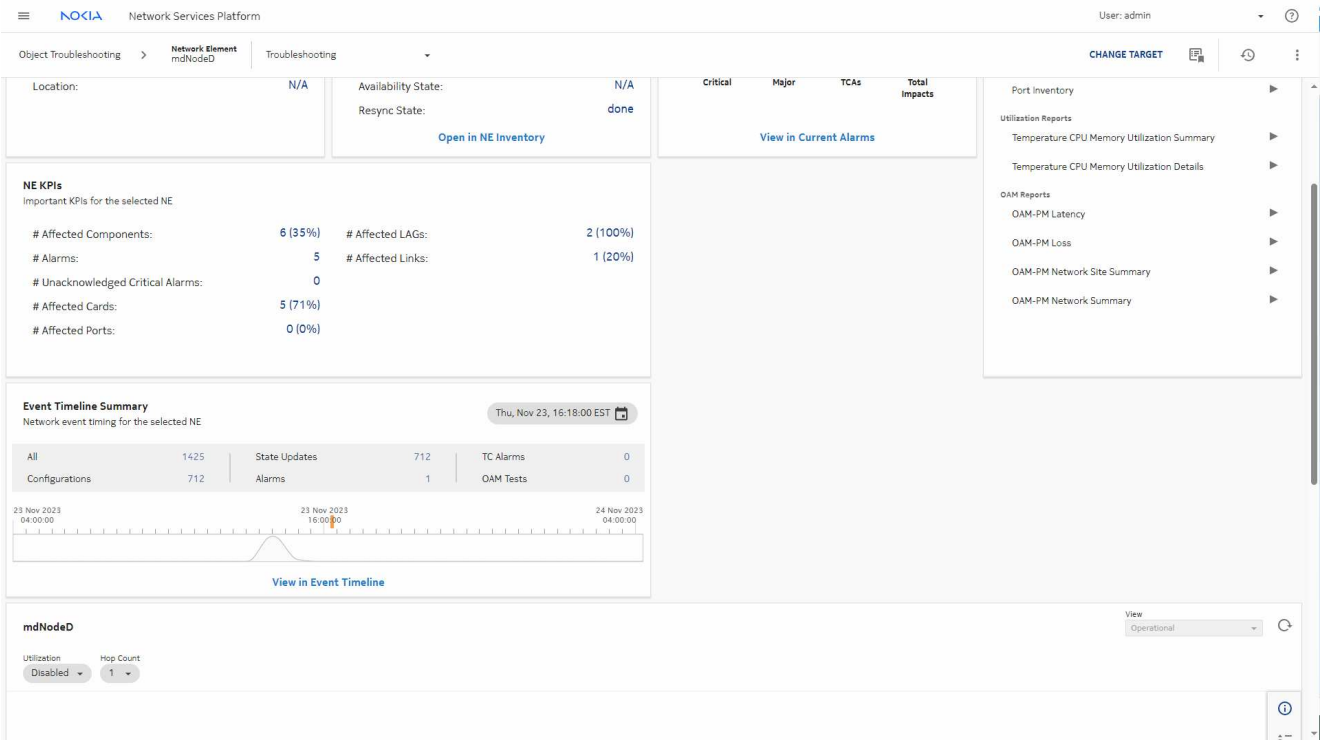
In the **Object Troubleshooting** map, we can change the **Hop Count** to see nodes that are further from the target and enable **Utilization**.





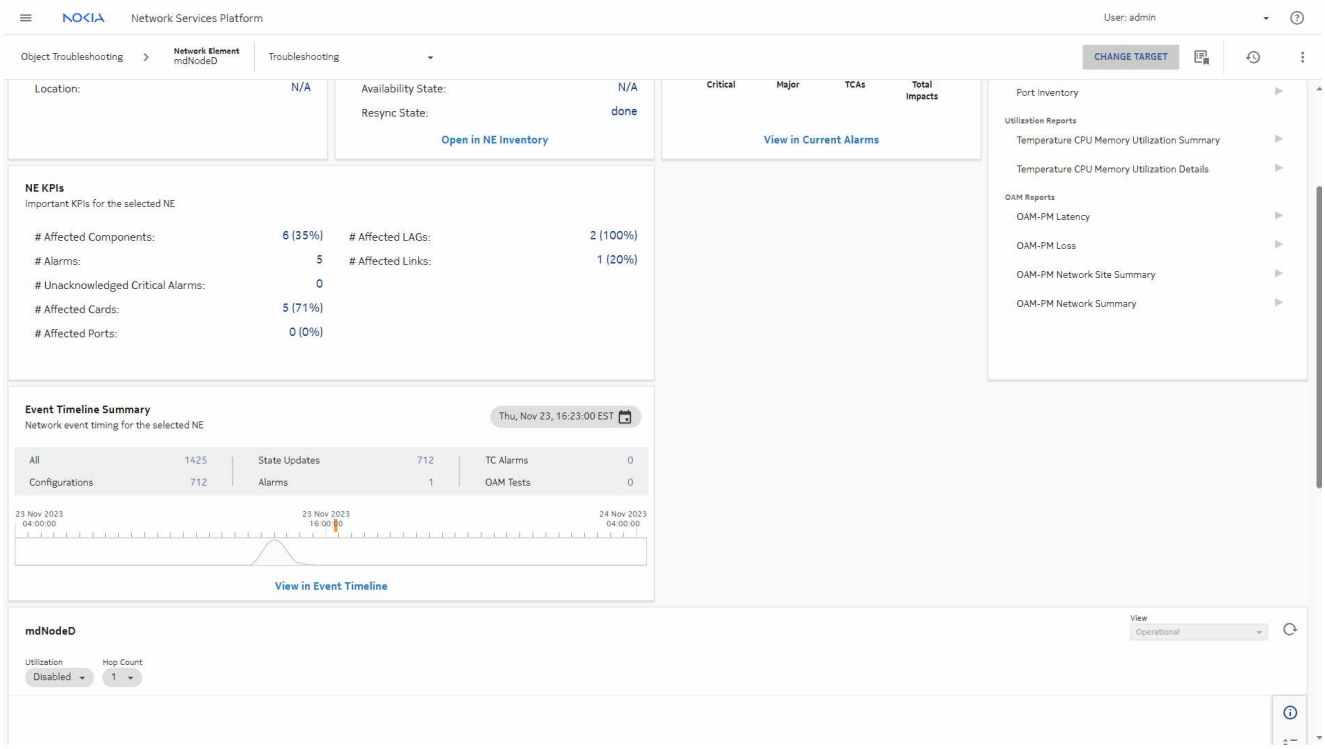
3

In the **Object Troubleshooting** dashboard, the **Event Timeline** dashlet show today's events summary. Click **View in Event Timeline** to launch the full view.



4

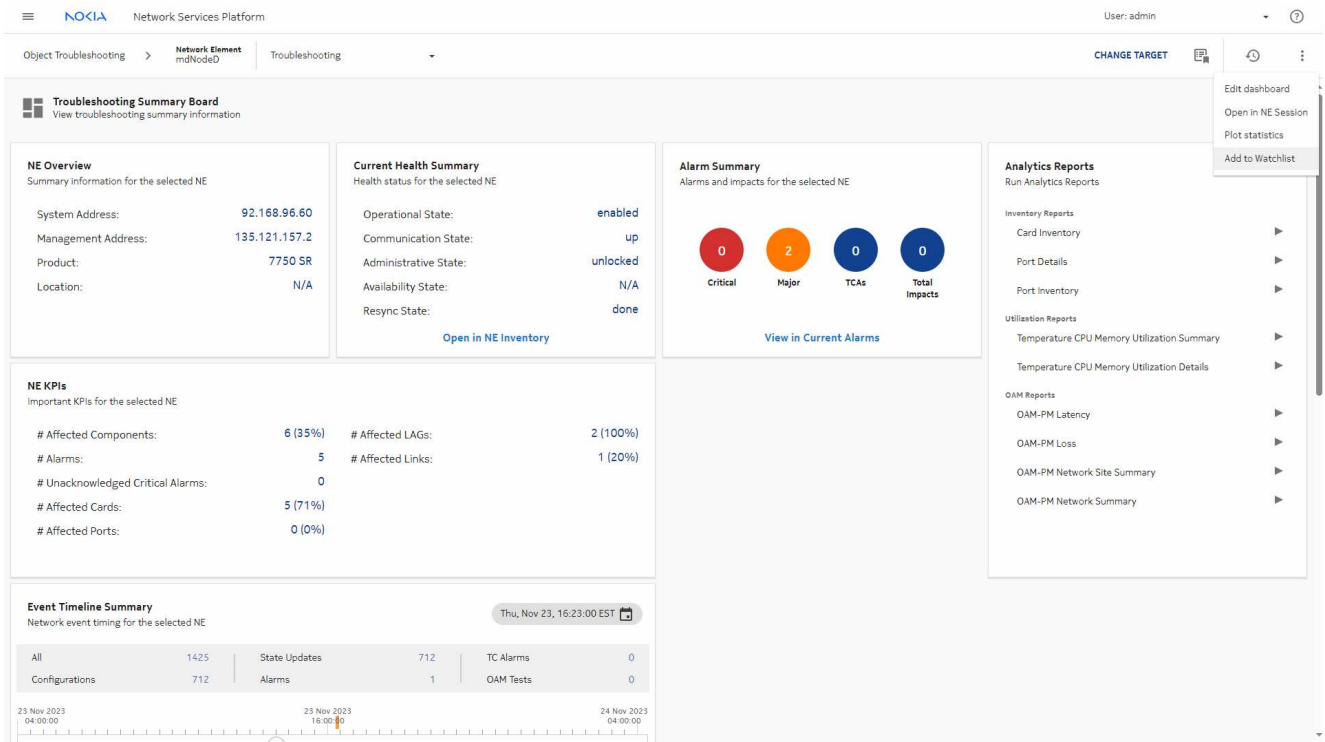
In the **Object Troubleshooting** dashboard, click **CHANGE TARGET** to troubleshoot other NEs or other types of objects.



5

In the **Object Troubleshooting** dashboard, click **Add to Watchlist** in the More menu.

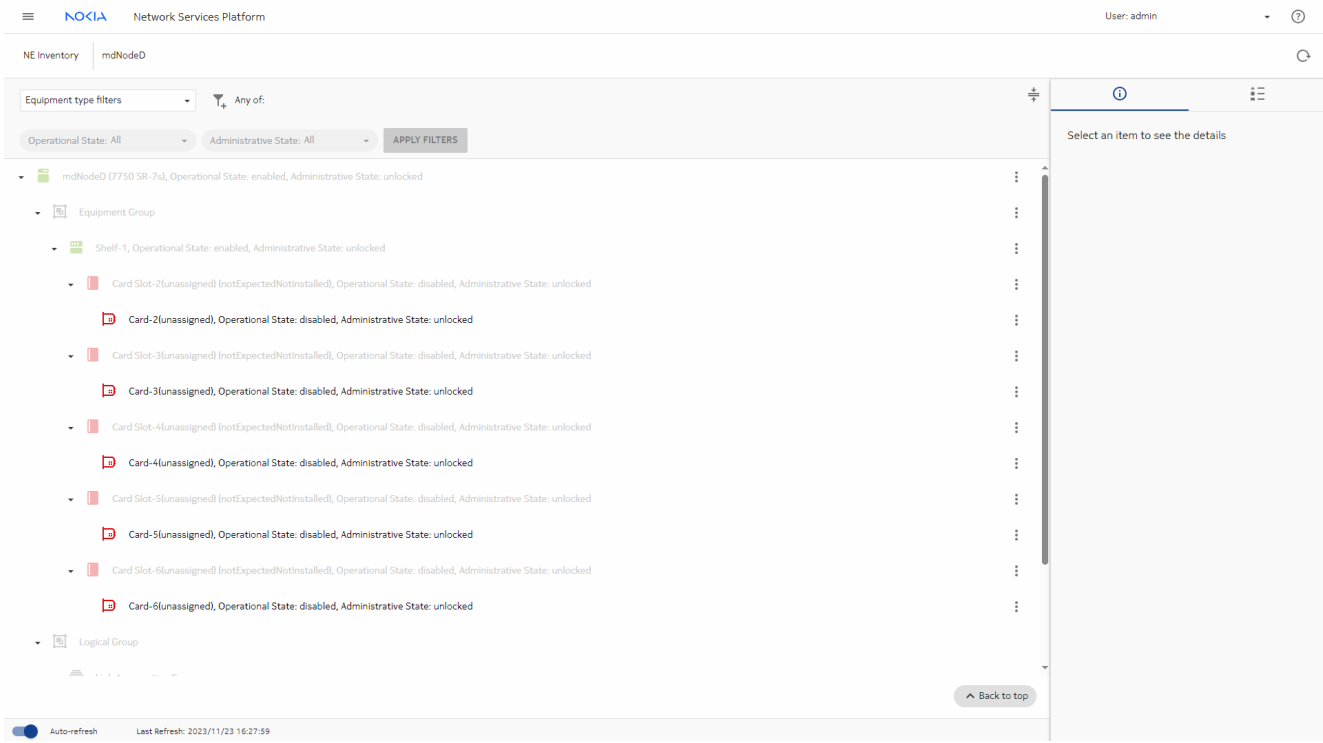
Adding the NE to a watchlist will allow you to navigate quickly to the NE in the future. To open the watchlist, click Watchlist ( ).



5.7.6 Check configuration alignment and operation history in the NE Inventory

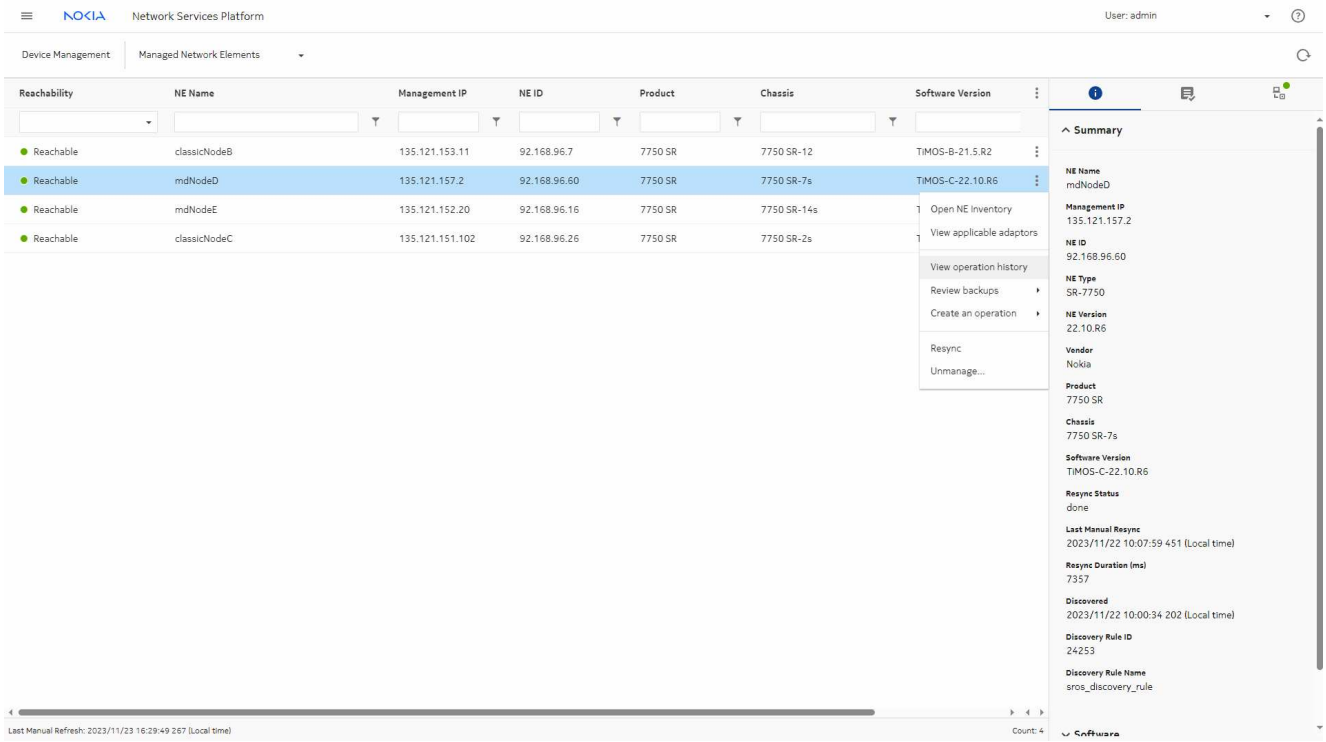
1

From the **Current Health Summary** dashlet, click **Open in Network Inventory** to launch equipment inventory.



2

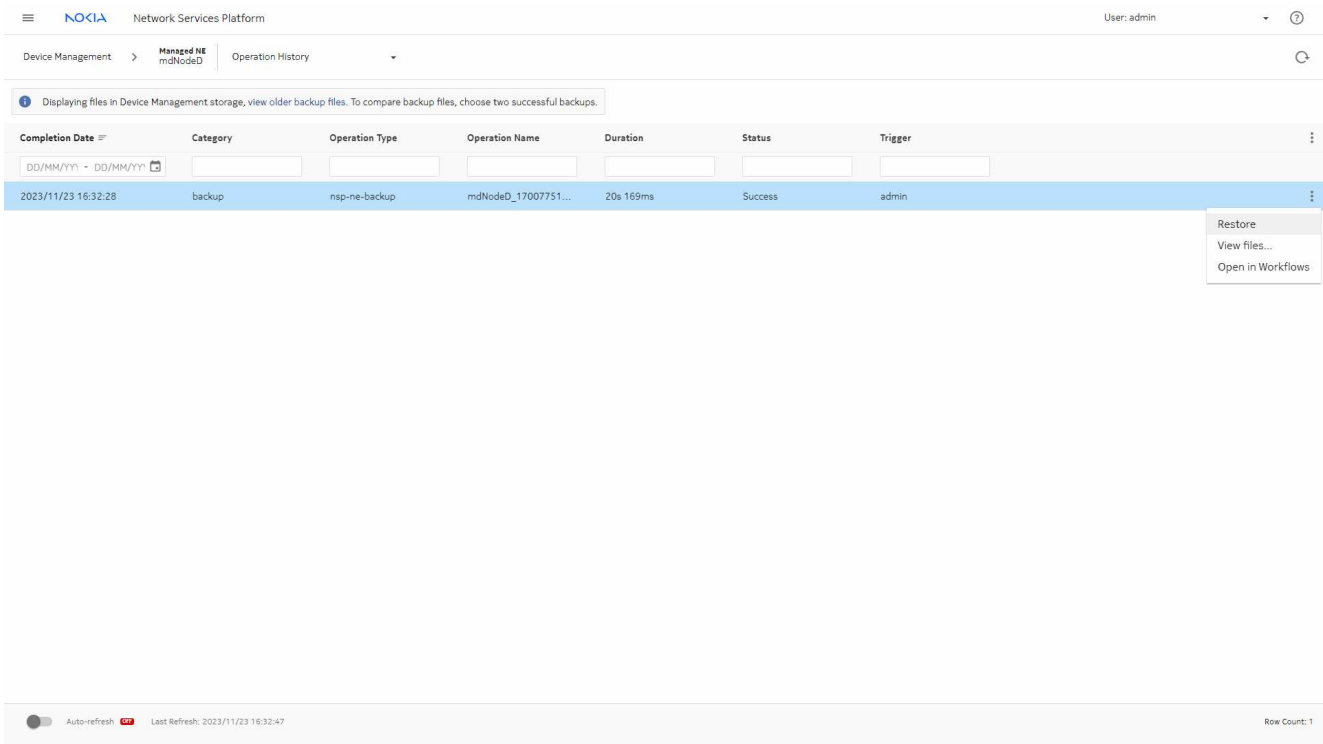
In the **Device Management**, **Managed Network Elements** view, select the NE and click ⋮ (Table row actions), **View operation history**.



From the history list, we can see when the most recent successful backup was performed, and see if any recent operations have failed.

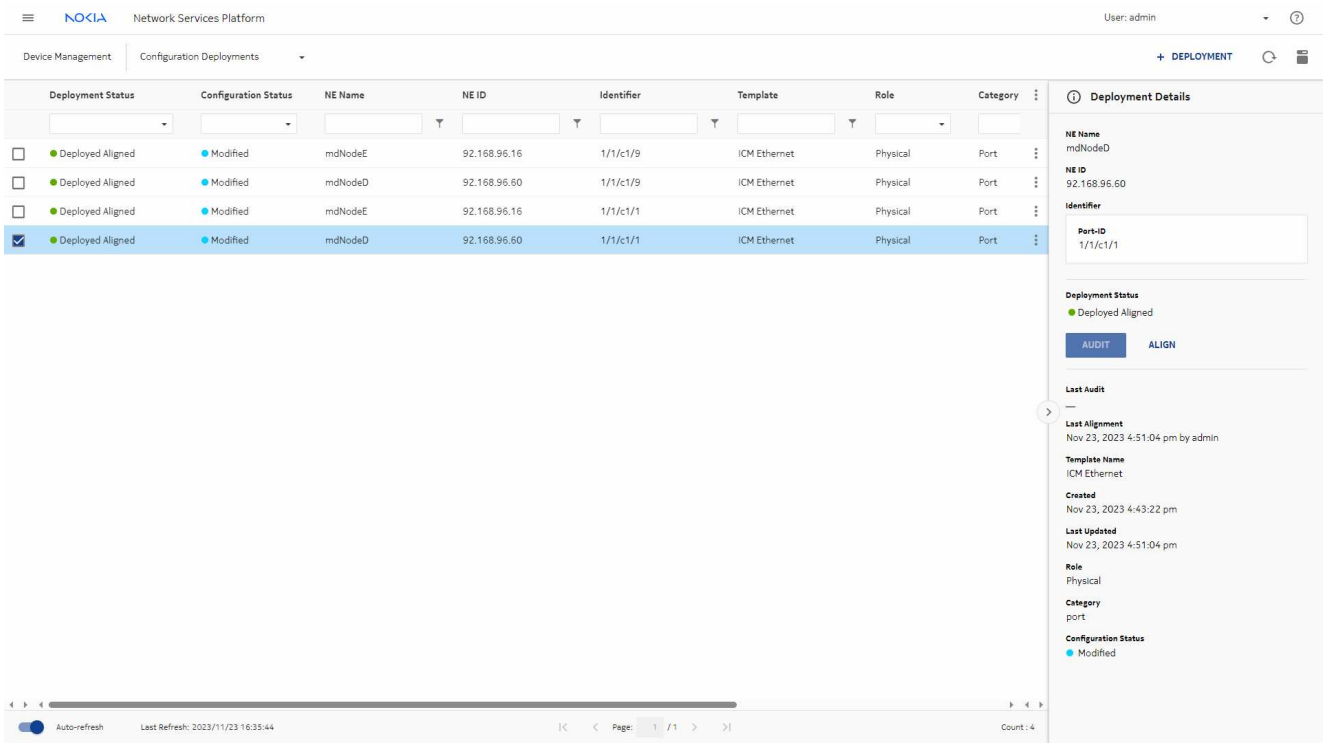
3

To restore from a backup, select a successful backup and choose ⋮ (Table row actions), **Restore**. The restore operation is launched.

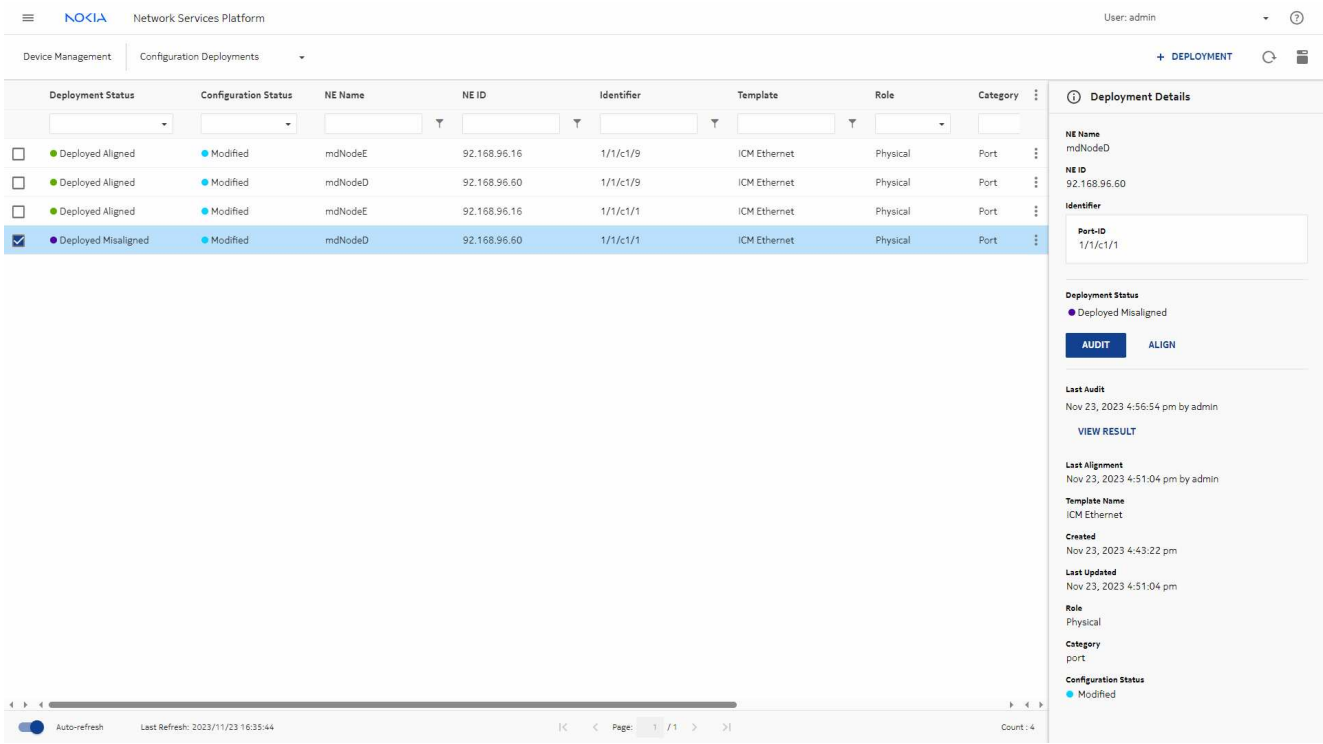


4

Go to **Configuration Deployments** view in **Device Management** and check for misaligned objects on the affected NE by running an **AUDIT** on deployments related to that NE.

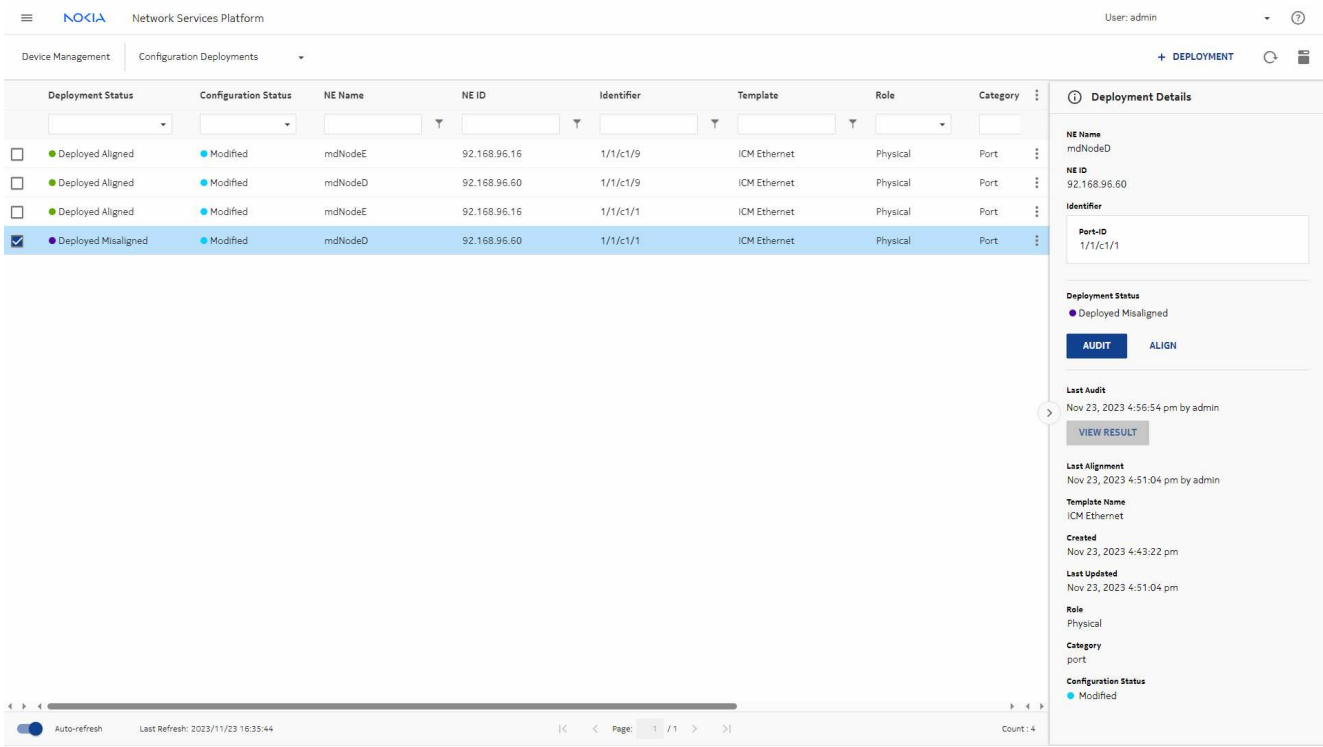


The audit results show the misaligned attributes.



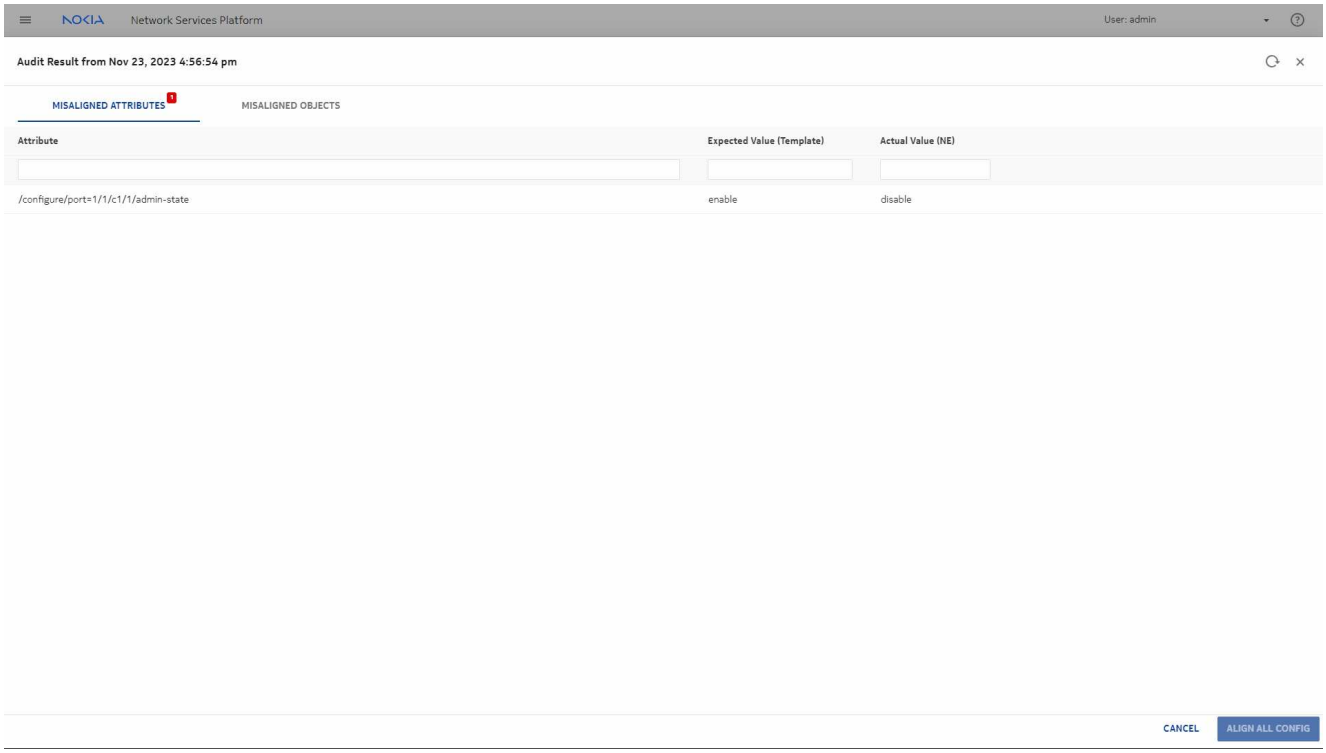
5

Click **VIEW RESULT** in the **Deployment Details** panel.



6

The results open. Click **ALIGN ALL CONFIG** to fix the misalignment.



5.8 End-to-end service troubleshooting scenario

5.8.1 Purpose

This process shows you how to troubleshoot issues on services.

In this scenario, a service is experiencing problems.

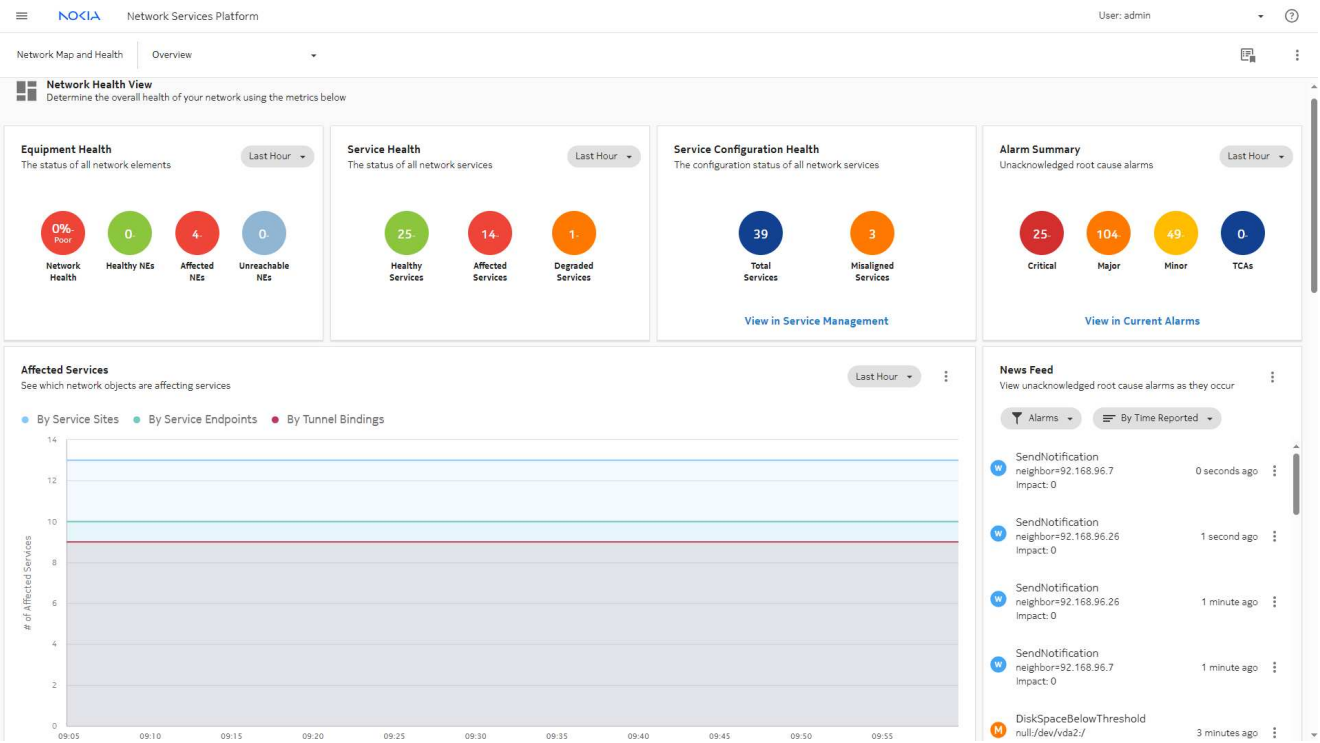
5.8.2 View service health summary

1

The Service Health dashlet in the Network Health dashboard uses KPIs to show service states.

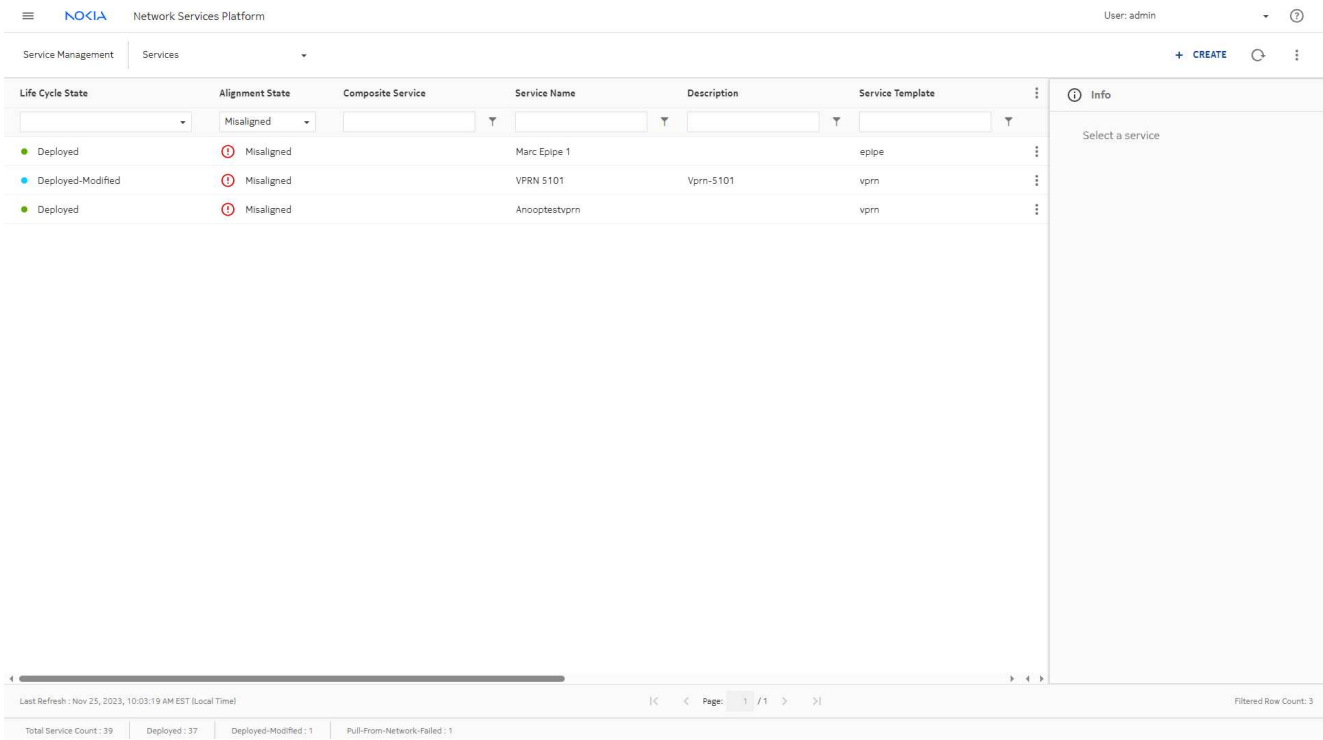
The Affected Services KPI indicates that there are several unhealthy services in the network.

The Service Configuration Health dashlet indicates that three of the services are misaligned from the templates used to create them.



Click on the **Misaligned Services** circle.

The **Service Management**, **Services** view opens, filtered to show the misaligned services.

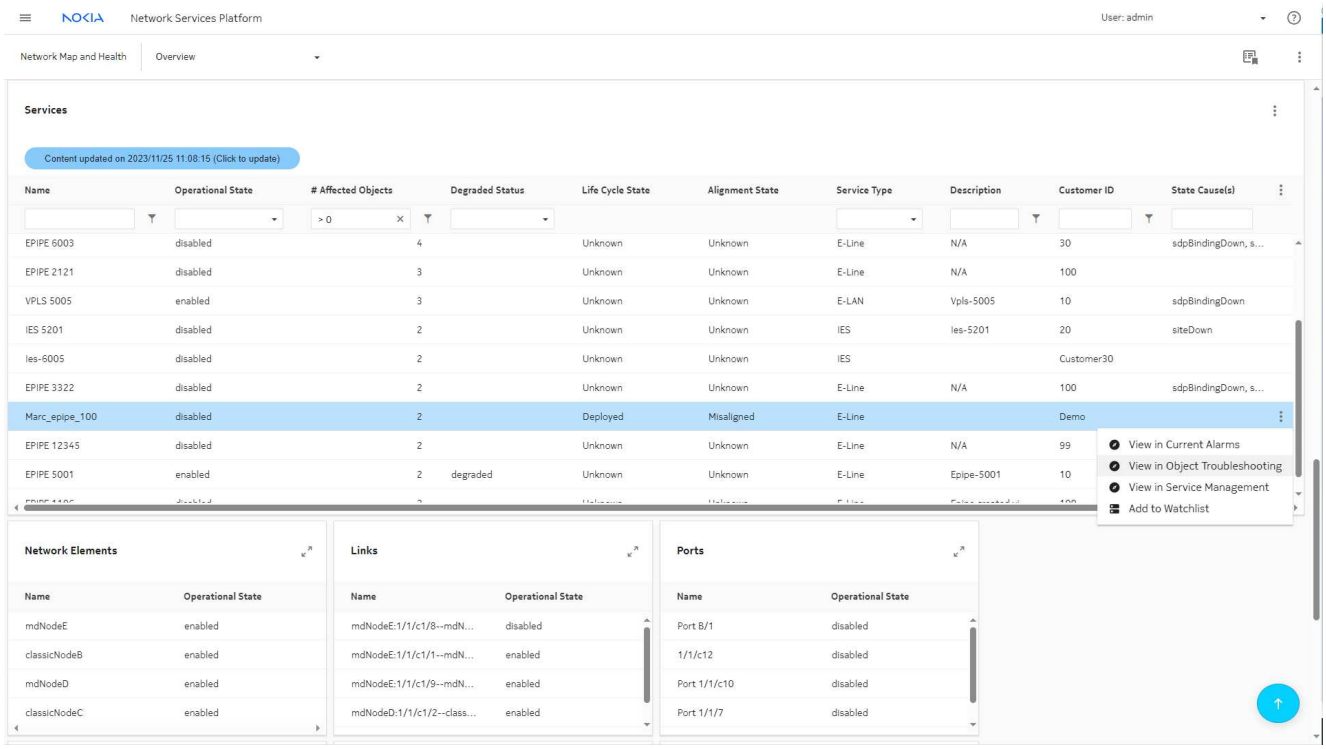


2

Returning to the Network Map and Health dashboard, click on the **Affected Services** circle.

The Services data page appears, filtered to show the list of services with at least one affected object. The default filter can be changed if needed, for example, to focus on services with more affected objects. From the Services data page, we can see that the Operational State of our service of interest is disabled.

Let’s open the object troubleshooting dashboard to get more details. Select the affected service and choose ⋮ (Table row actions), **View in Object Troubleshooting**.

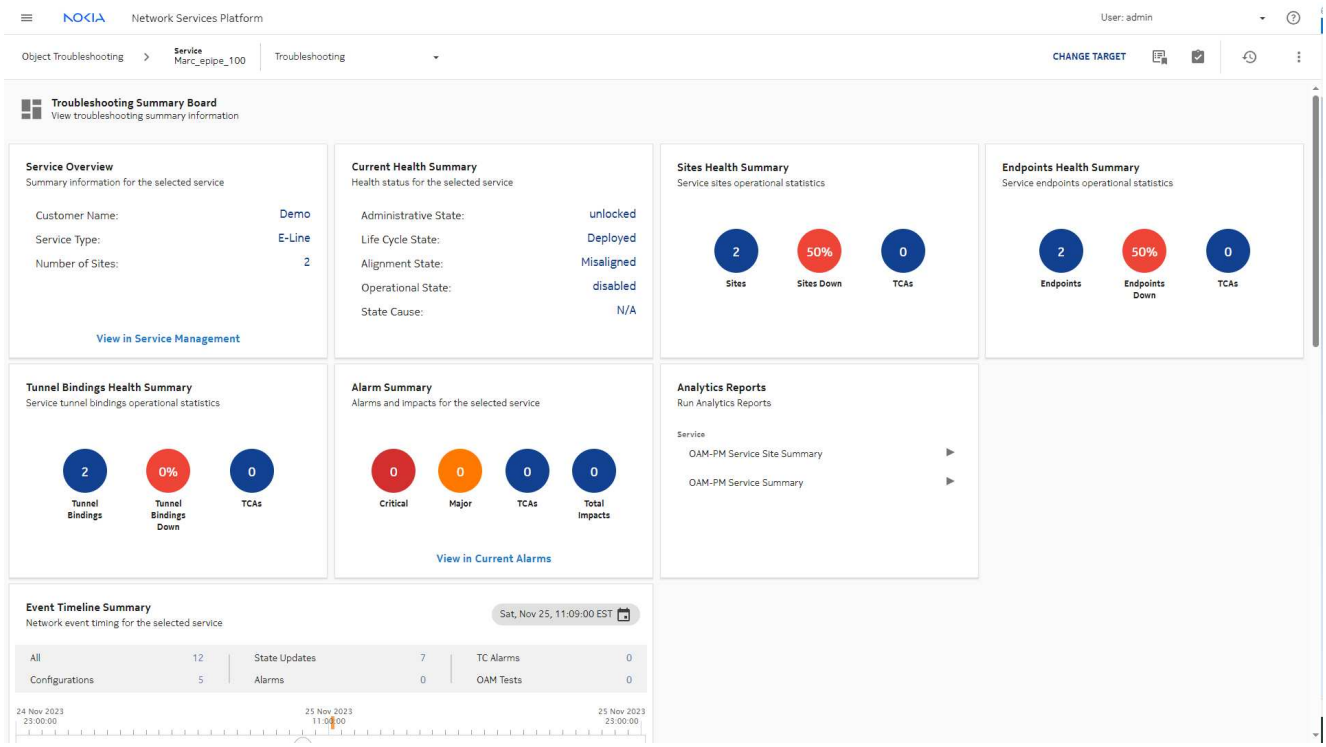


The Object Troubleshooting dashboard opens, filtered to show the service we're investigating.

5.8.3 Explore the Object Troubleshooting dashboard

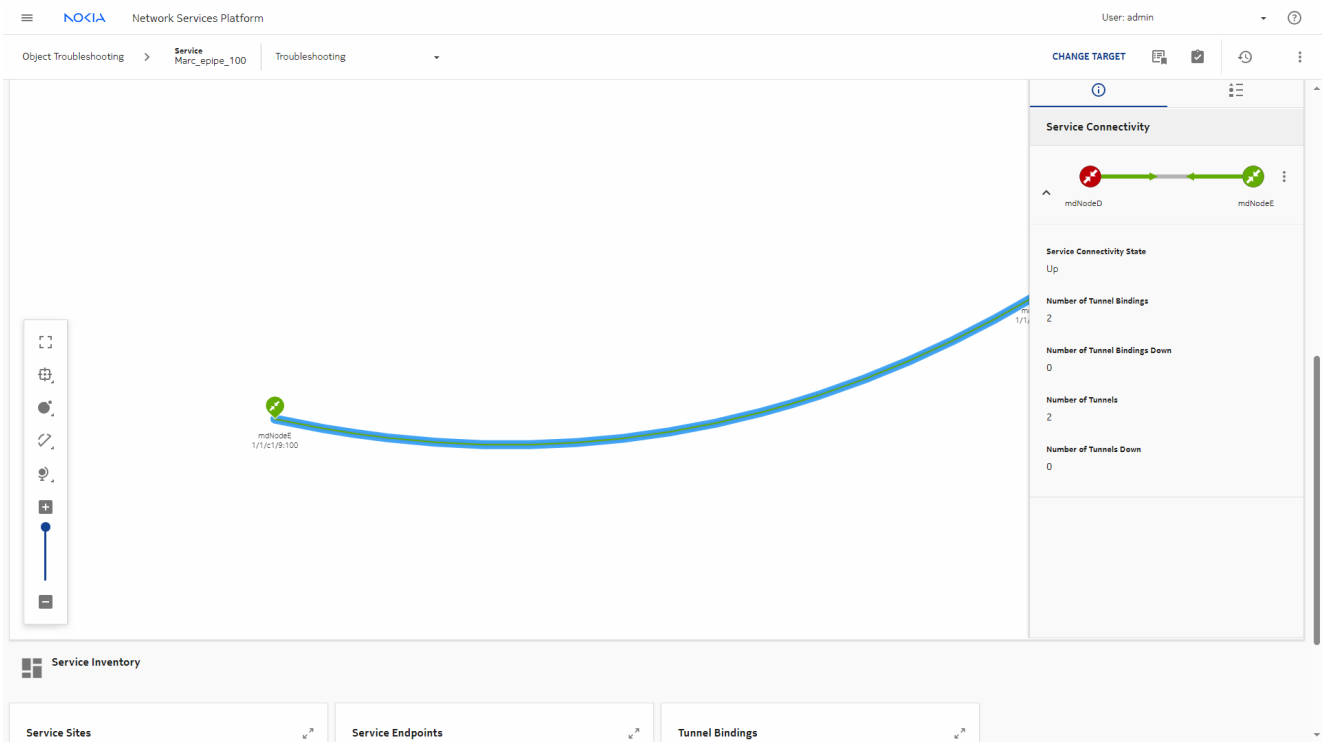
1

Let's take a look at the Troubleshooting Summary Board. The Service Overview and Current Health Summary dashlets show similar information to what we saw in the Network Health dashboard: The dashboard also includes health summaries for the sites, endpoints, and tunnel bindings. Here we can see that there is a problem with one site and one endpoint. The tunnel bindings look healthy.



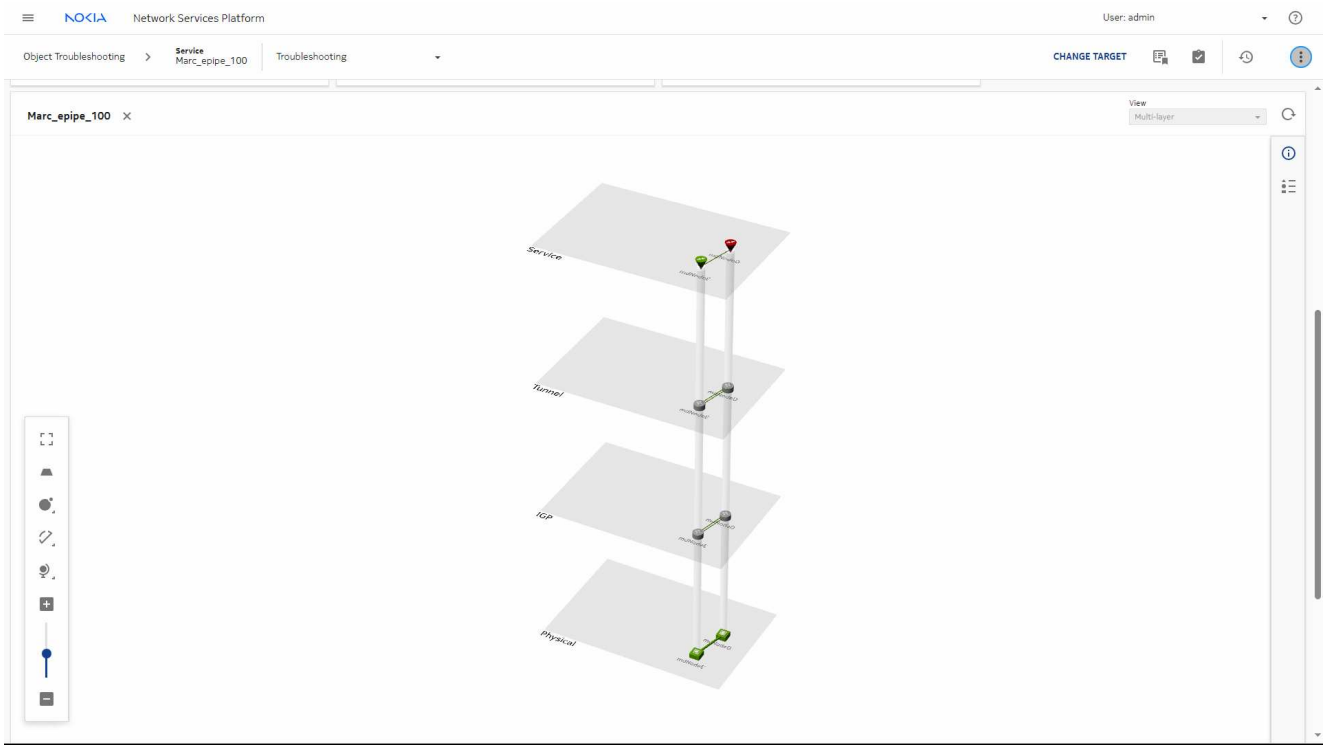
2

Scroll down to the service map, select the link and click **Details** (ⓘ) to see more information in the service summary panel.



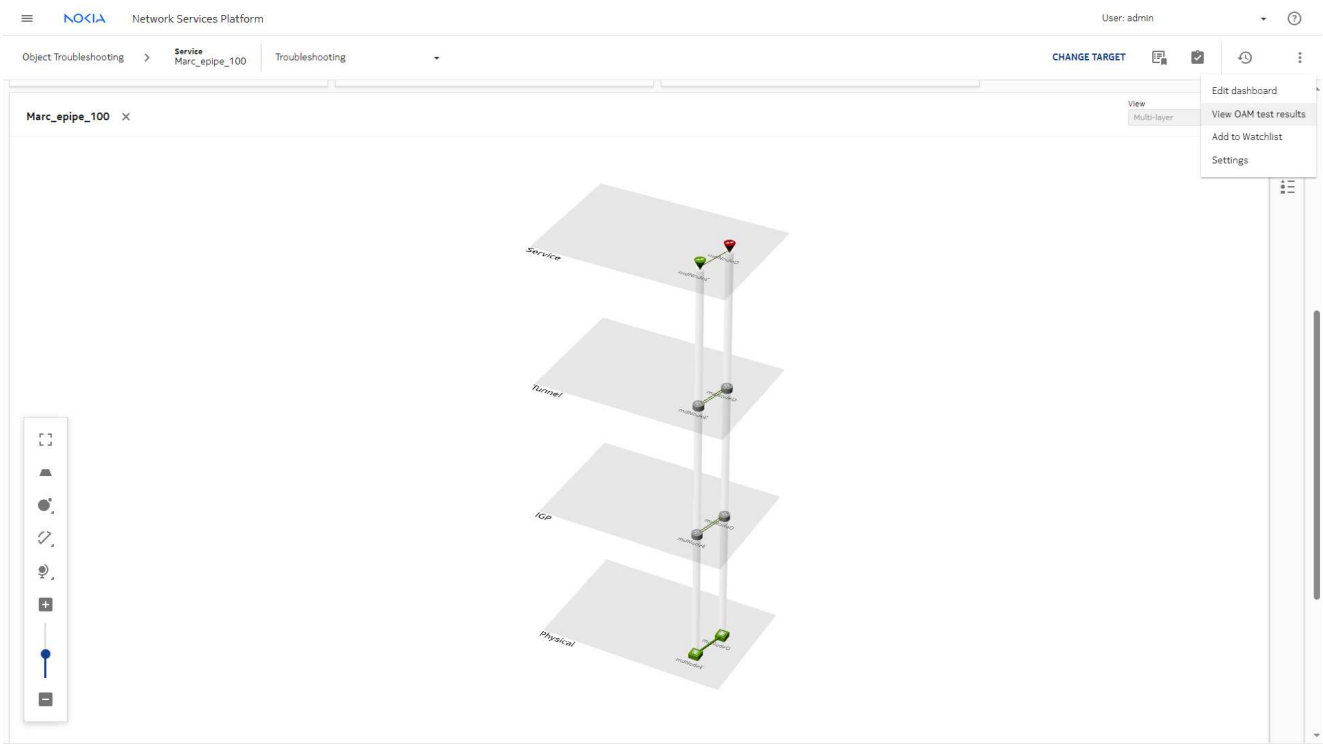
3

Select **Show in multi-layer map** from the More (⋮) menu in the service summary panel. The multi-layer map shows the health of the service, the tunnel, and the IGP and physical layers.



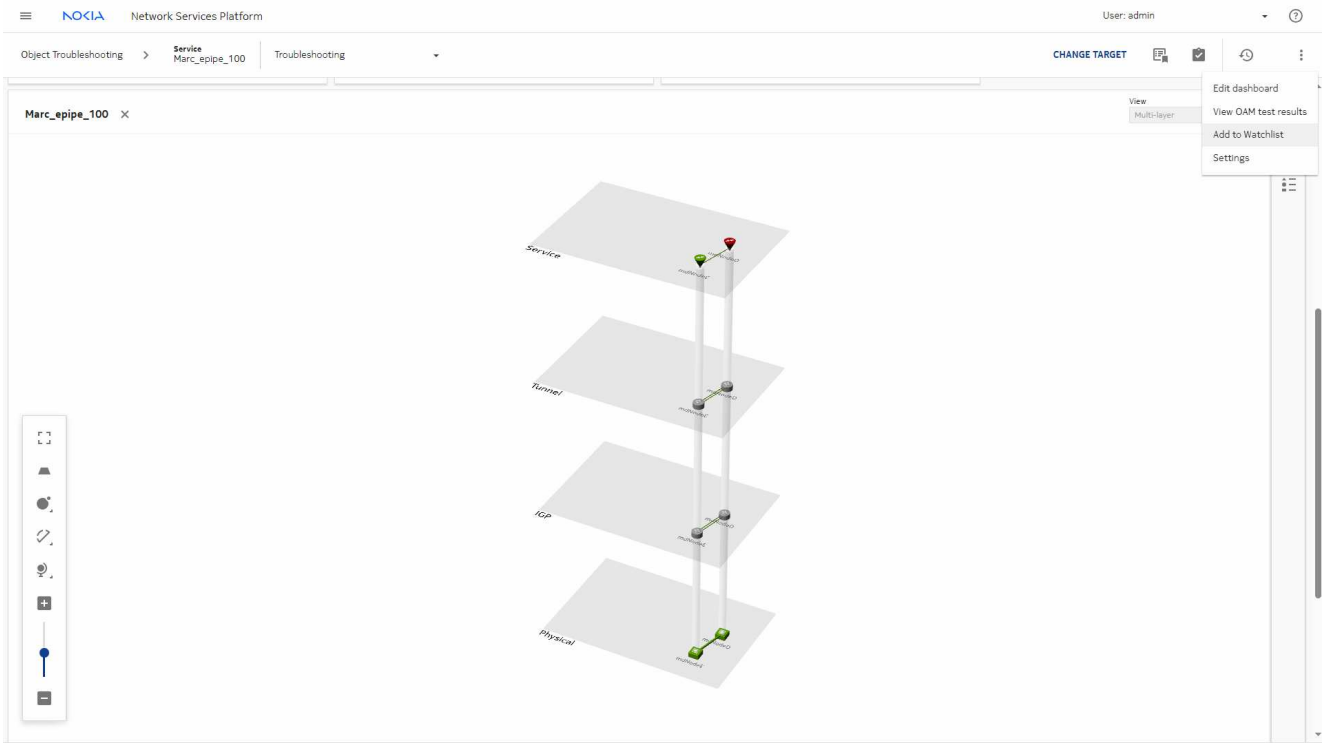
4

From the **Object Troubleshooting** dashboard, we can also create an OAM test suite ( ), or select **View OAM test results** from the More ( ) menu. OAM testing can provide valuable information about traffic flow.

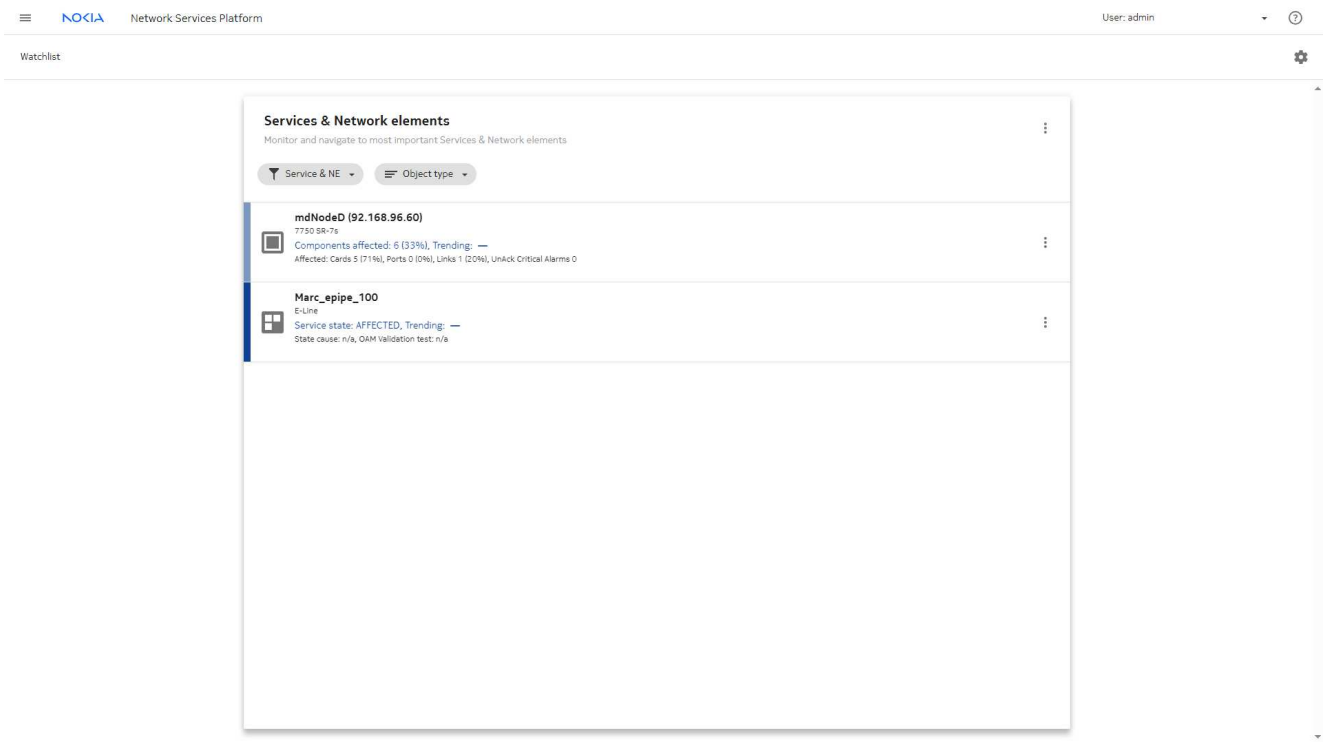


5

Also from the More menu, we can add the service to the Watchlist. Adding an object to the watchlist allows us to navigate quickly and directly to the object in the future. Choose **Add to Watchlist**.

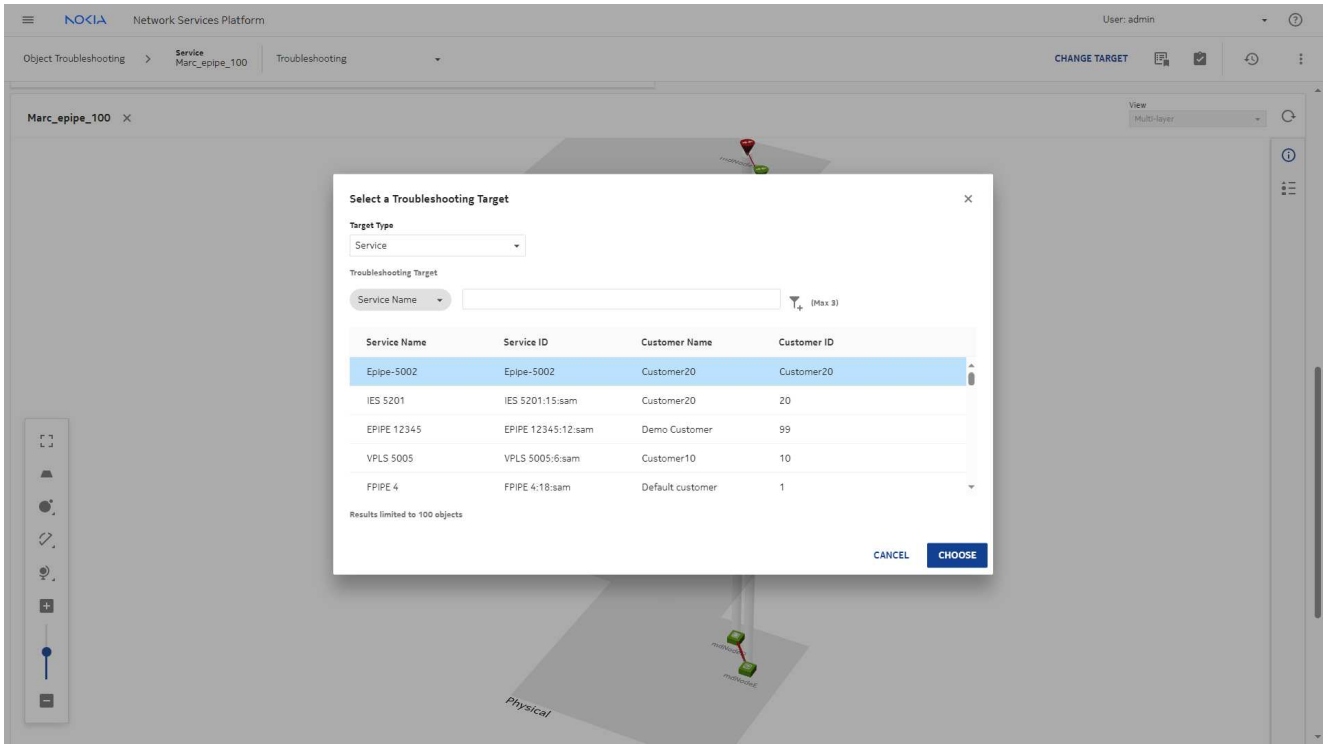


Click **Watchlist** ( ) to view the Watchlist.



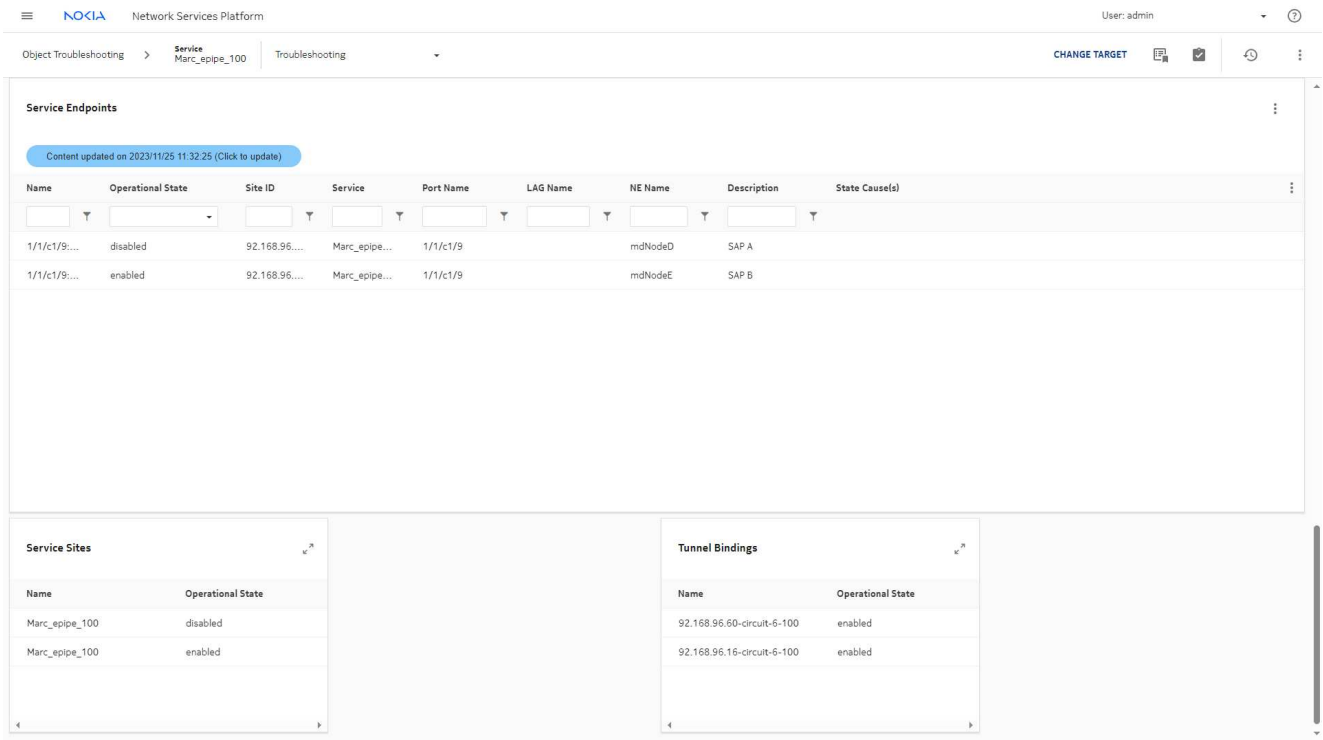
6

You can click **CHANGE TARGET** in the Object Troubleshooting dashboard to troubleshoot other services or objects.



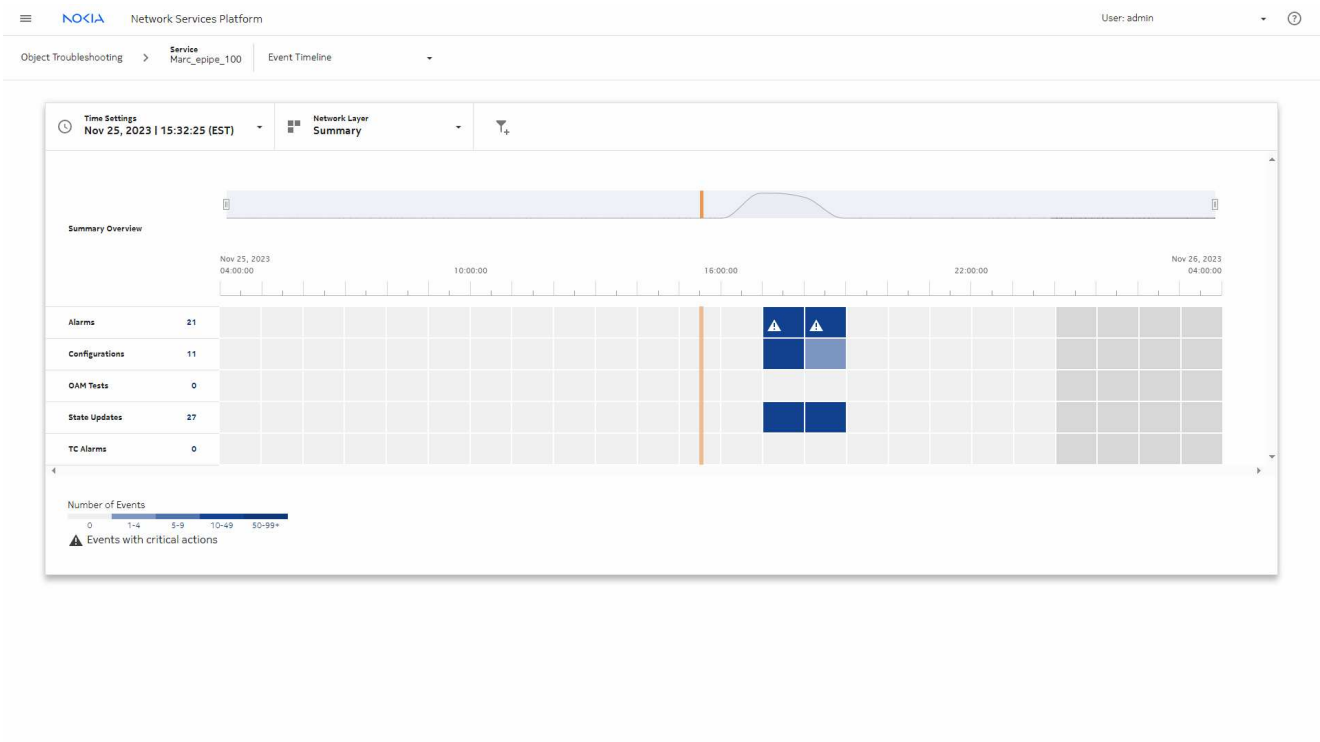
7

Expand the Sites, Tunnel Bindings, and Endpoints dashlets in the Service Inventory area to see details about service components.



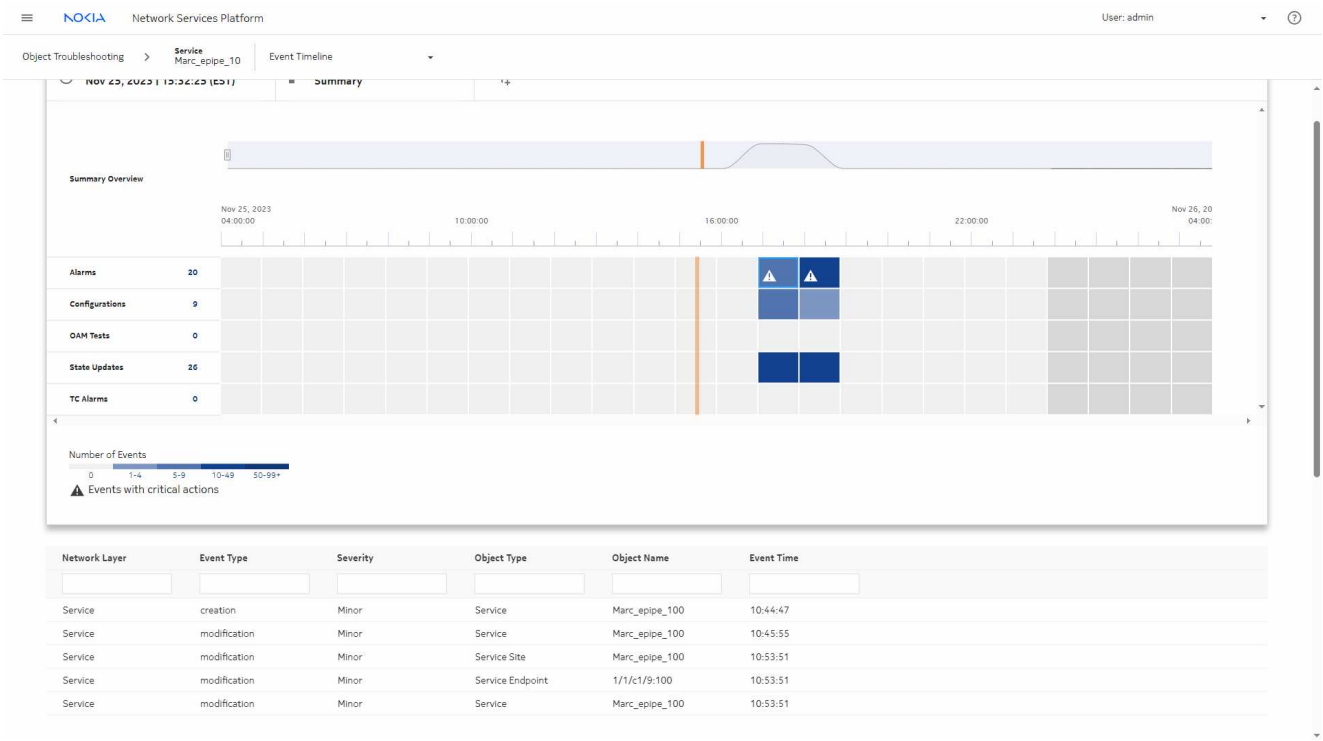
8

Select a faulty endpoint and choose **View in Event Timeline** from the Table row actions menu (⋮) to view a history of events for the service.



9

Click on an event to see a list of actions and alarms associated with the event.

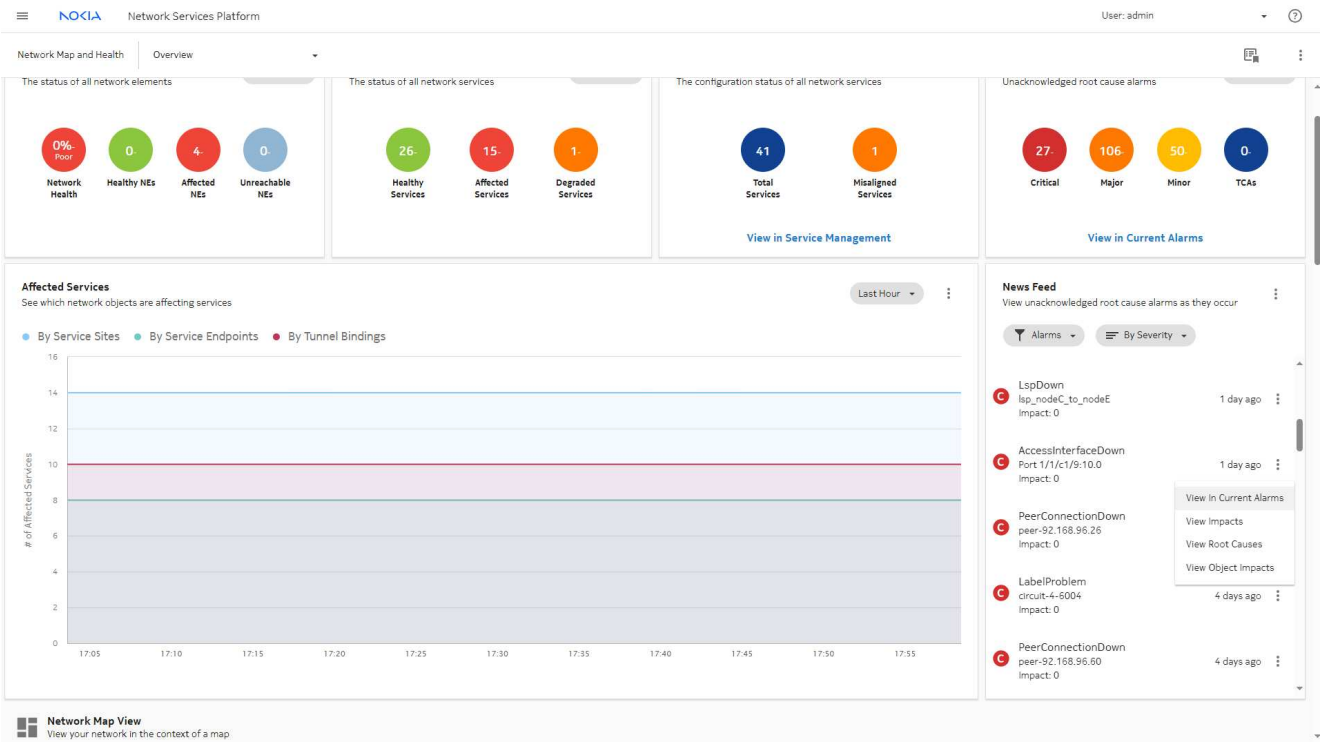


5.8.4 Investigate service alarms from the News Feed

Another option for investigating alarm details is to start from the News Feed. The News Feed provides a live feed of unacknowledged root cause alarms as they occur in real time. Alarm severity and number of impacts are displayed, and cross launch is available depending on the alarm. All alarms can cross launch to the Current Alarm List.

1

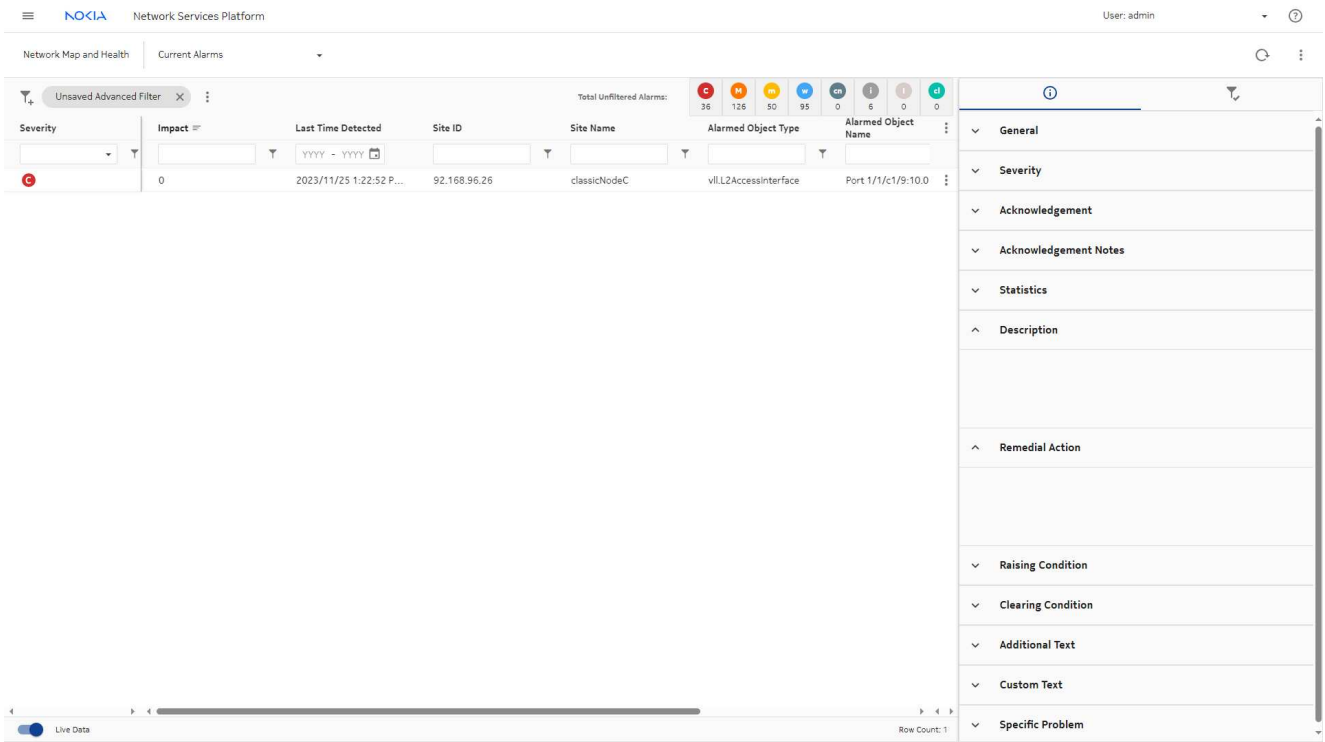
From the **News Feed**, select the alarm and choose **View in Current Alarms** from the More menu.

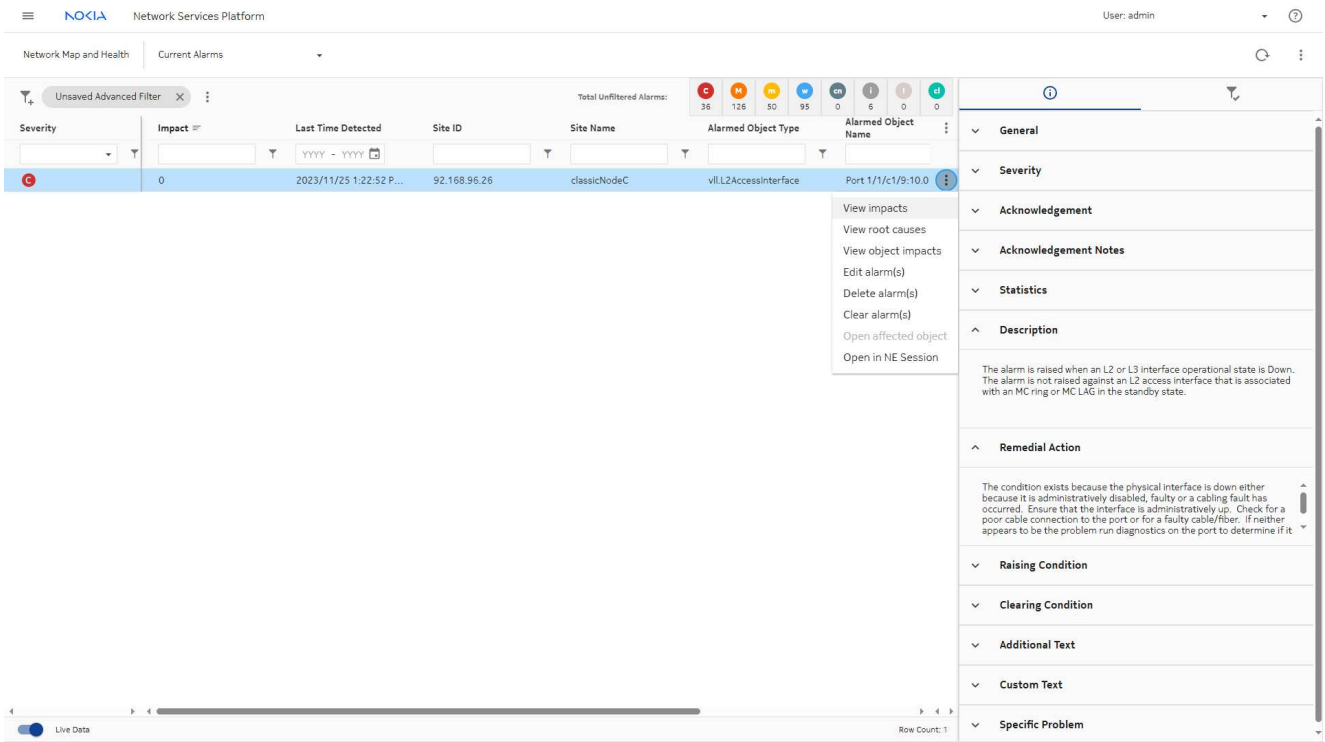


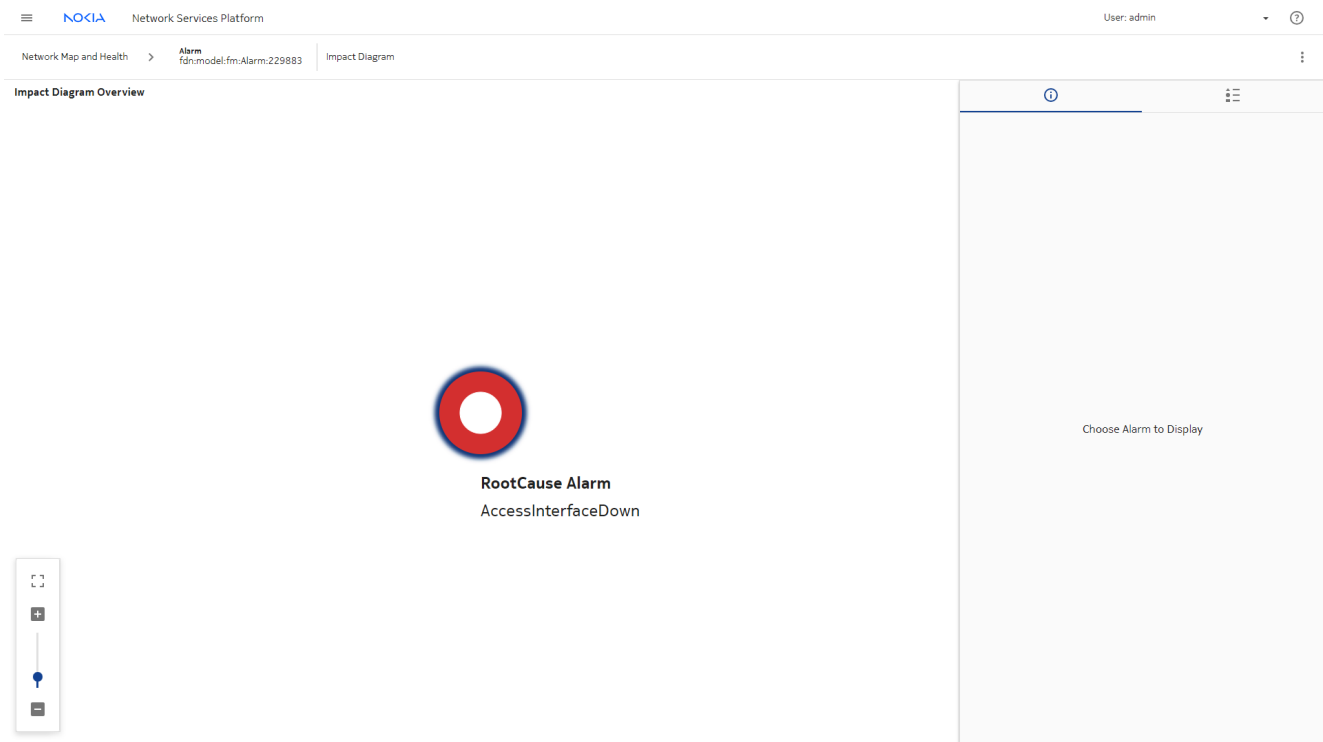
The Current Alarms list opens, with the alarm selected.

2

From the Current Alarms list, you can click **View Impacts** from the table row actions menu for the alarm. This alarm has no impacts.

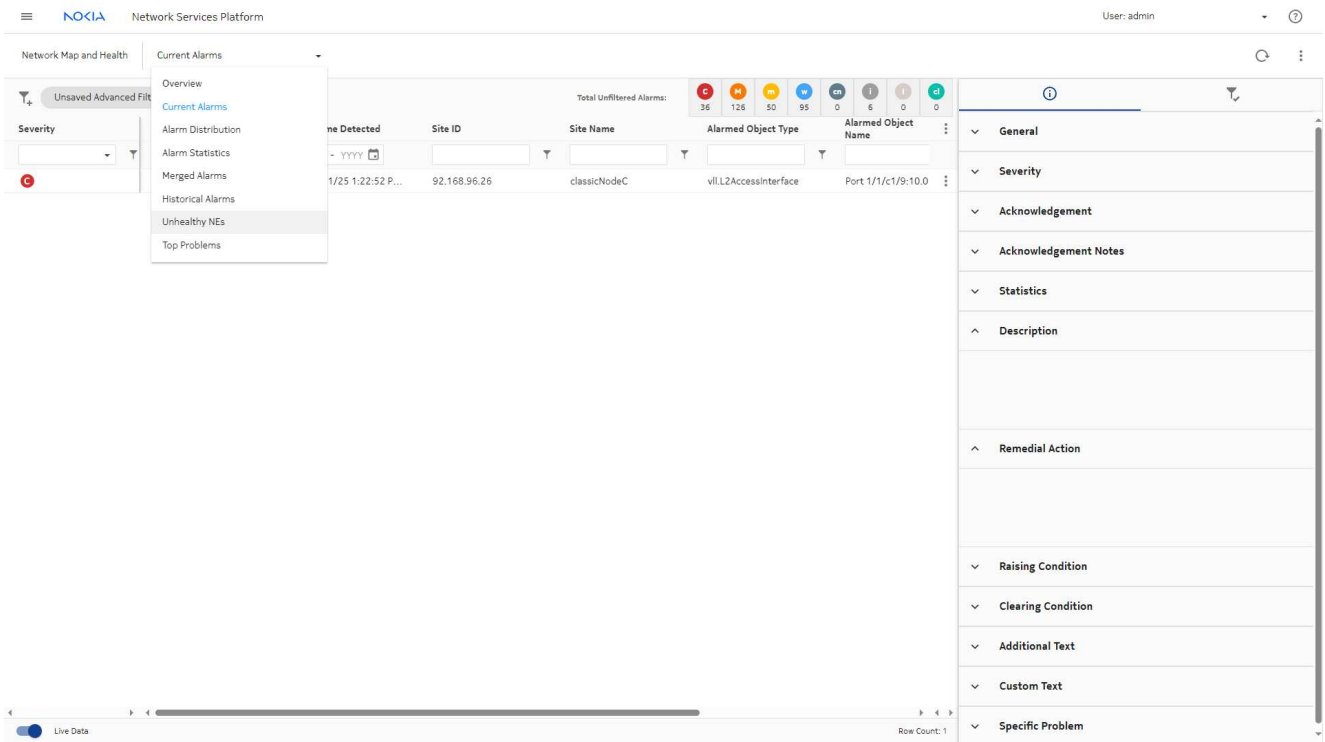


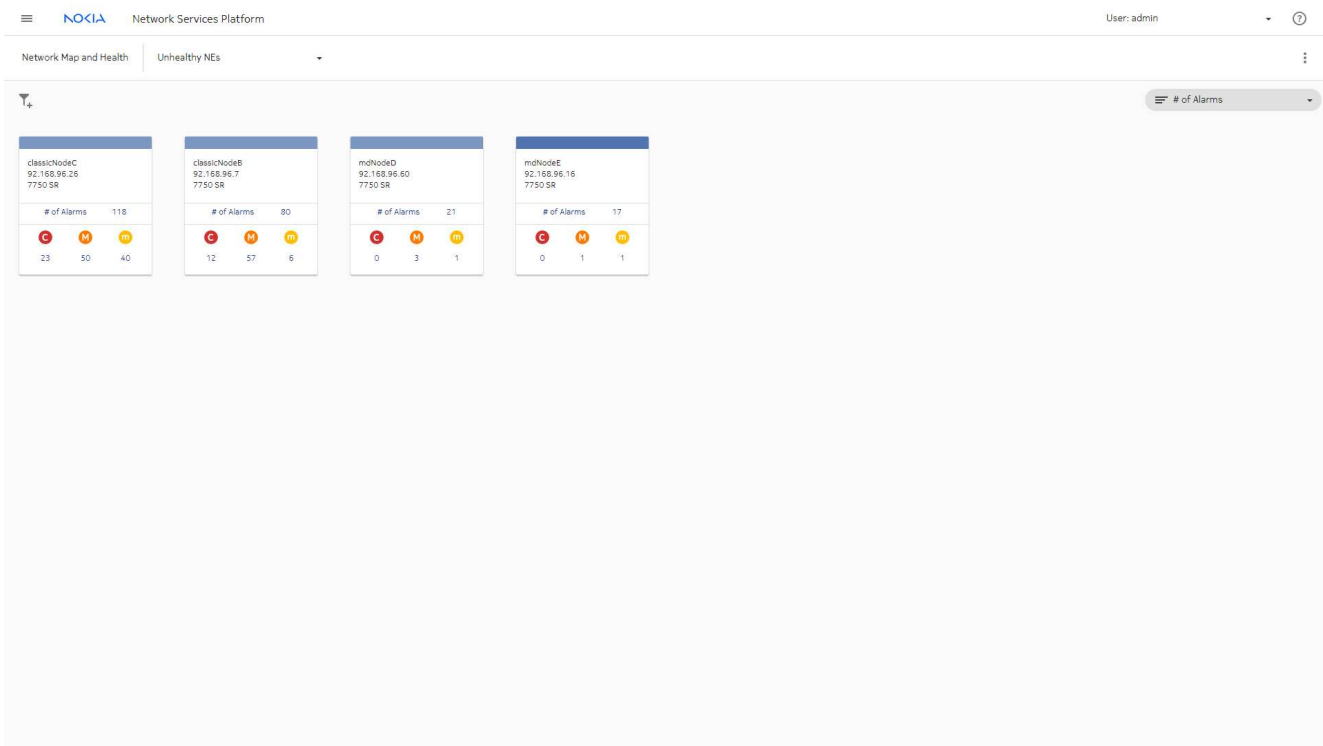


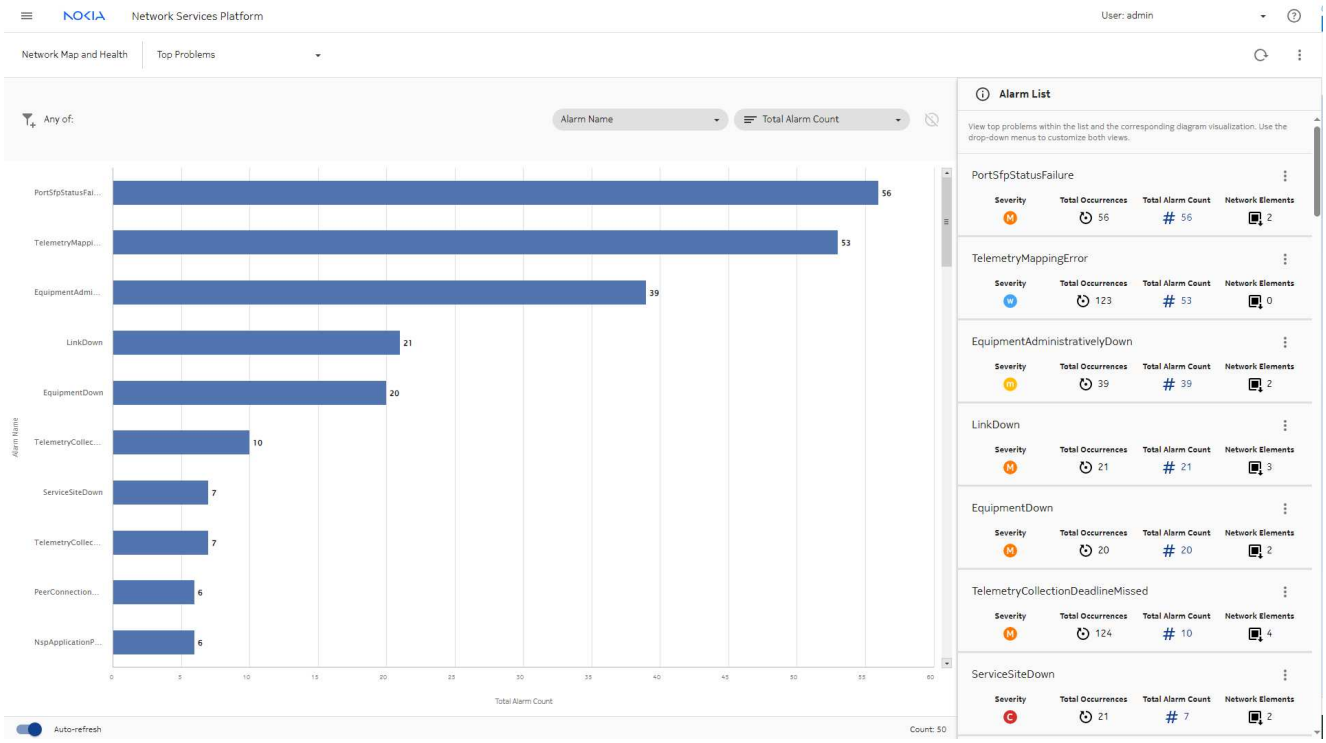


3

Use the drop-down menu at the top of the view to switch to the Top Unhealthy NEs or Top Problems views to see more information about problems in the network.





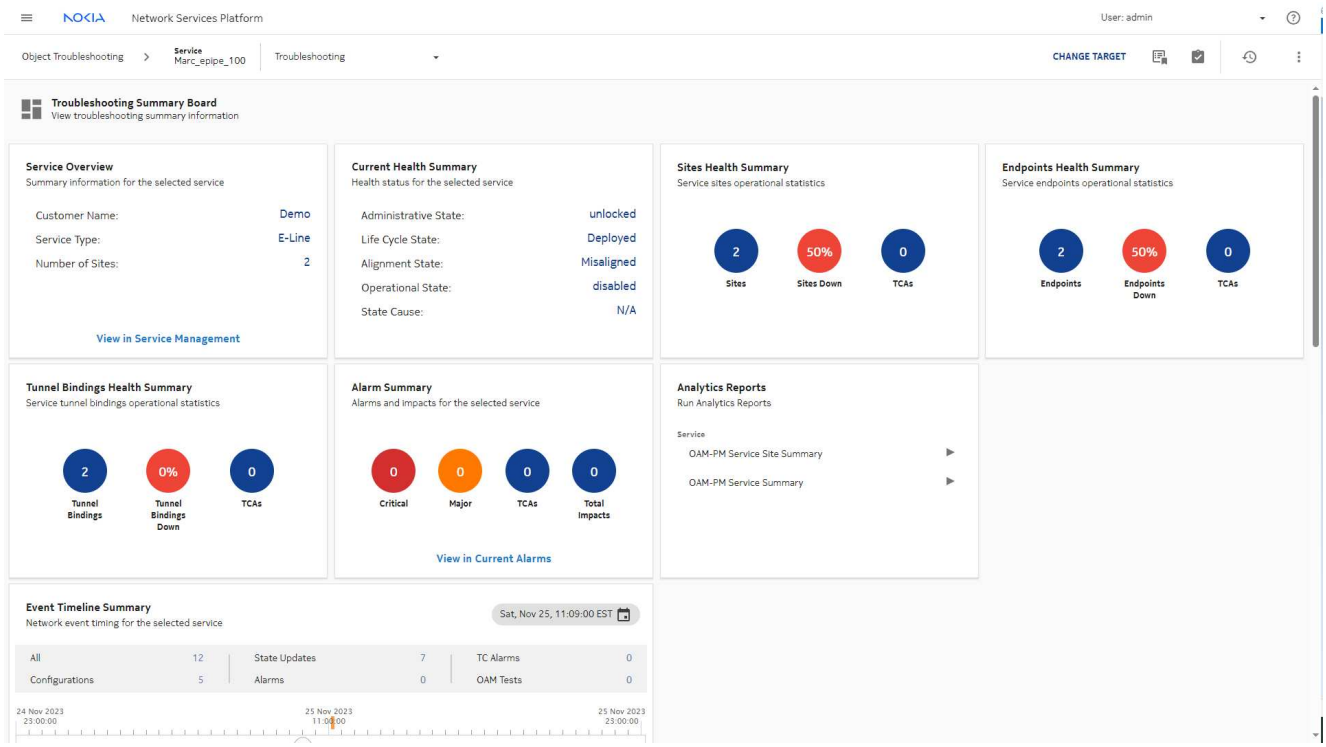


5.8.5 View service provisioning details

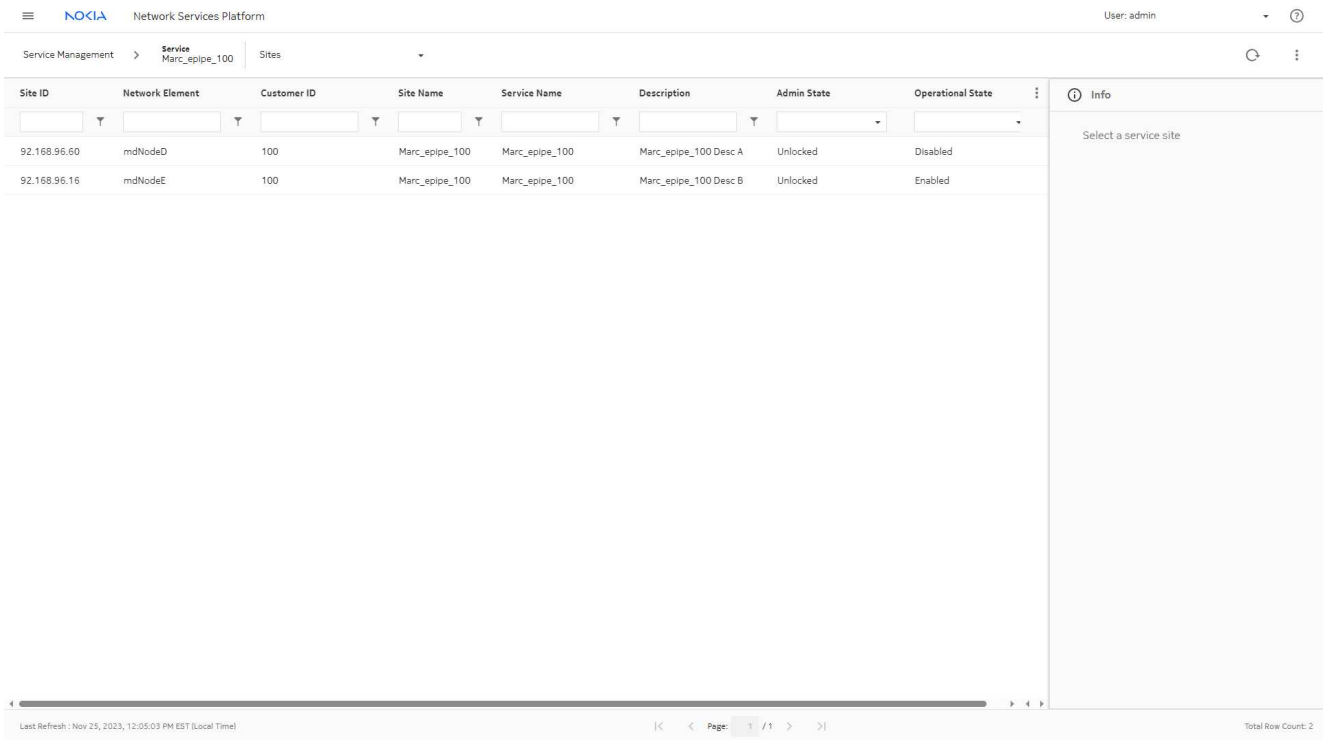
Returning to the Troubleshooting dashboard, we can also launch Service Management to look at the provisioning of the service.

1

From the Service Overview dashlet, click **View in Service Management**.



Service Management opens, filtered to show the service in question.



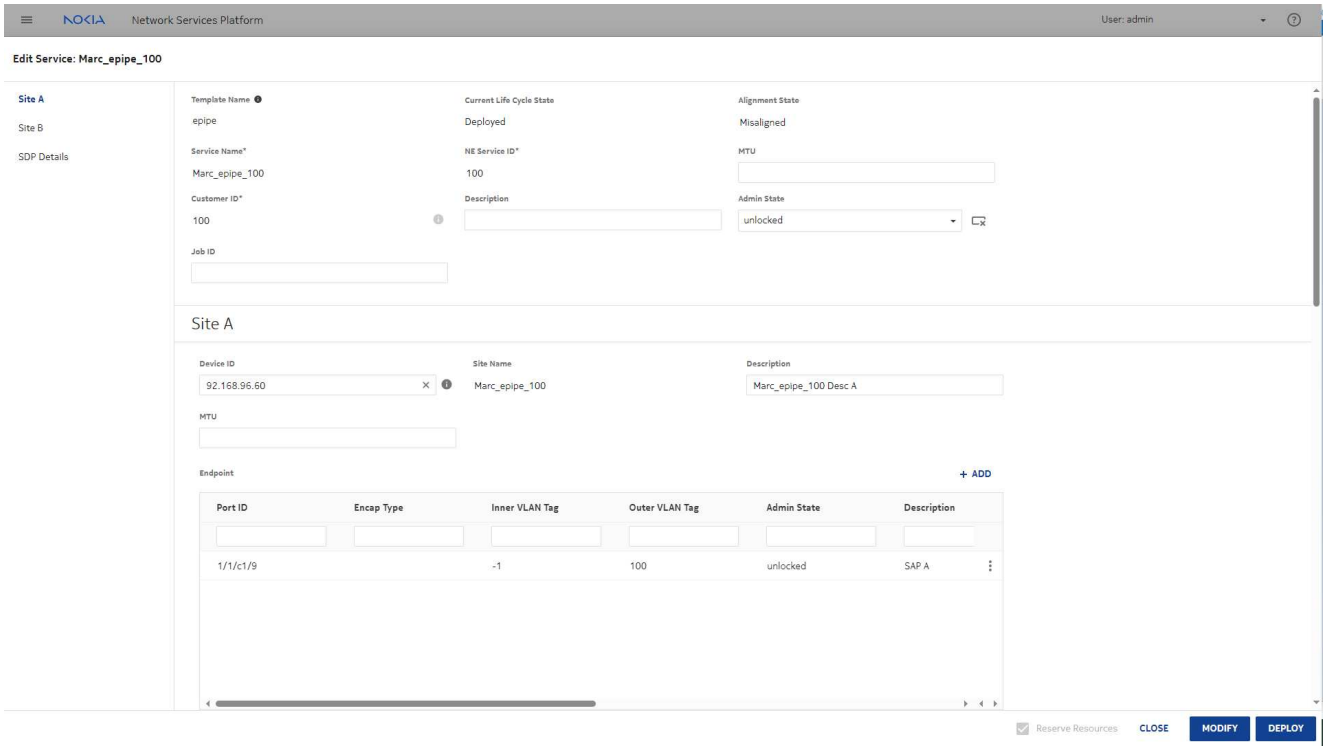
2

From here, we can open the service for editing to verify that the service provisioning is correct. Click ⋮ (Table row actions), **Edit Service**.

3

In the Edit form, we can see that all the mandatory fields for the service are populated and the administrative state is unlocked as expected.

We'll scroll further down to look at the sites.



For both sites, everything looks good. The administration state is unlocked, inner and outer VLAN tags are present and correct.

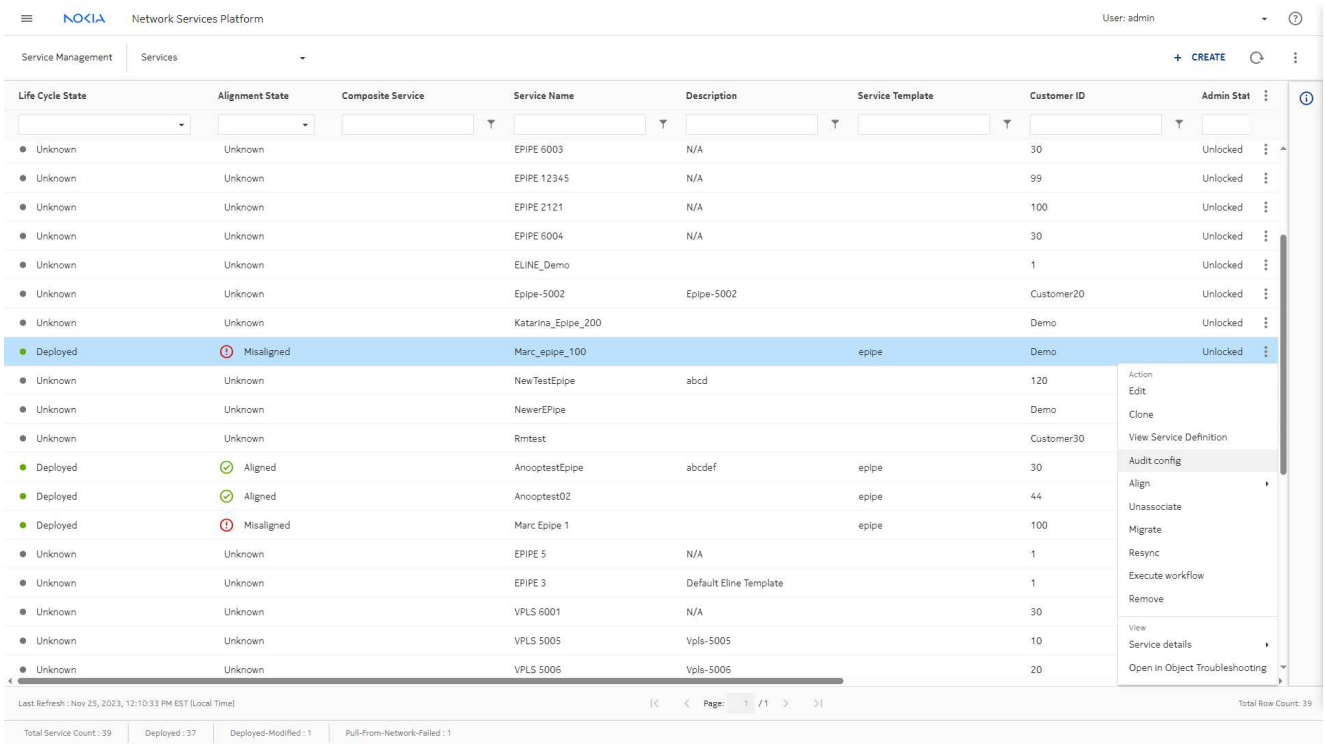
If we scroll further down to look at the service tunnels, they're both unlocked and provisioned with a source and destination.

The provisioning looks good on the NSP side, so we'll close the Edit form.

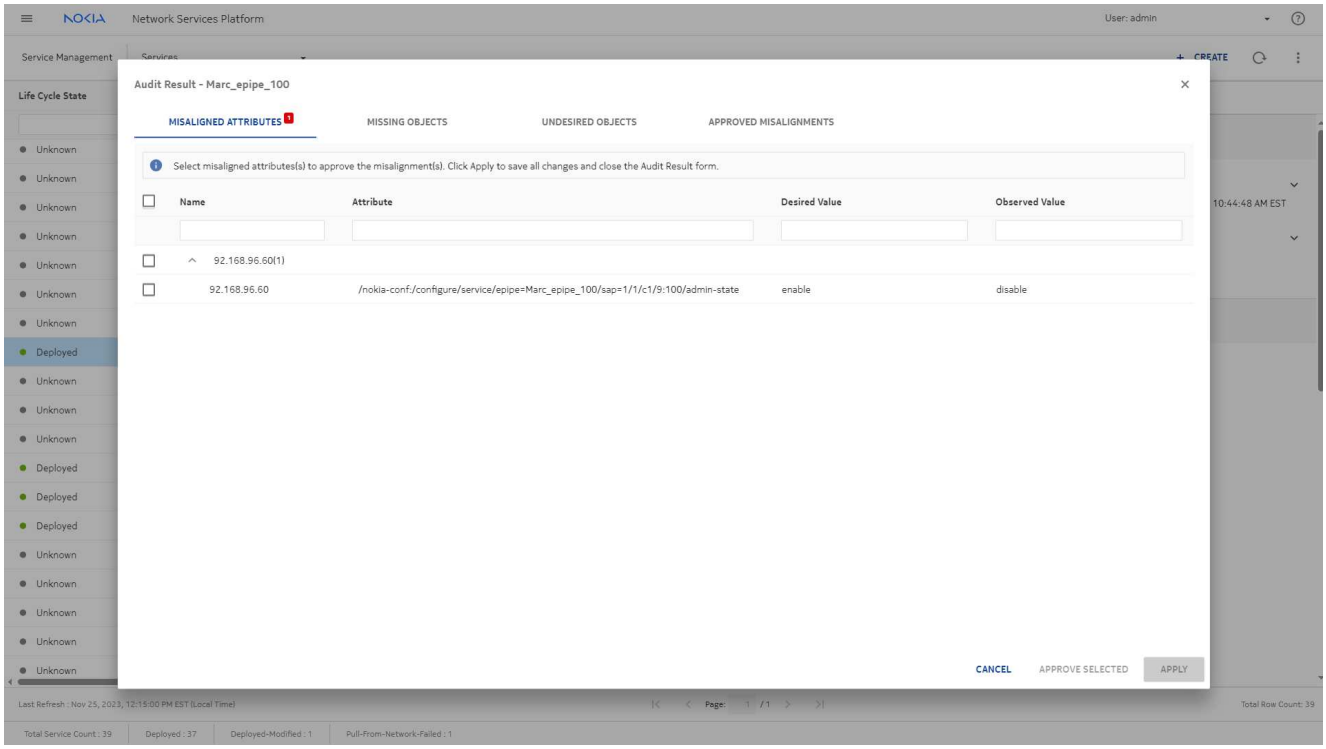
4

The next thing we can do is confirm that the provisioning is also correct on the NEs by doing an audit config. This will compare the configuration on the NSP with what is present on the NE.

From the **Service Management**, **Services** view, select the service and click ⋮ (Table row actions), **Audit config**.



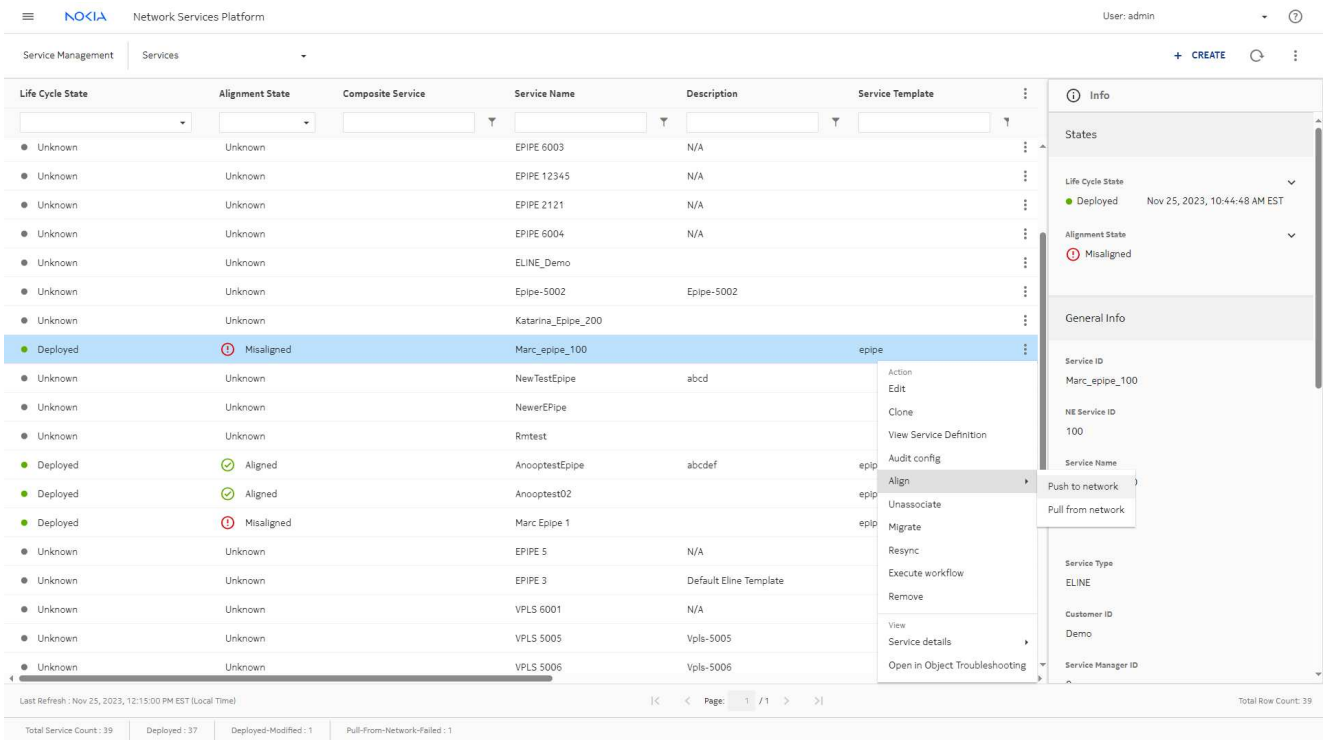
The audit operation has found a misaligned attribute. The NSP configuration shows that the state of this SAP should be enable, but the actual value is disable.



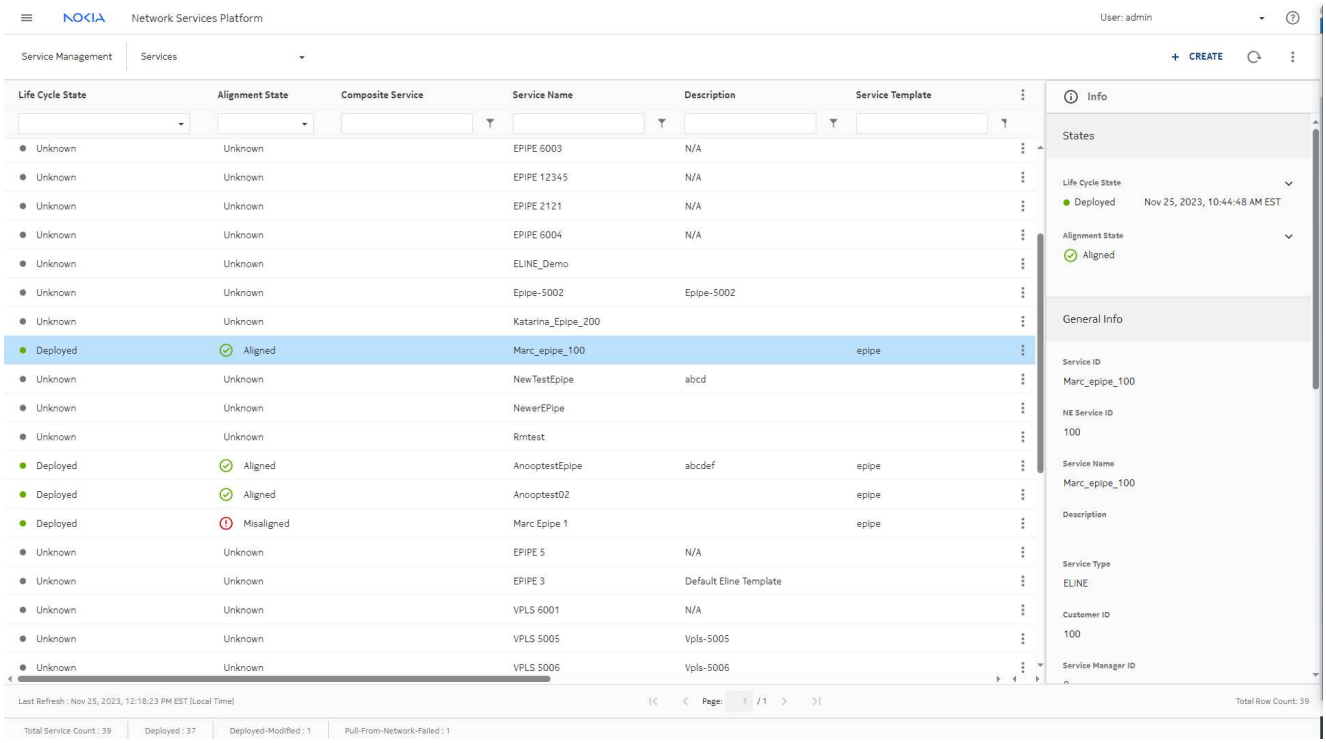
5

Now that we have verified that there is a mismatch between NSP provisioning and the NE, we can use the align function to push the configuration to the network.

From the services tab, click ⋮ (Table row actions), **Align**, **Push to network** and confirm.



When the alignment operation is complete, the Alignment State shows as Aligned. Within a minute or two, the operational state should be changed to enabled and the service should be working.



5.9 End-to-end link troubleshooting scenario

5.9.1 Purpose

This process shows you how to use NSP in troubleshooting issues on links.

In this scenario, a link is experiencing problems.

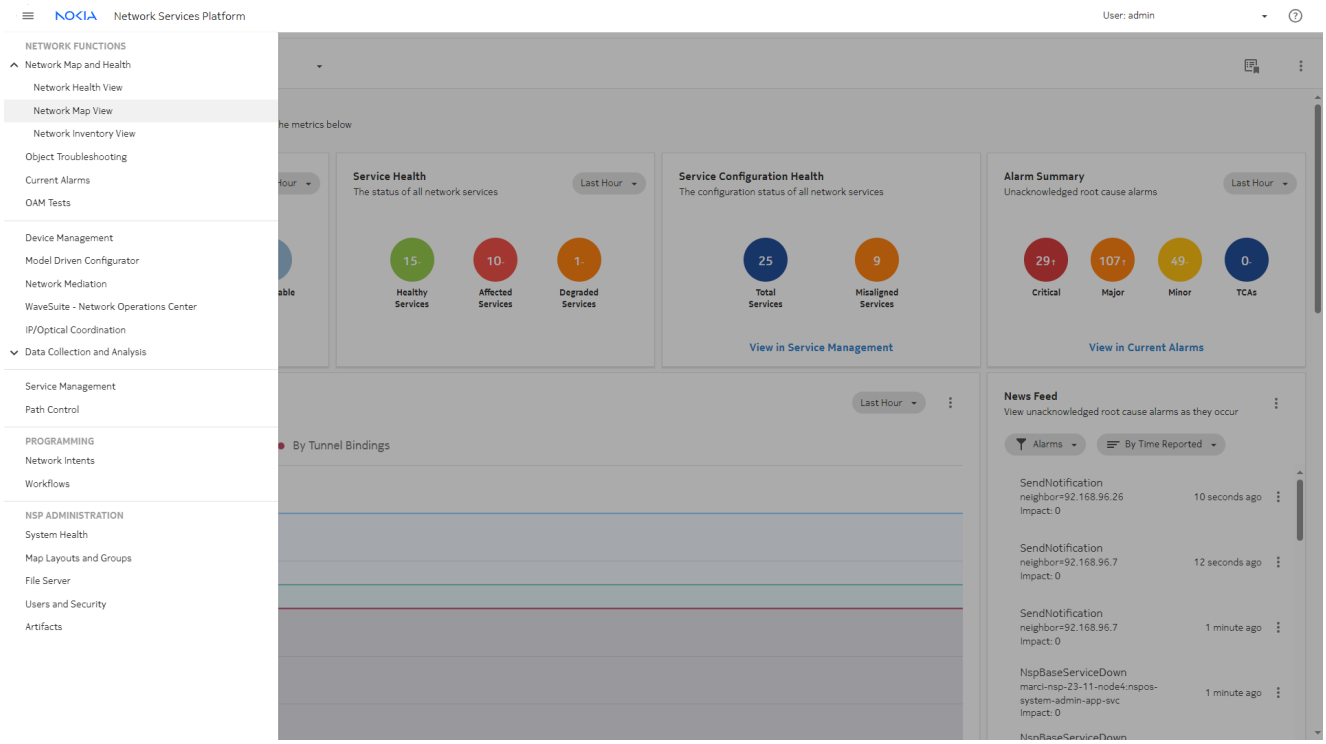
5.9.2 View the Network Map

1

The Network Map provides a graphical view of links in the network. Problem links are displayed in red on the map.

Open **Network Map and Health**, **Network Map View**.

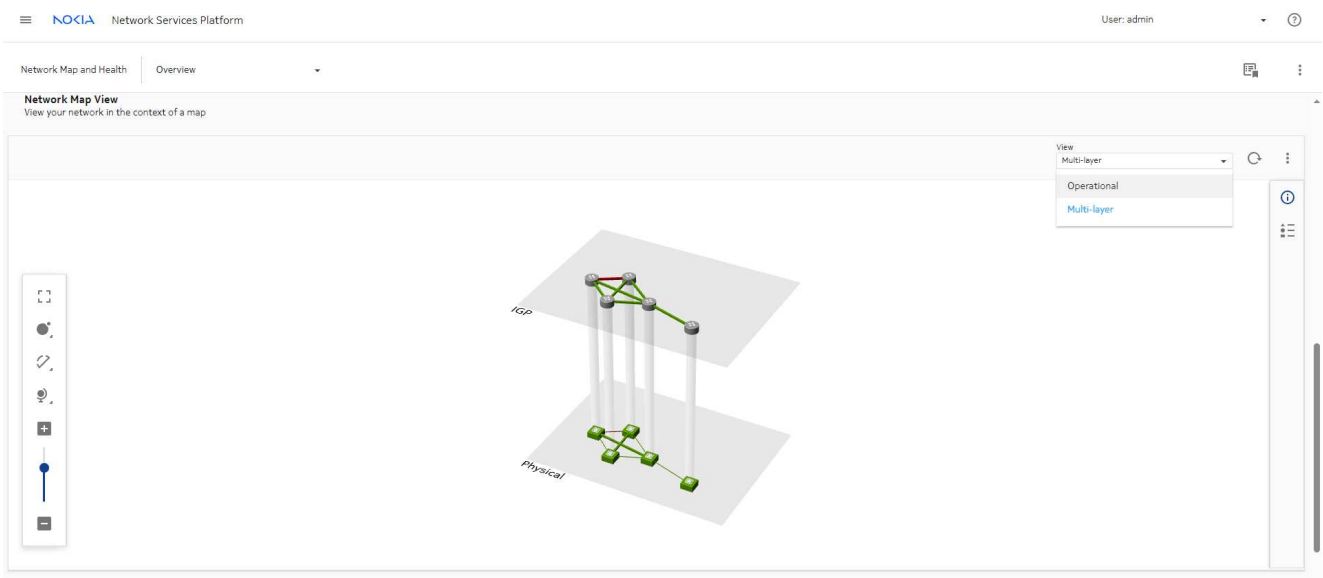
Hover over a problem link to display link details.



2

Choose **Multi-layer** from the **View** drop-down above the map to show the IGP links in a plane above the physical links.

If there are problems in both layers, the link is displayed in red on both planes.



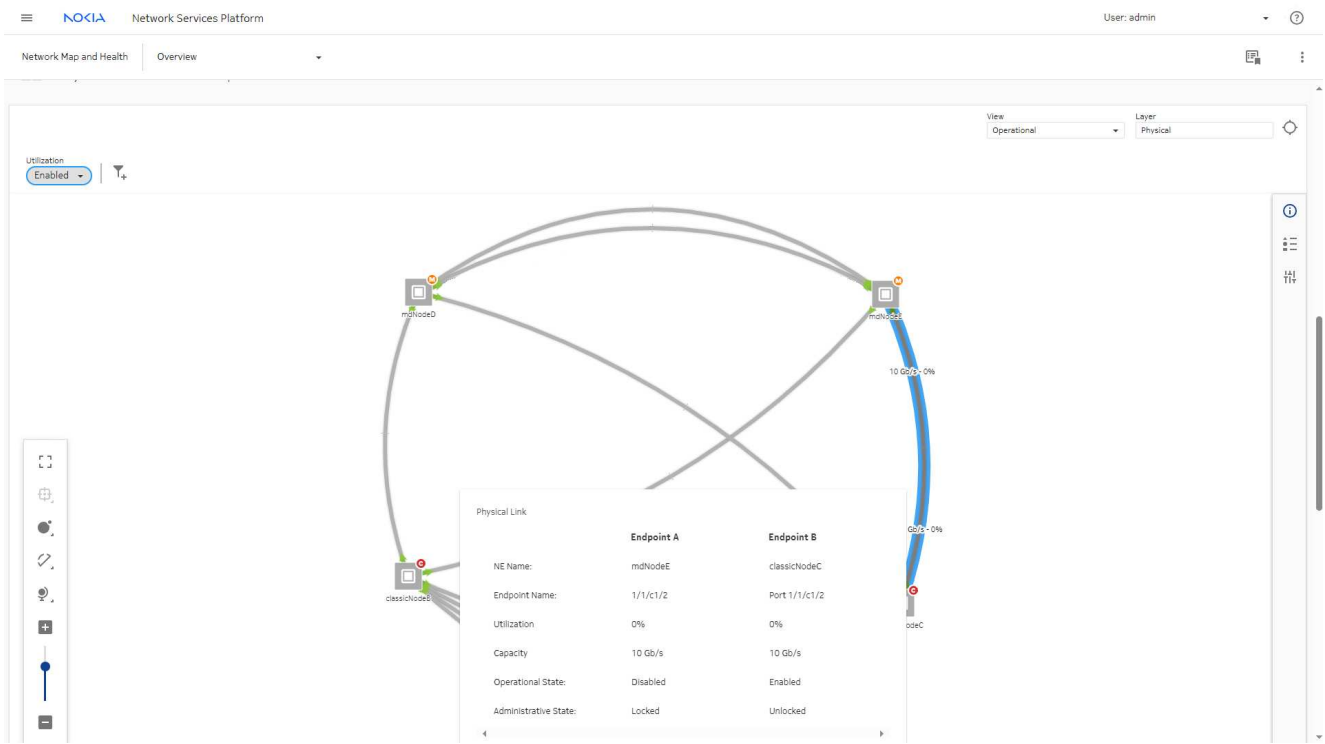
3

Choose Operational from the View drop-down to return to the previous view.

4

We can view utilization data from the **Network Map**.

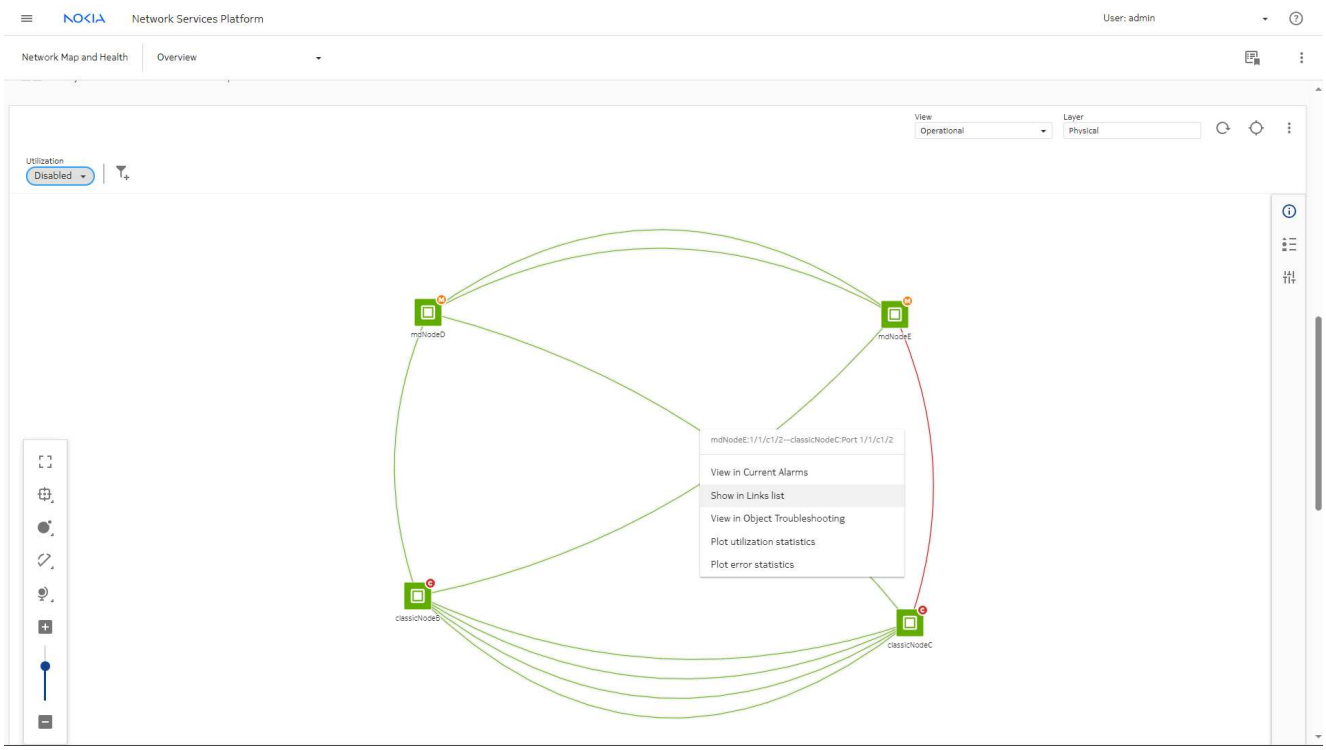
Choose **Enabled** from the **Utilization** drop-down. With utilization enabled, hover over the problem link to see utilization information. Utilization on our link of interest is currently zero.



5

We can also open a utilization tracking chart from the link list in the **Network Map and Health** dashboard.

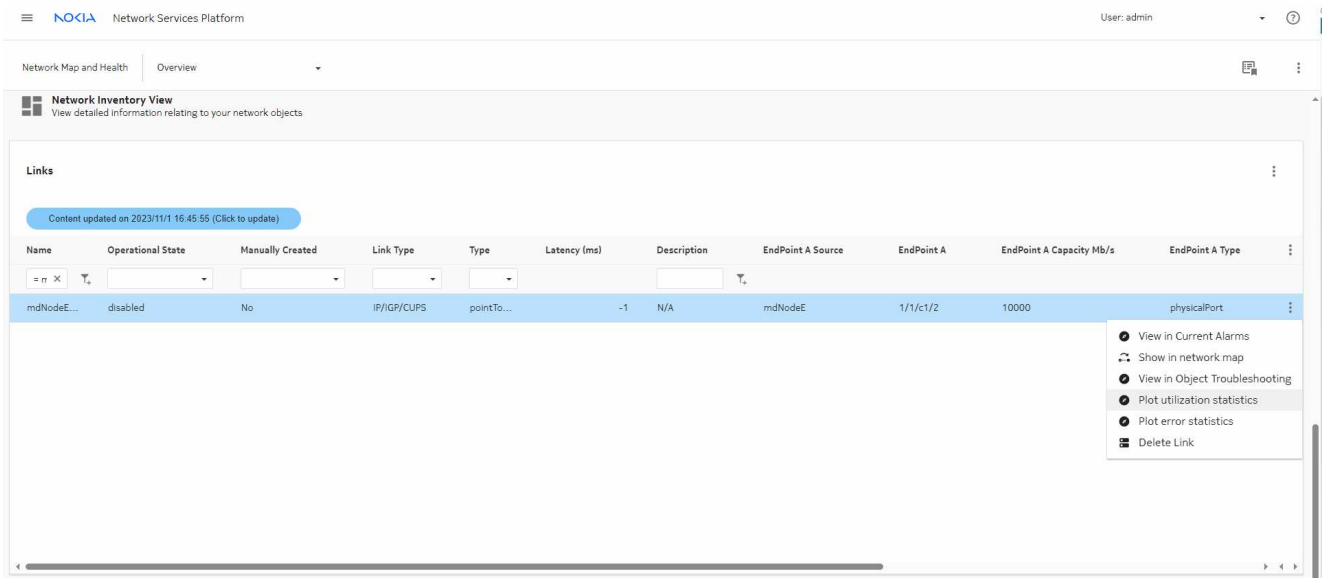
Choose **Disabled** from the **Utilization** drop-down, then right-click on the link and choose **Show in Links list** from the context menu.



The **Links** dashlet in the **Network Map and Health** dashboard opens, filtered to the target link.

6

Click on the link and choose ⋮ (Table row actions), **Plot utilization statistics**.



7

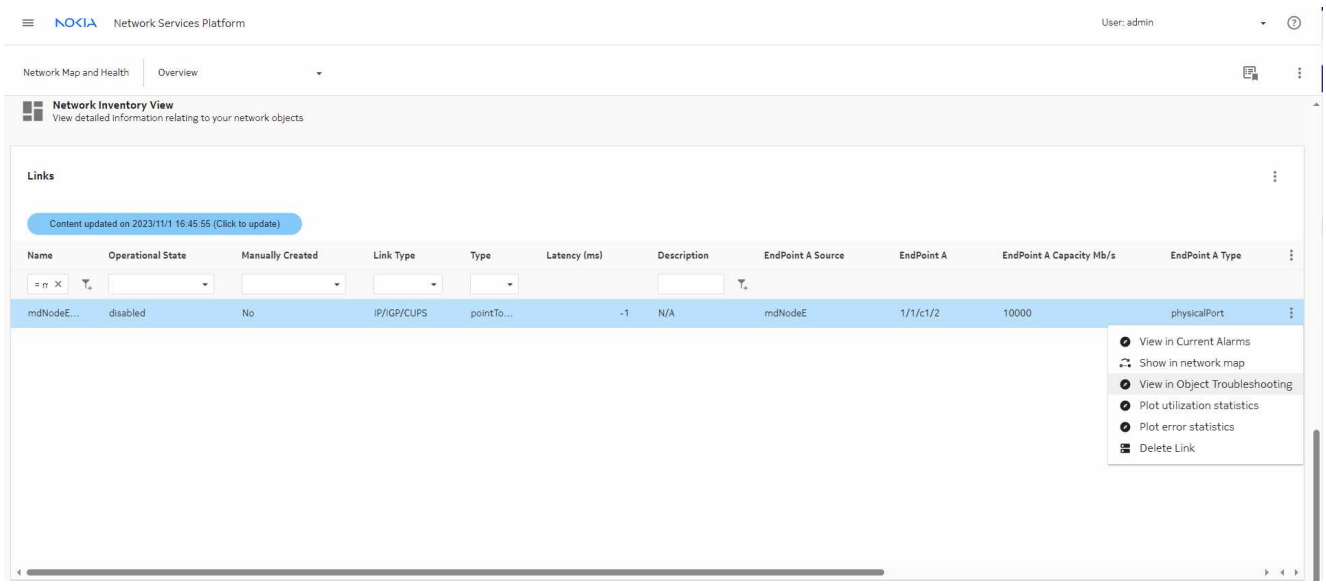
A new tab opens in **Data Collection and Analysis Visualizations**, showing utilization charts.

We'll leave the tab open to check again later.

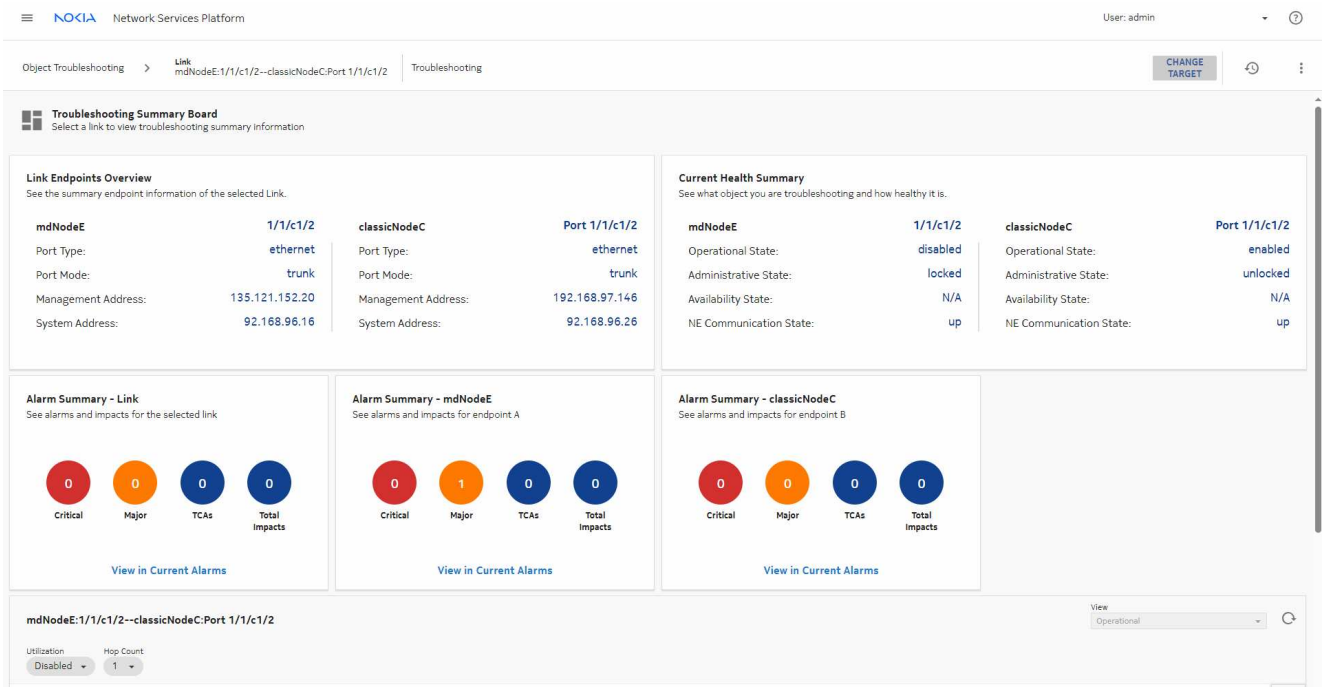
5.9.3 Investigate from the Object Troubleshooting dashboard

1

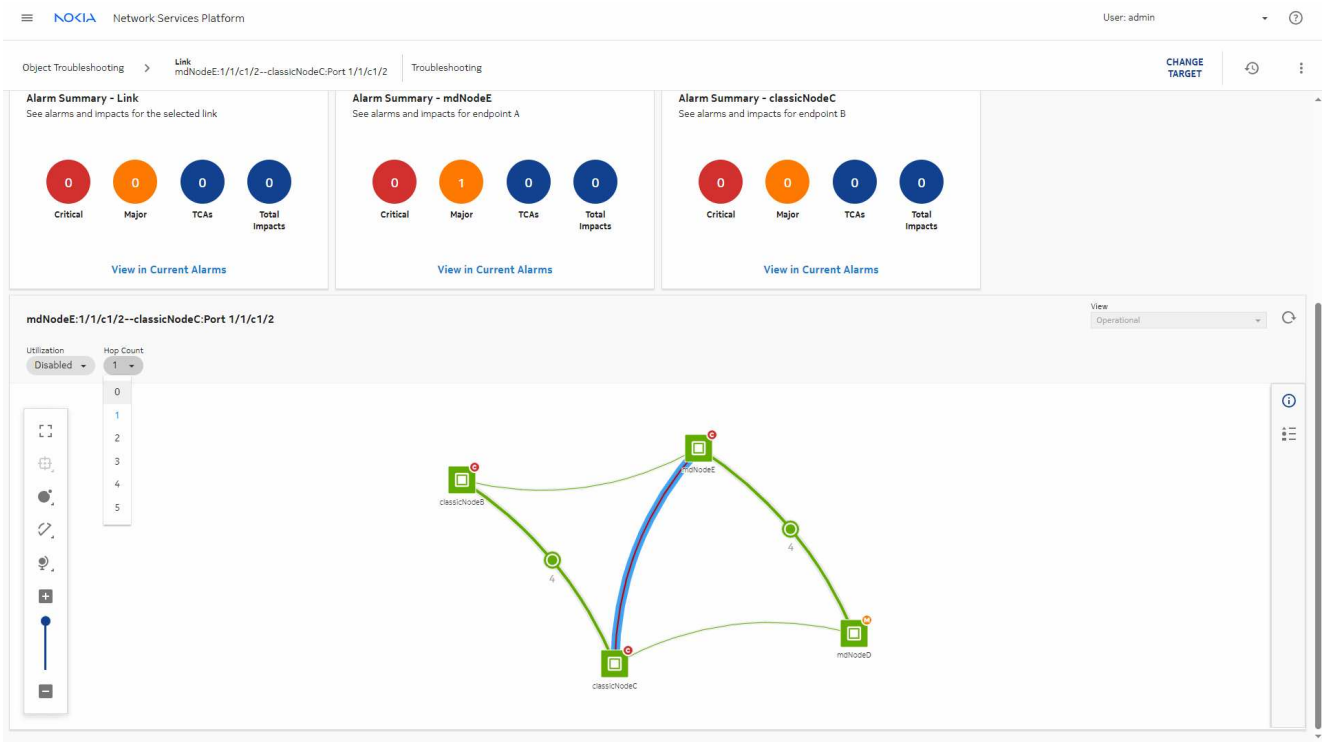
Returning to the **Links** dashlet, choose ⋮ (Table row actions), **View in Object Troubleshooting**.



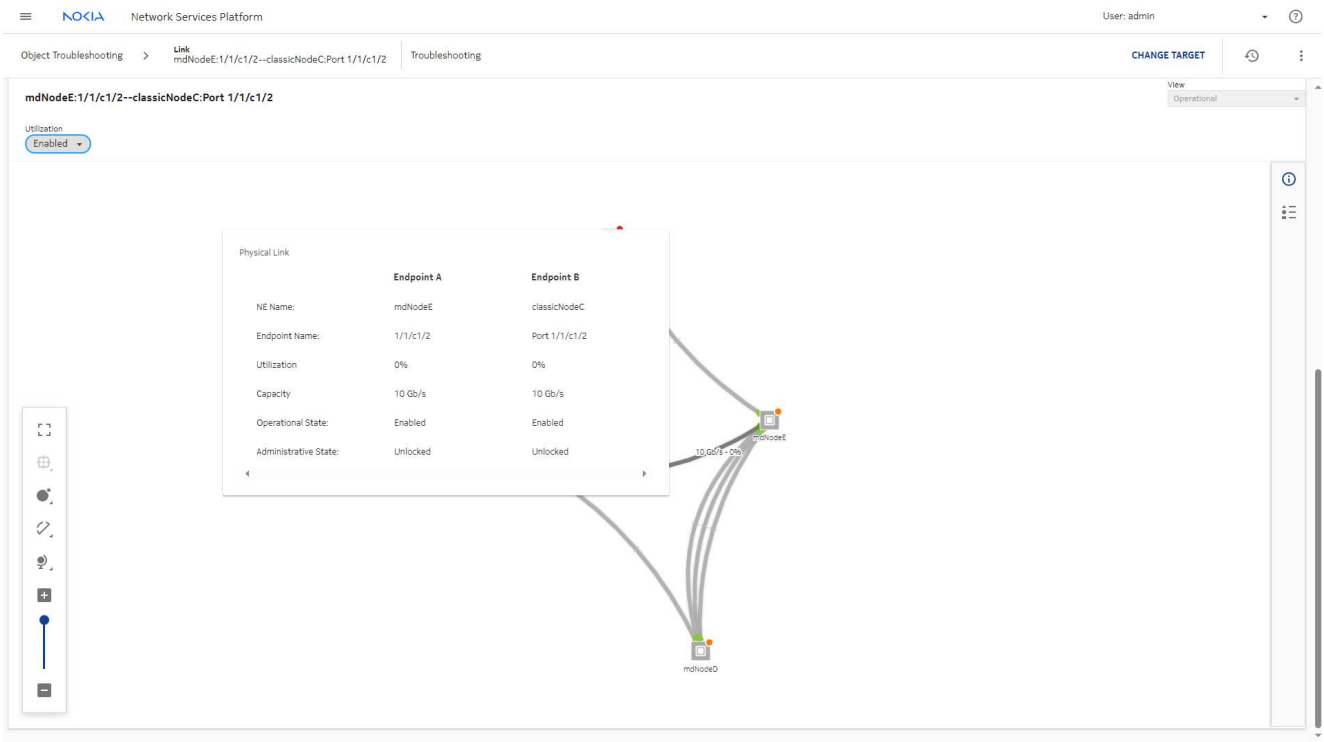
The **Object Troubleshooting** dashboard shows summary dashlets with information about our object of interest. You can click **CHANGE TARGET** to view another object if needed.



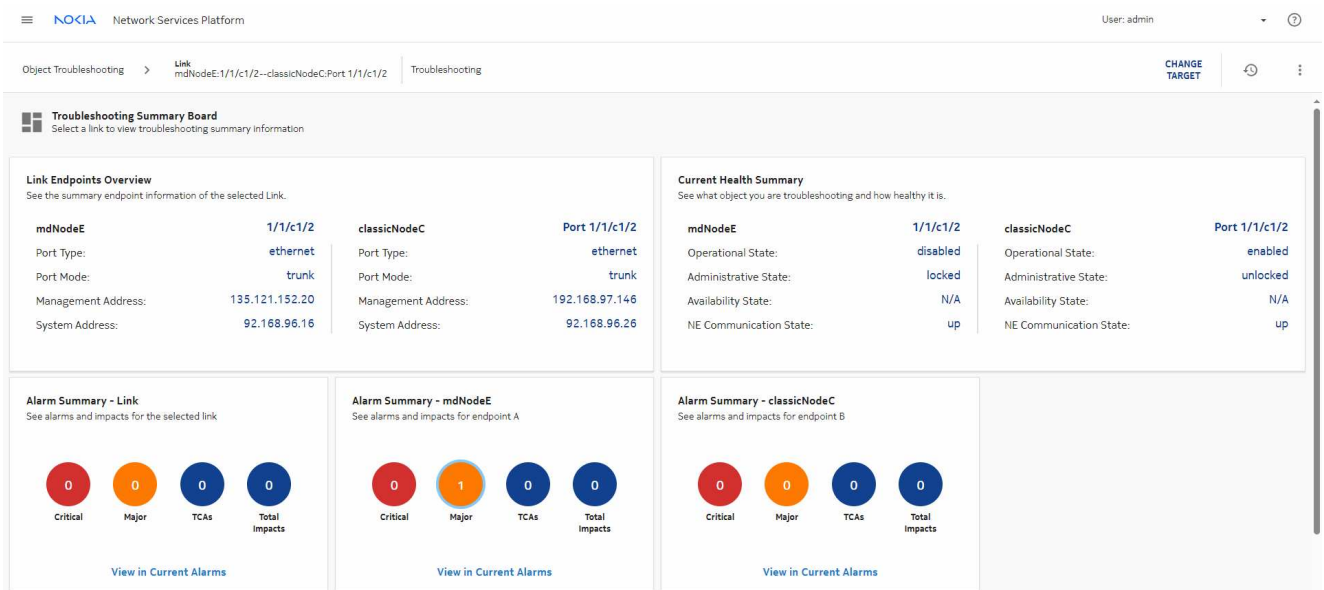
In the **Object Troubleshooting** dashboard map, we can change the **Hop Count** to see nodes that are further from the target.



You can select **Utilization** to display link utilization statistics on the Troubleshooting map, just as we can on the Network map.

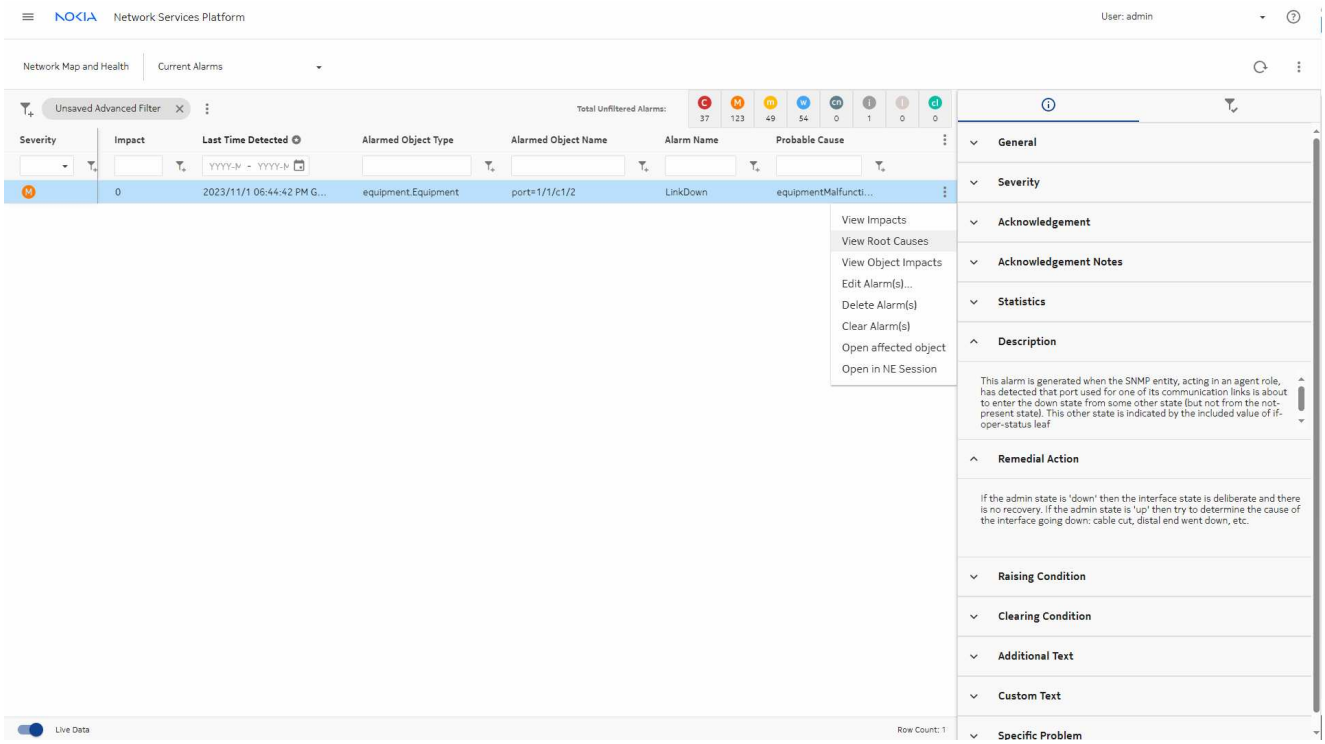


Back in the **Object Troubleshooting** dashboard, navigate to the **Alarm Summary** dashlet and click the **Major** alarm circle to view **Current Alarms** with a filter for the pertinent alarm.

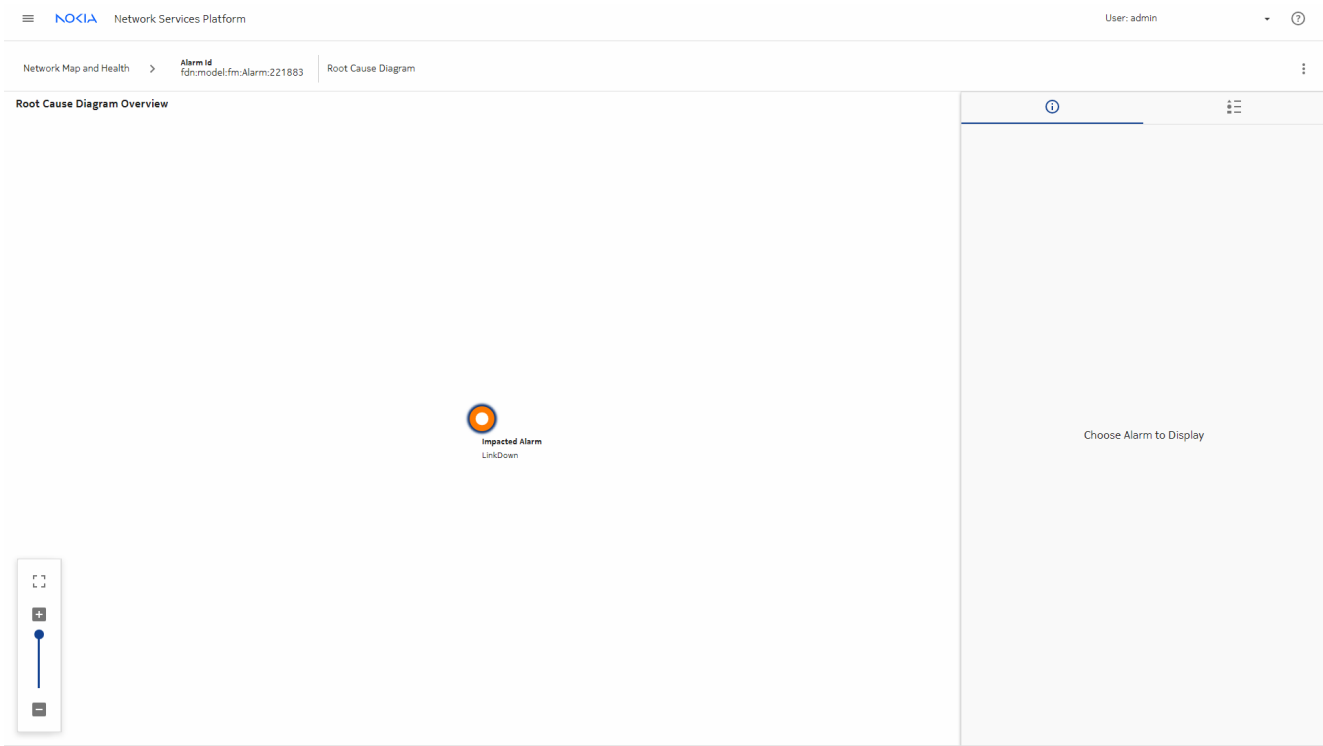


We can see that there are no impacts, but there may be a root cause.

Click on the alarm, choose ⋮ (Table row actions), select **View Root Causes**.



In this case, the root cause diagram does not show a specific root cause: the alarm in question is the only one present.

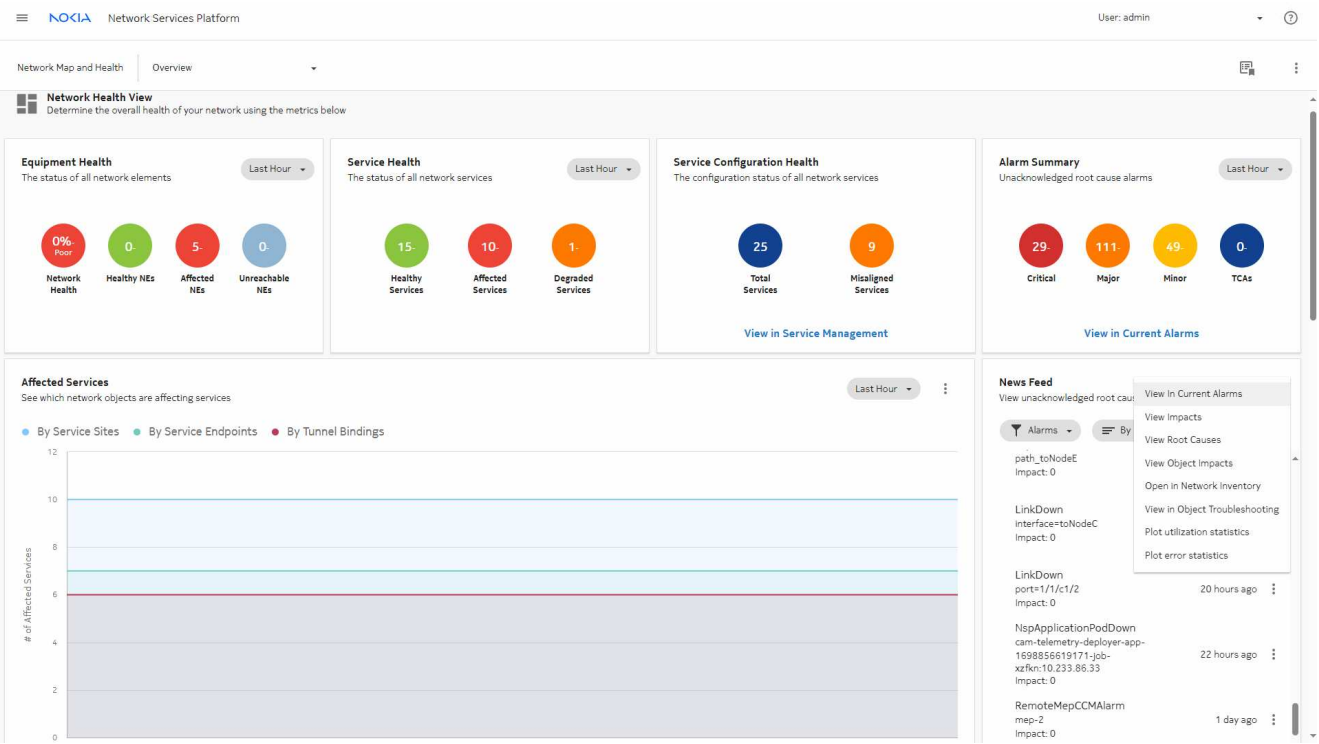


5.9.4 Investigate link alarms from the News Feed

Another option for investigating alarm details is to start from the News Feed. The News Feed provides a live feed of unacknowledged root cause alarms as they occur in real time. Alarm severity and number of impacts are displayed, and cross launch is available depending on the alarm. All alarms can cross launch to Current Alarms.

1

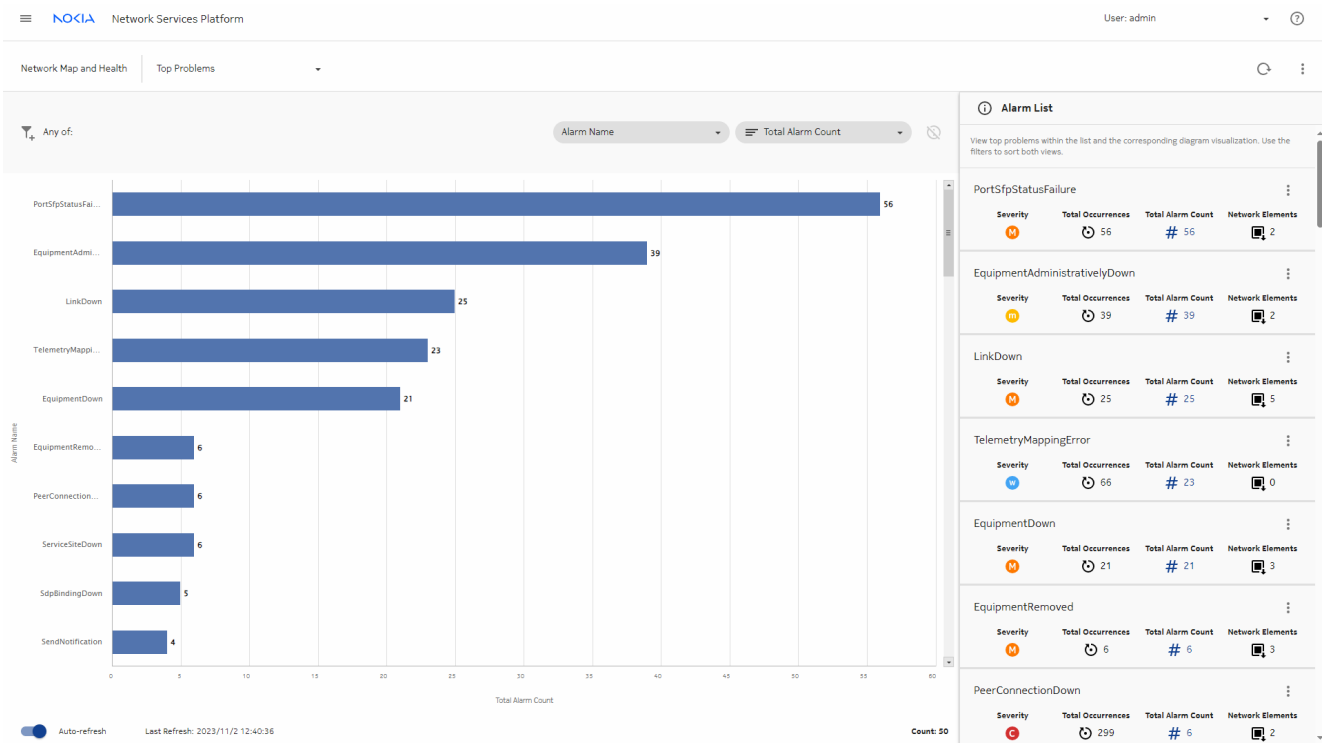
From the **News Feed** in the **Network Map and Health** dashboard, select the alarm and choose **View in Current Alarms** from the More menu.



Current Alarms cross launches, with the alarm selected.

2

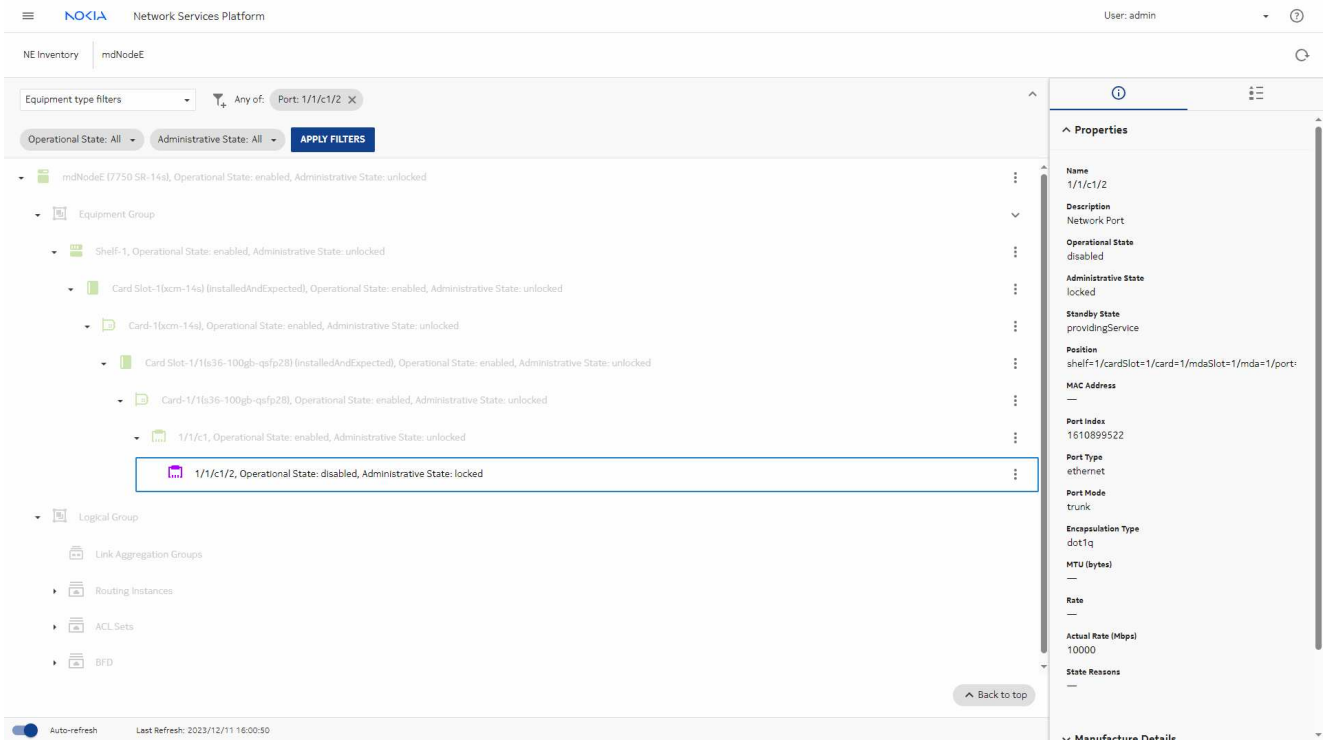
From **Current Alarms**, you can view the NE in the **Unhealthy NEs** tab to see what correlated alarms may be present on the endpoint NEs, or check **Top Problems** to see what other issues the network is experiencing. Here we see that Link Down is currently the third most common problem.



5.9.5 View port details

1

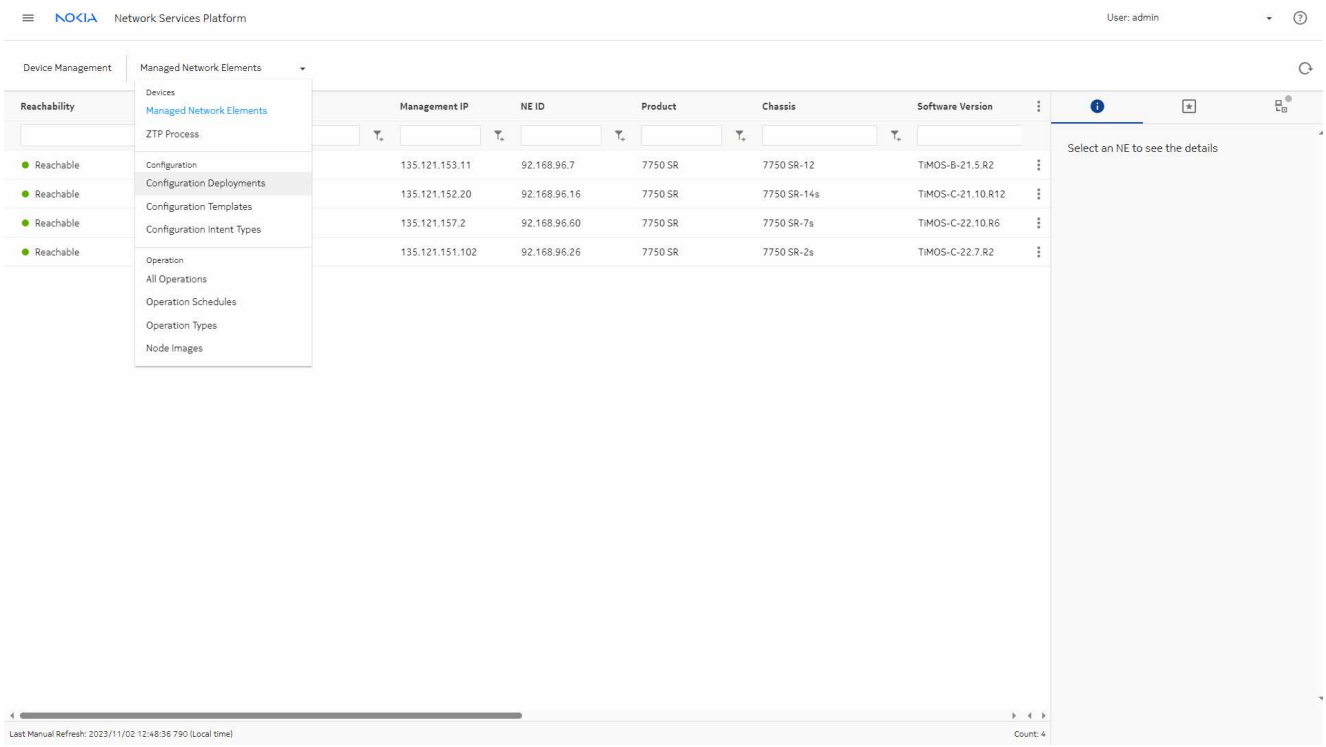
Returning to the **Object Troubleshooting** dashboard, click on one of the ports to cross launch **Network Inventory** to look at the status of the endpoint ports.



5.9.6 Evaluate the NE configuration

1

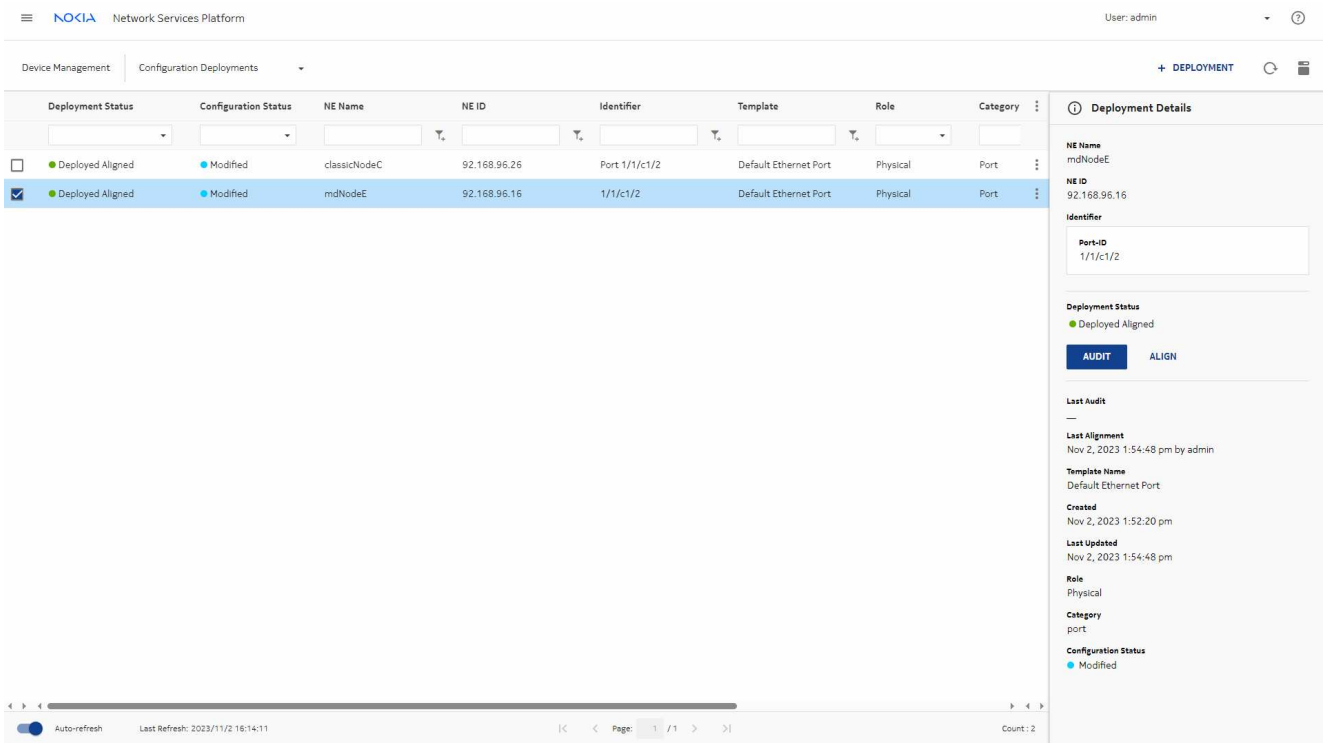
In **Device Management**, select **Configuration Deployments** to check the state of the link endpoint port deployments.



If required, filter the Identifier column with the port number to display the deployments that configured the ports in the link. The deployment status column shows the status from the last audit operation performed.

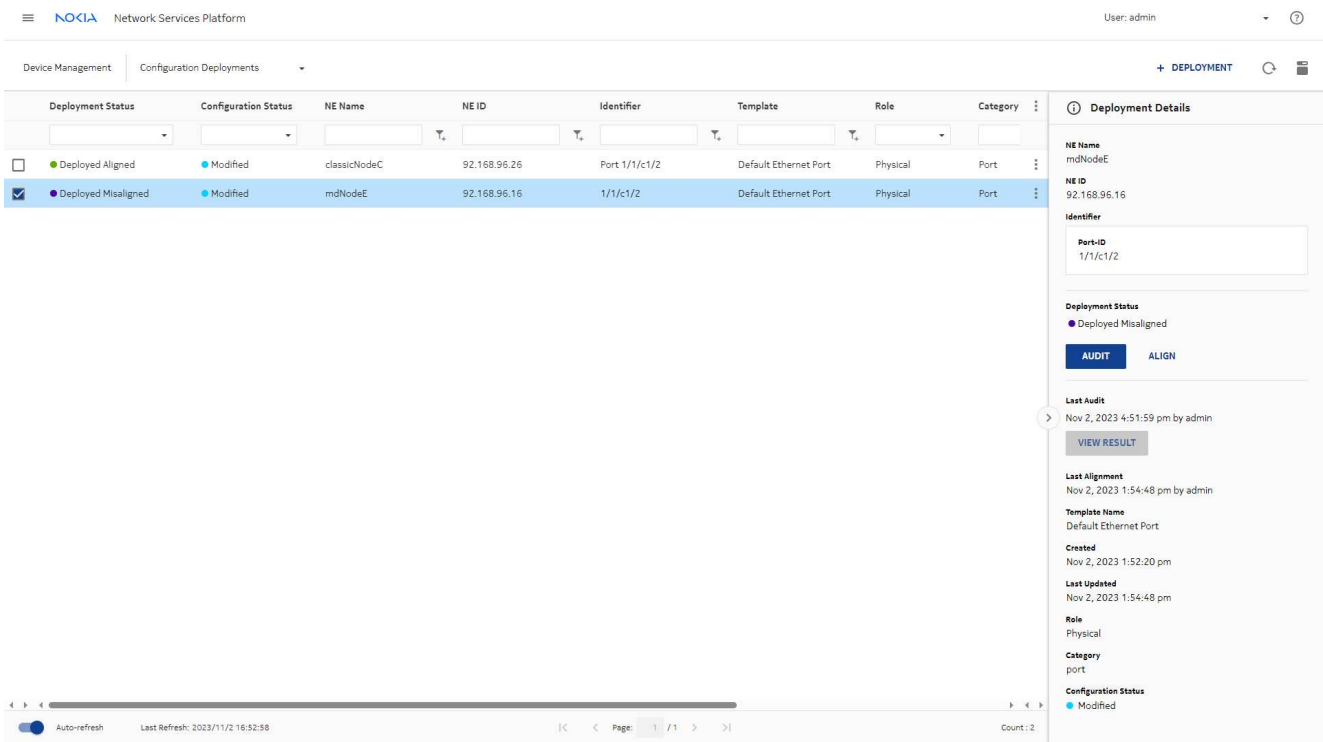
2

For each port, click **AUDIT** in the **Deployment Details** panel to compare the NSP configuration against the NE configuration.

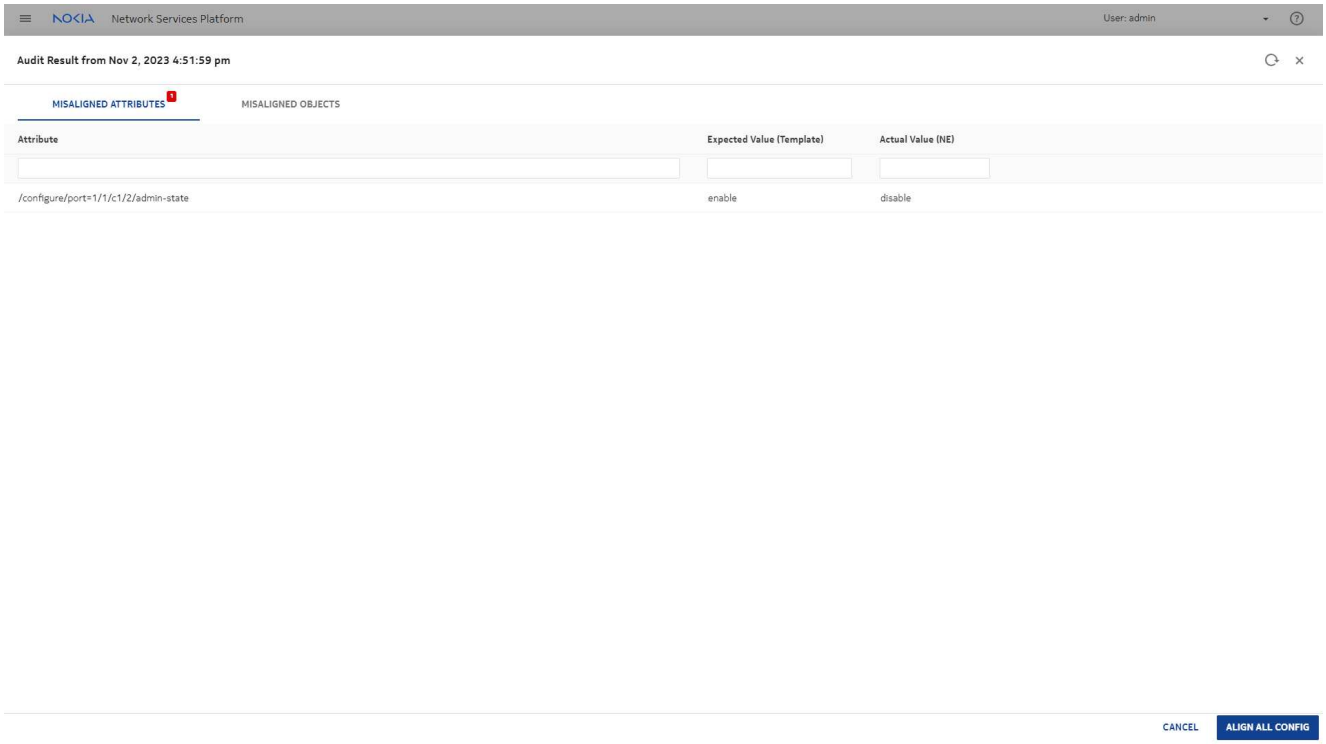


3

After auditing the port deployment, we can see that it is misaligned. Select the deployment and click **VIEW RESULT** to see the results of the audit.

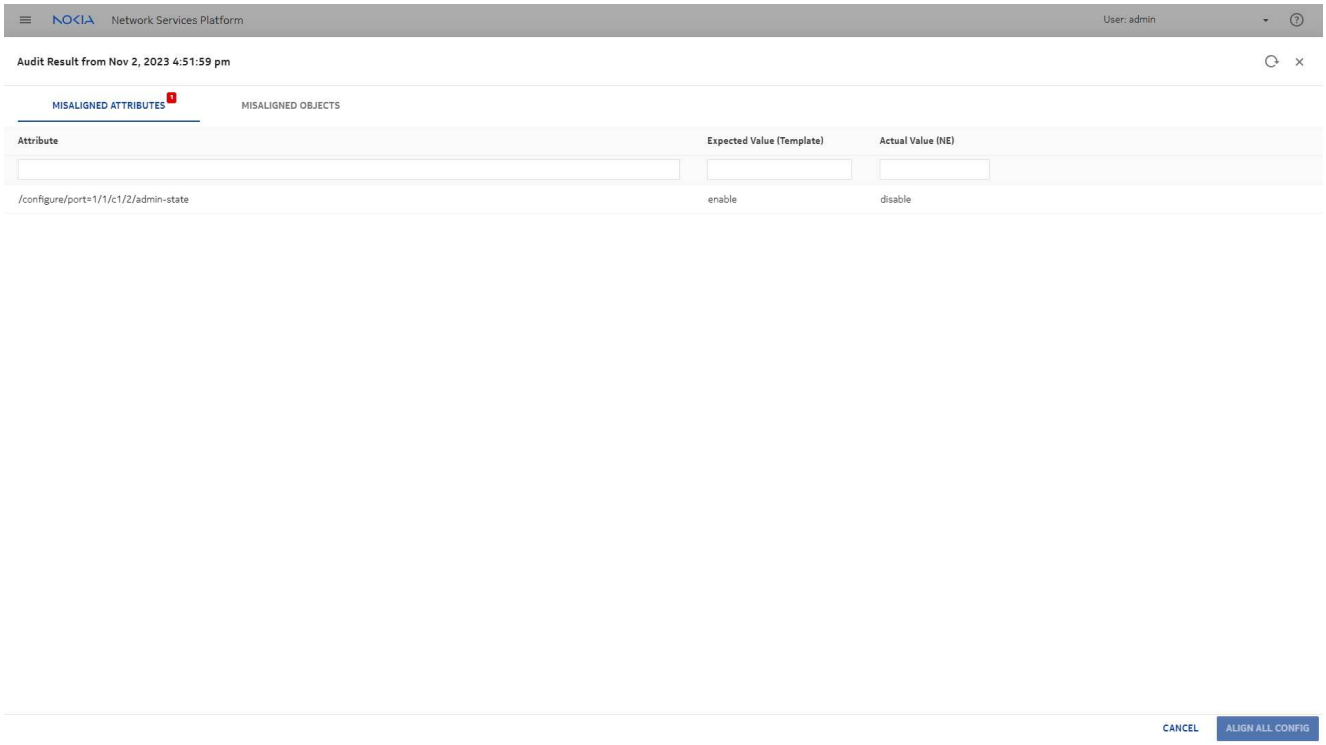


The results show a misaligned attribute. The administrative state for one of the ports is incorrect.



4

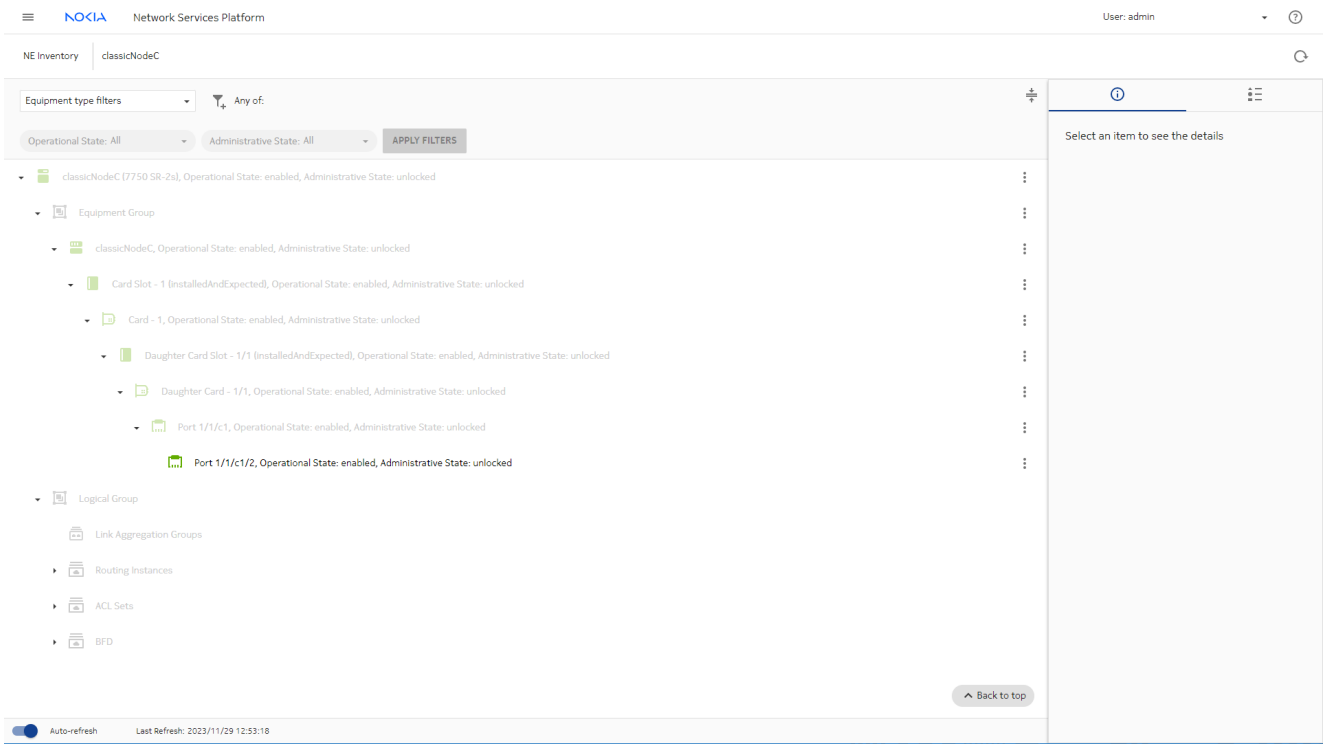
Select **ALIGN ALL CONFIG** to perform an alignment to fix the discrepancy.



Perform another **AUDIT** to confirm the alignment.

5

Returning to **Network Inventory**, we can see that the port now displays green and its administrative state is unlocked.



6

In the Multi-layer view, the links now also display green.

7

Returning to **Data Collection and Analysis Visualizations**, we can also see that traffic utilization has resumed.

5.10 End-to-end port troubleshooting scenario

5.10.1 Purpose

This process shows you how to use NSP in troubleshooting issues on ports.

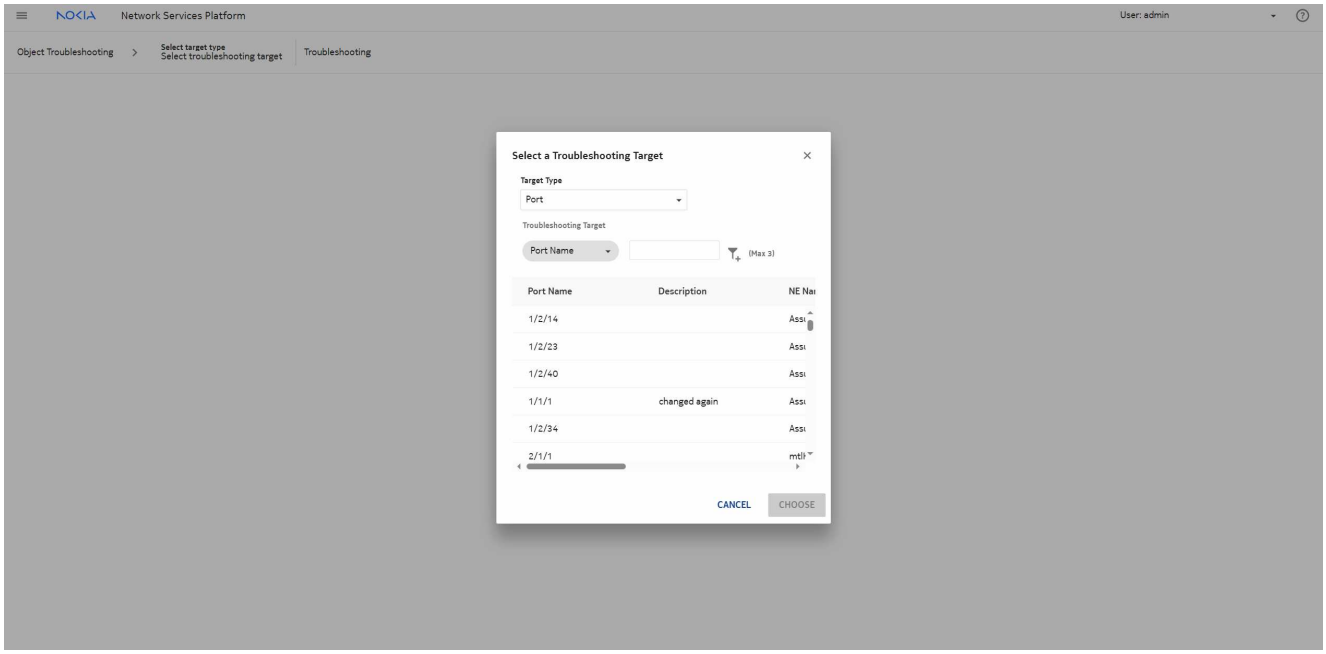
In this scenario, a service has been affected or an alarm has come up. Investigation will show that the problem is due to a port issue.

5.10.2 View the Object Troubleshooting dashboard

Viewing a target in the Object Troubleshooting dashboard can help you see where else you can look to investigate a problem.

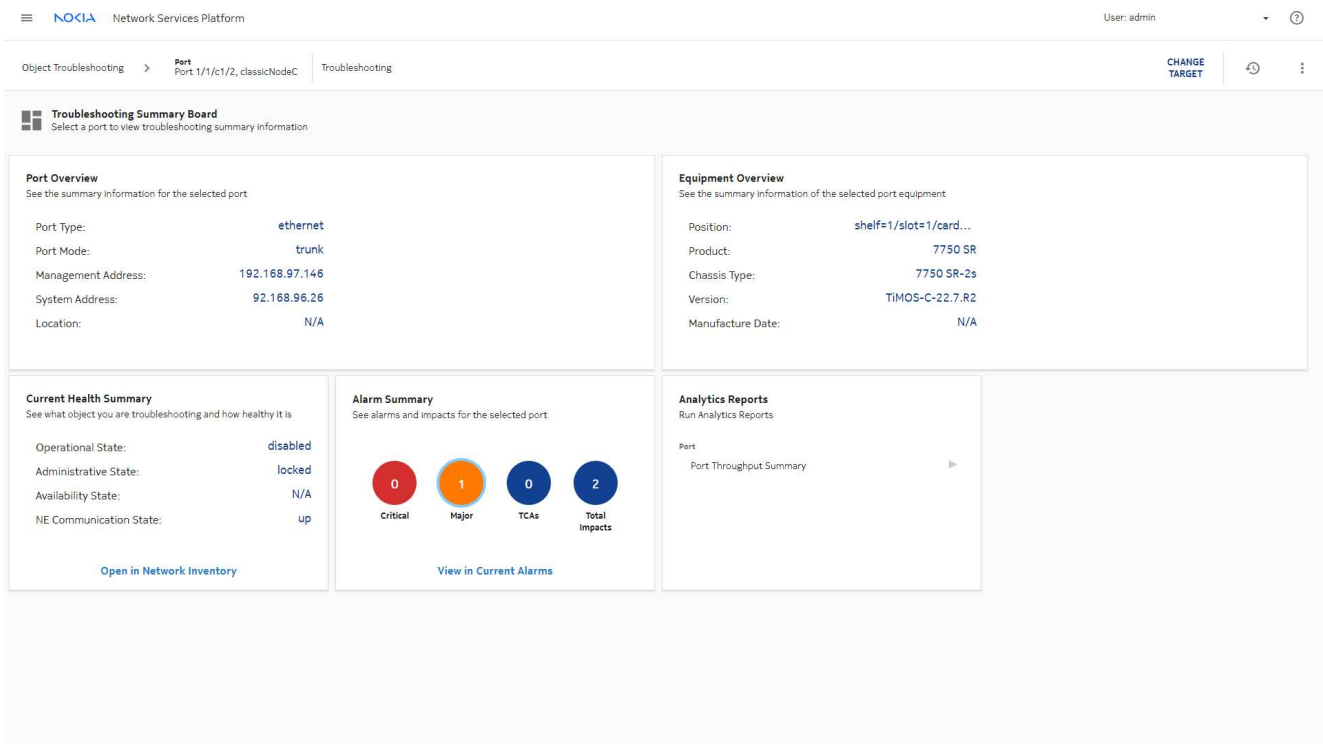
1

Start from the **Object Troubleshooting** dashboard, select **Port** for Target Type, and then select the target port of interest.



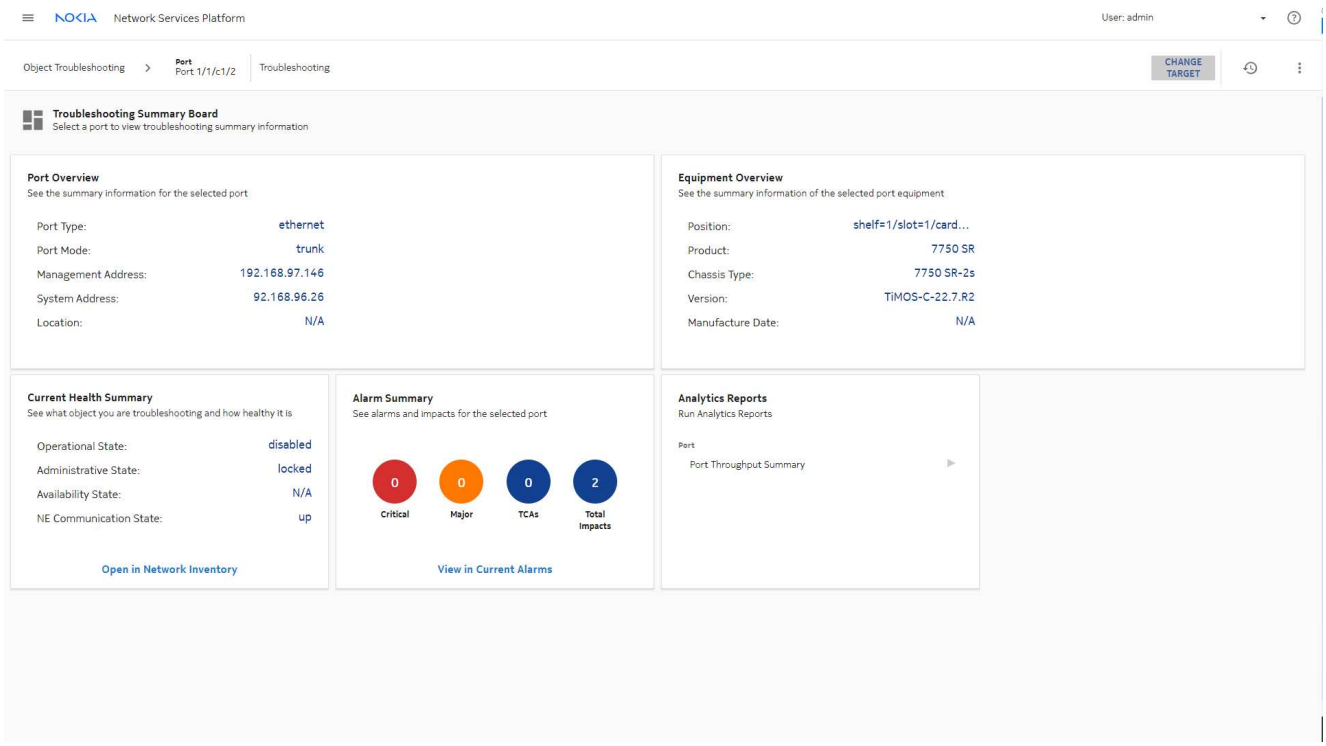
2

The **Object Troubleshooting** dashboard displays summaries of information about the port. The Alarm Summary shows that an alarm is present, and the Current Health Summary shows the operational and administrative states.



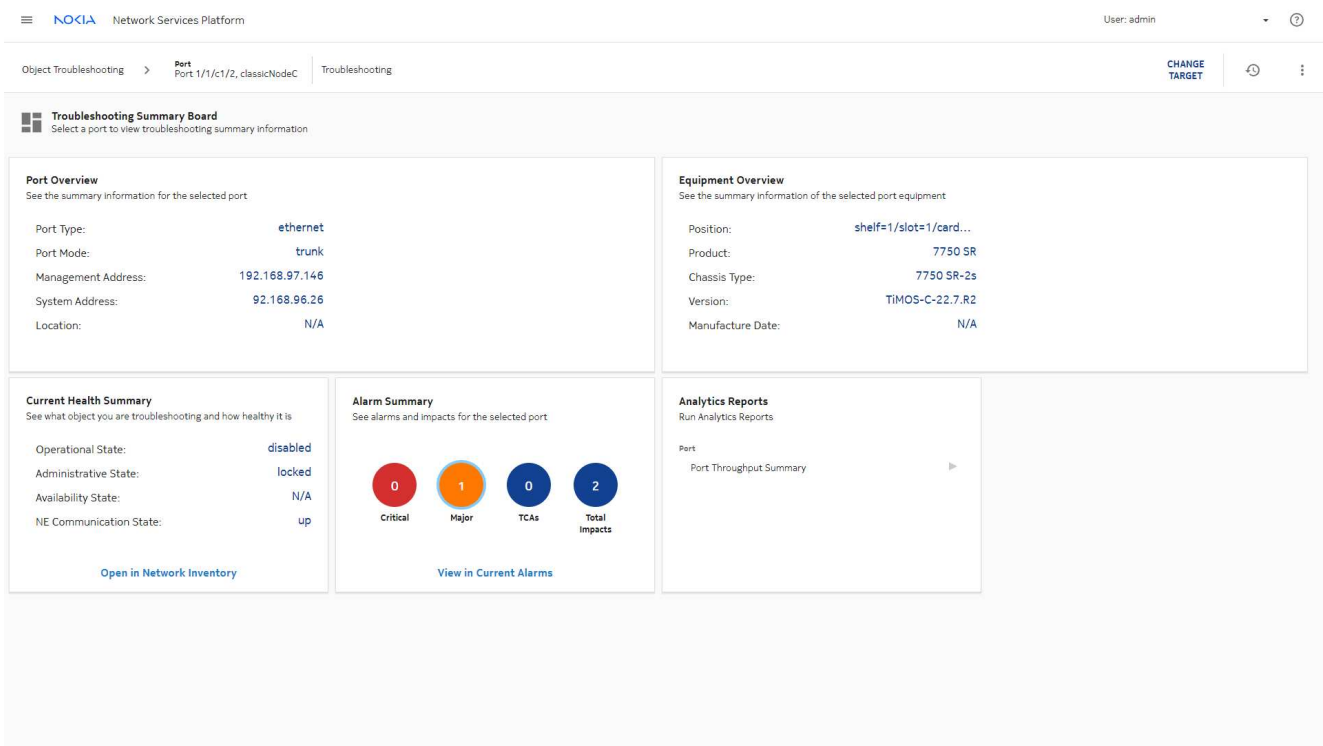
3

Use **CHANGE TARGET** if the wrong port is selected or if you wish to troubleshoot a different port.



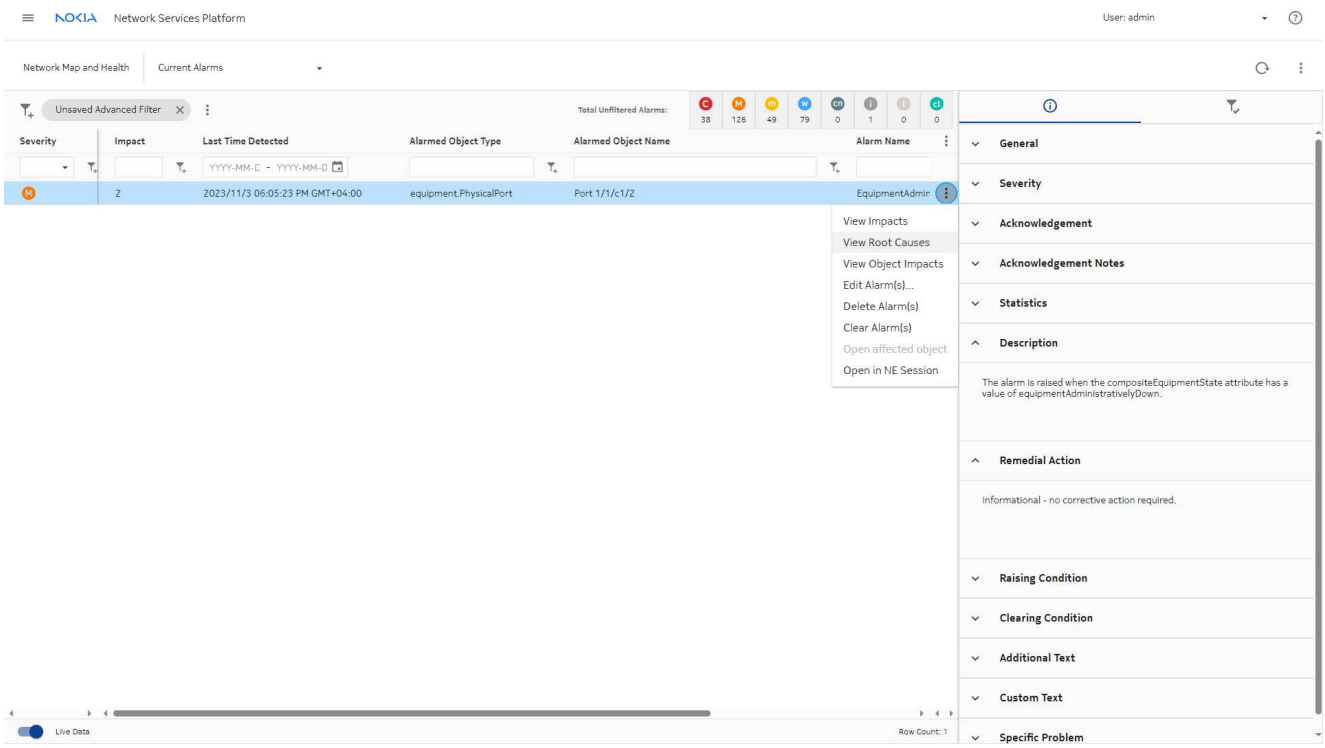
4

Click the **Major** alarm circle in the **Object Troubleshooting** dashboard to launch **Current Alarms**, with that pertinent alarm filtered.

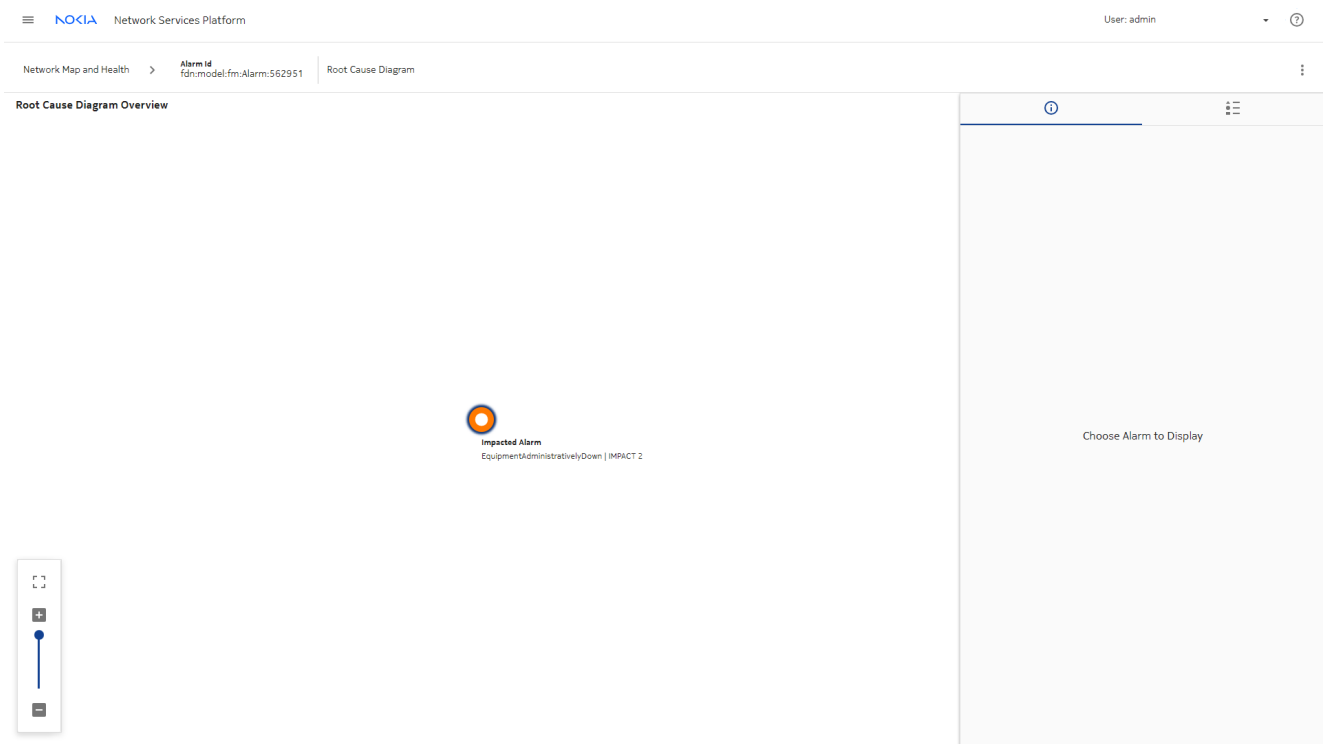


5

In **Current Alarms**, view the **Root Causes** for the alarm.



Current Alarms shows that there is no root cause for this particular alarm as it is a root cause alarm.



6

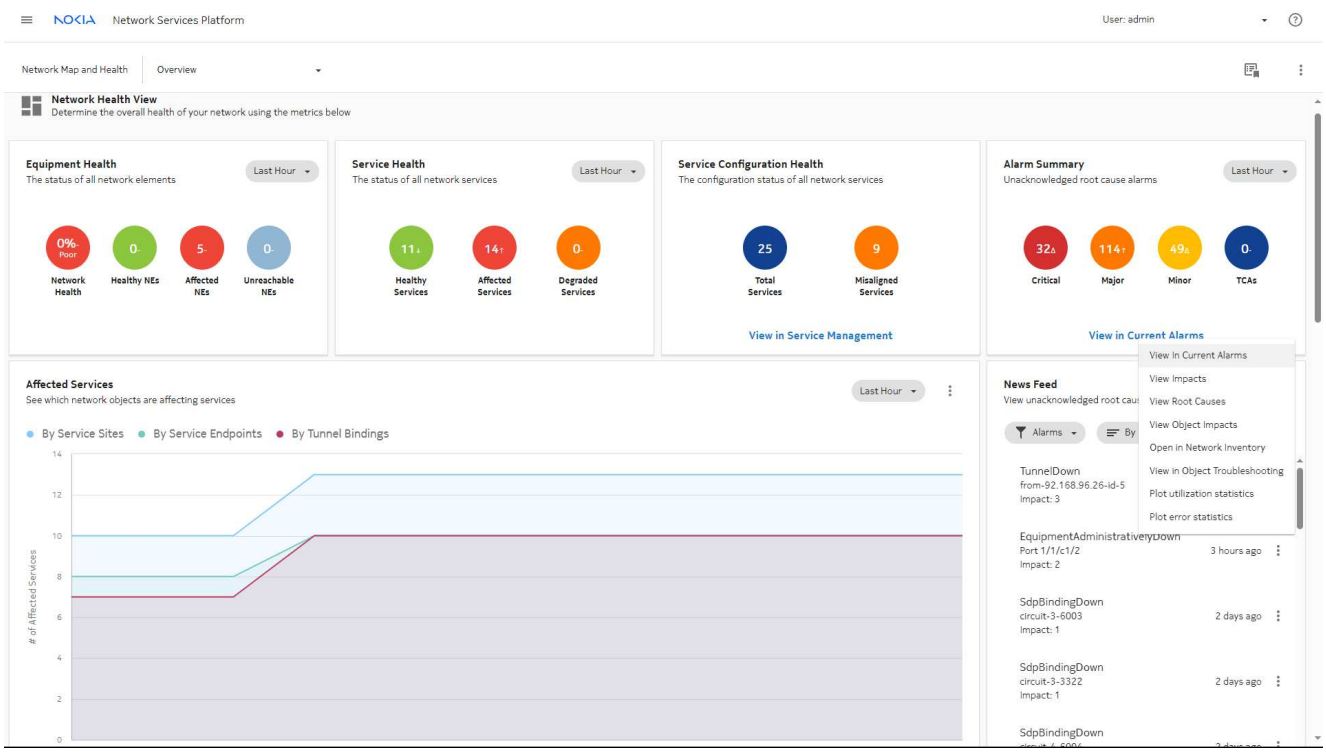
Another option is to switch to the **Unhealthy NEs** or **Top Problems** view in the **Network Map and Health** dashboard to see what other alarms are present on the NE, and to see what other issues the network is experiencing.

5.10.3 View the News Feed

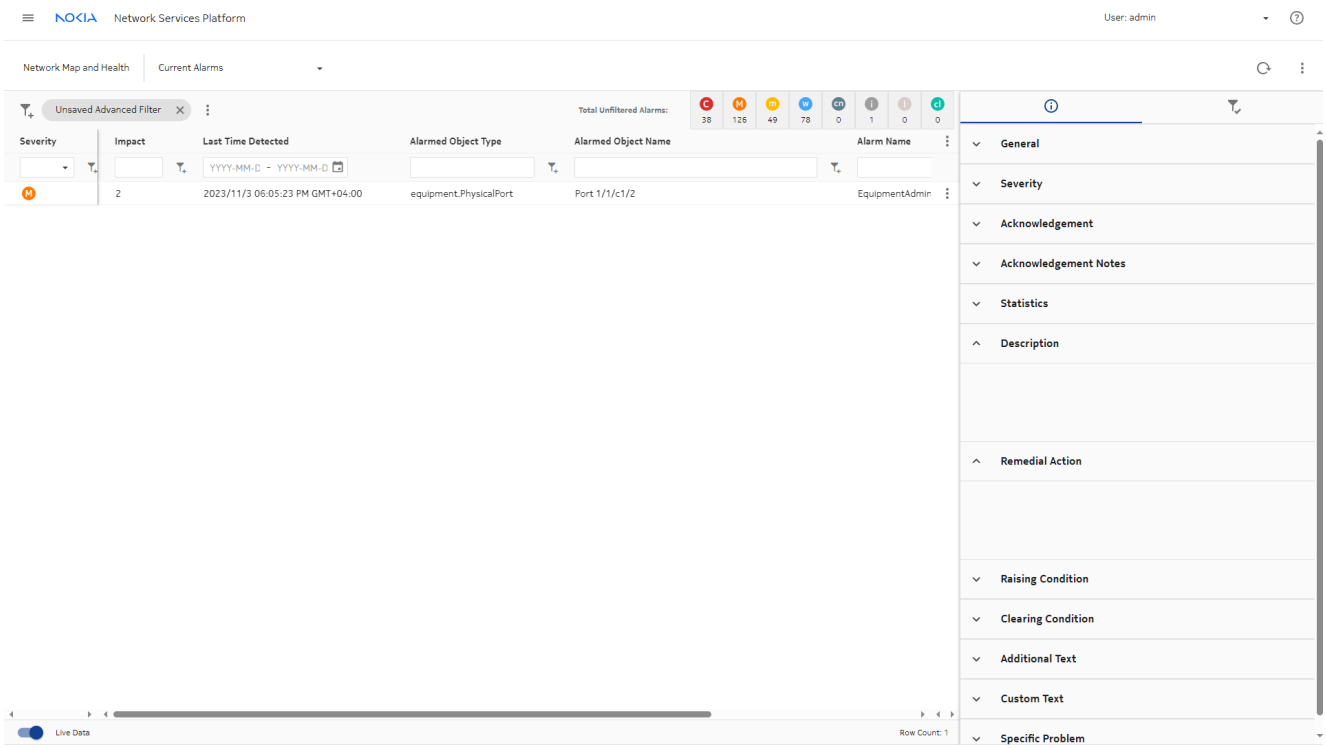
Another starting point could be the News Feed in the Network Map and Health dashboard. The News Feed provides a live feed of unacknowledged root cause alarms as they occur in real time. Alarm severity and number of impacts are displayed, and cross launch is available depending on the alarm.

1

The News Feed shows a Equipment Down alarm on a port. Select the alarm and choose **View in Current Alarms** from the More menu.



Current Alarms opens, showing the current alarm.

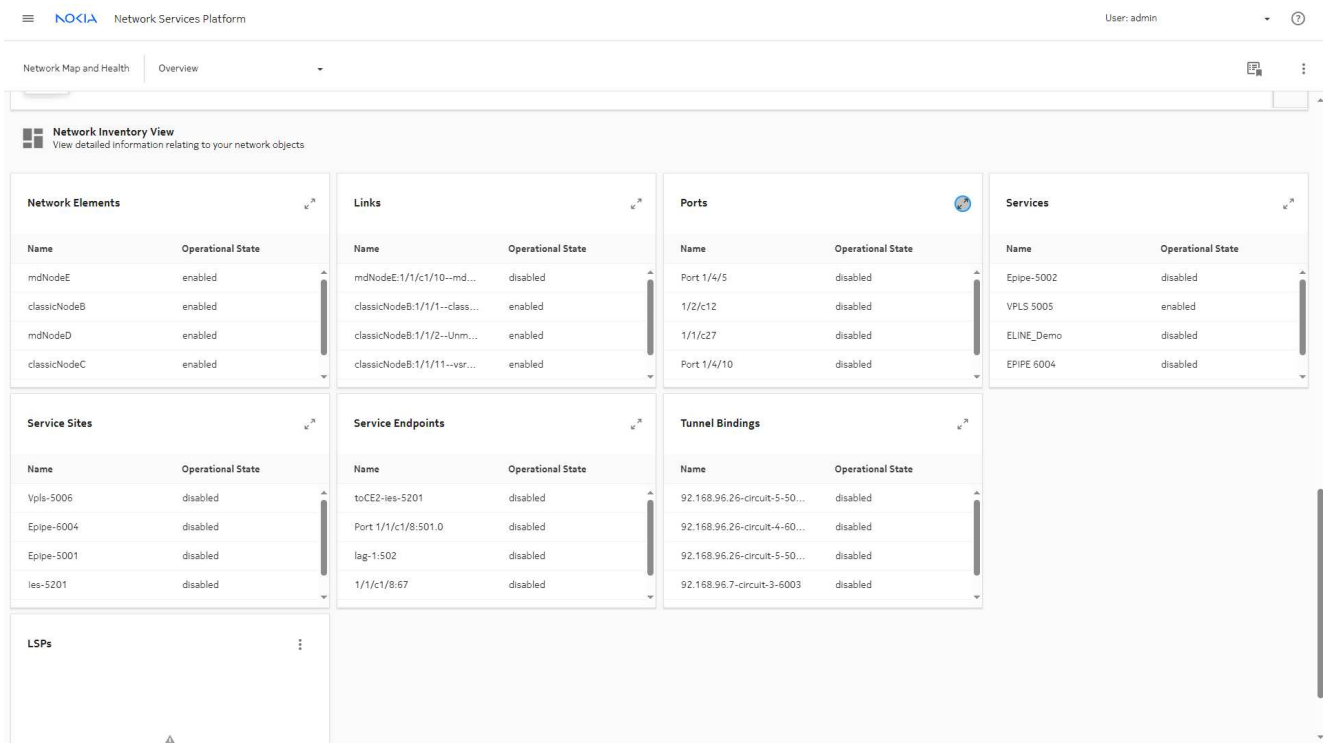


5.10.4 Investigate from the Ports data page

Viewing the port in the Ports list on the Network Map and Health dashboard will show us some configuration and state details.

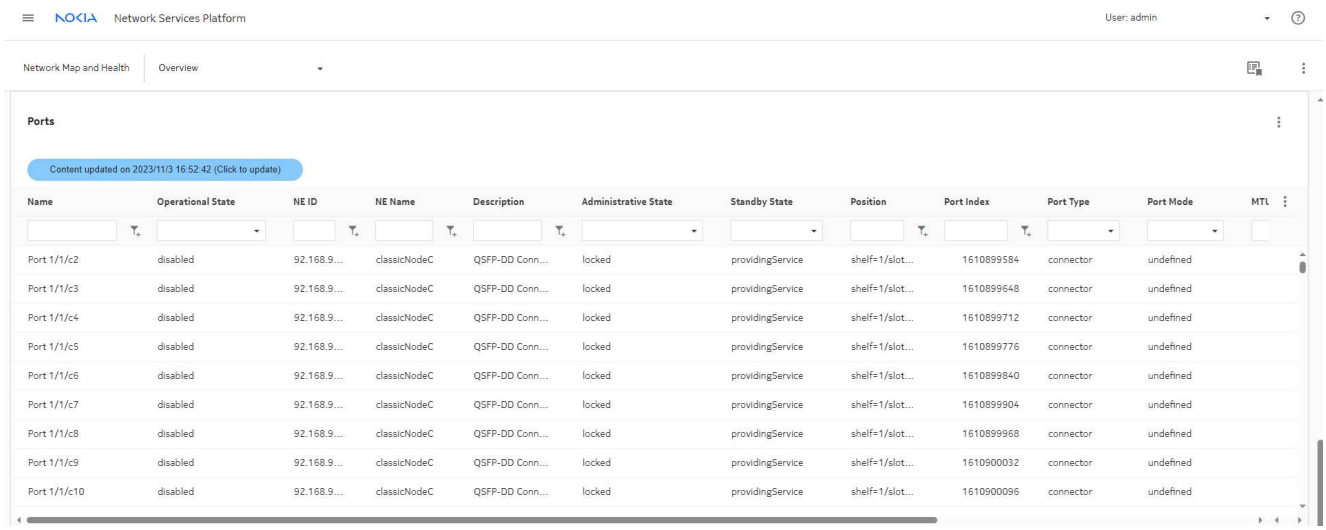
1

From **Overview** in the **Network Map and Health** dashboard, scroll down and expand the **Ports** dashlet and filter on the port being investigated.



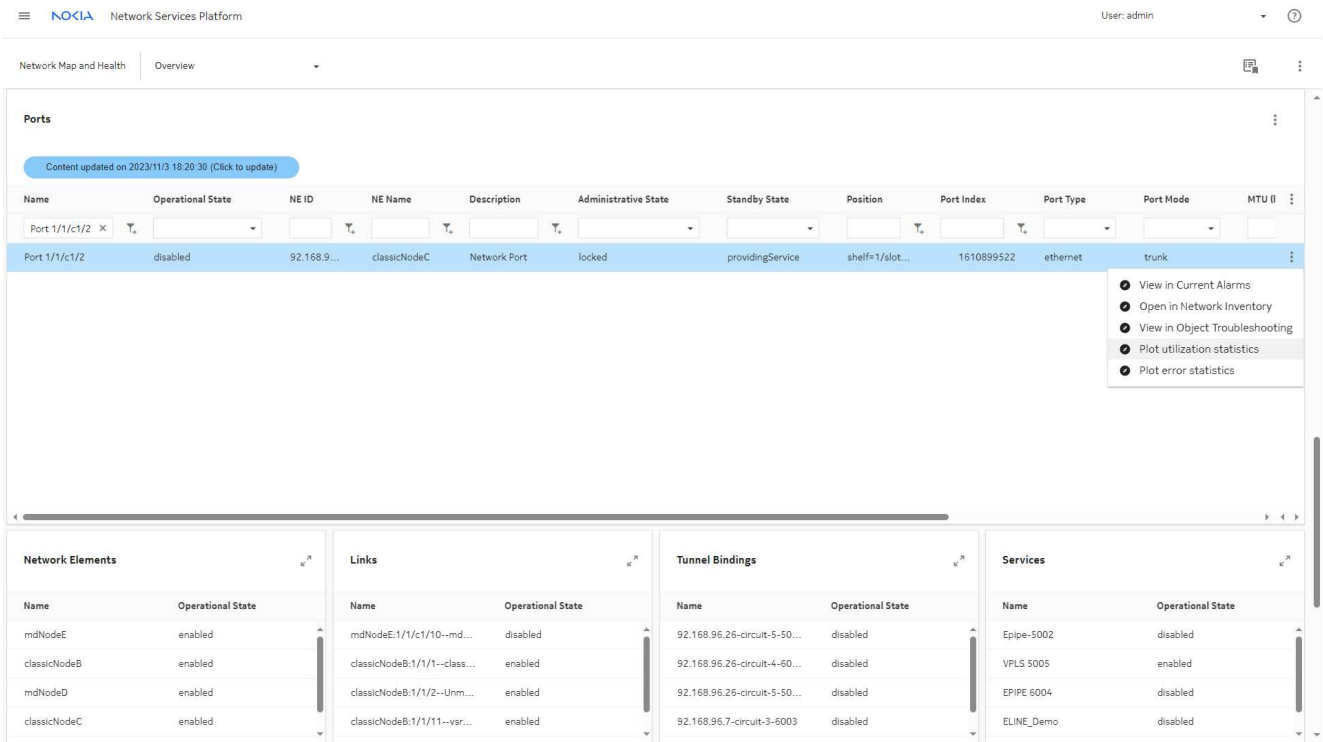
2

From the Ports list, filter on the port name in the Name column, and the NE in the NE Name column. The dashboard shows that the Operational State of the port is disabled and the Administrative State is locked.



3

We can continue to investigate the issue by plotting statistics. Select the port and choose ⋮ (Table row actions), **Plot utilization statistics**.



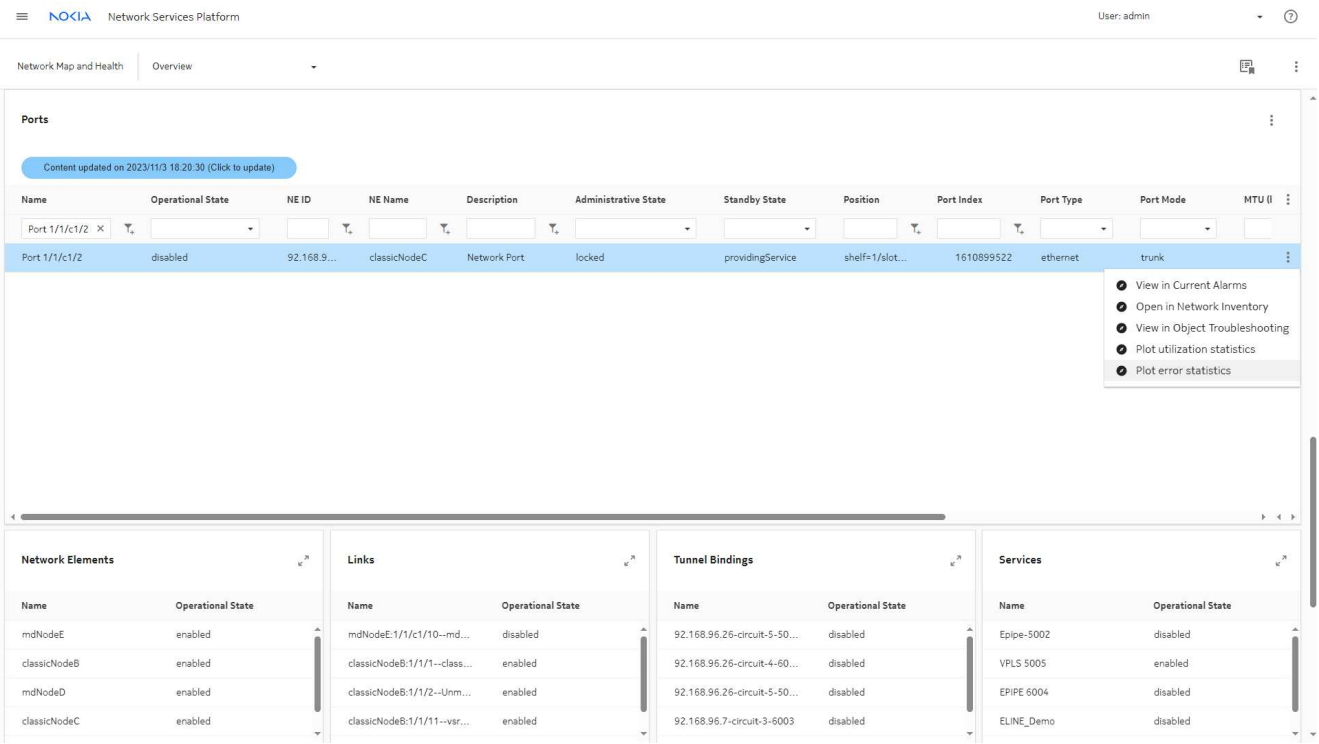
4

Data Collection and Analysis Visualizations opens, showing several charts of utilization statistics.

Here we can see that there is no traffic. This provides additional information about what has happened.

5

We can also plot error statistics for the port. Return to the port in the **Ports** list and choose ⋮ (Table row actions), **Plot error statistics**.

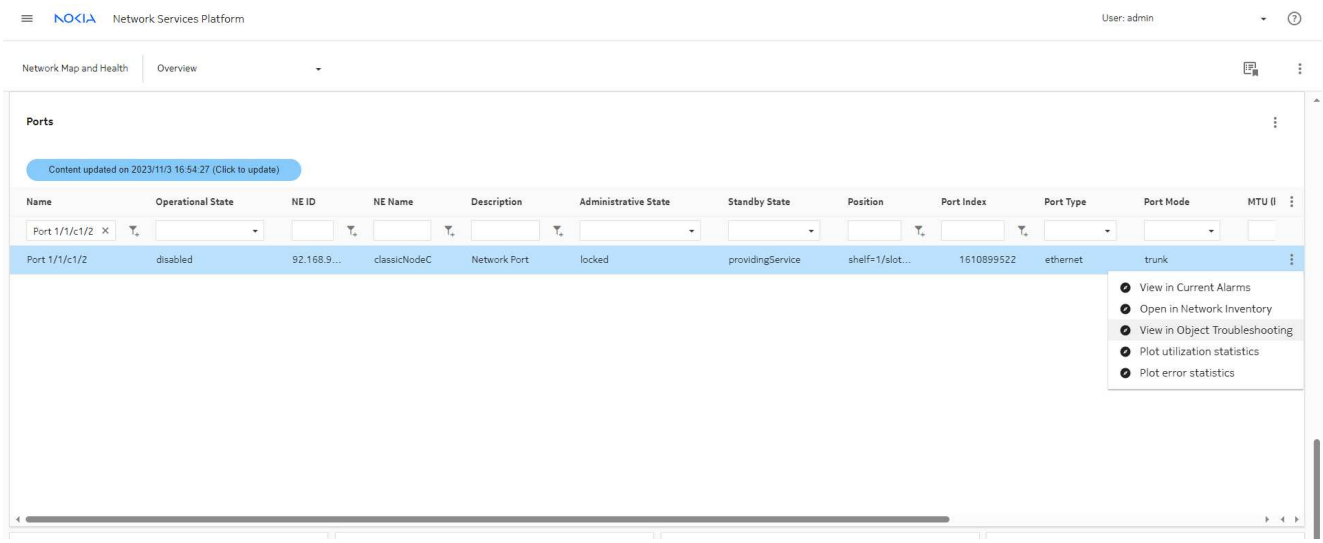


Another **Data Collection and Analysis Visualizations** tab opens, charting multiple error statistics counters, for example, received bad or discarded packets. For this port, there are no errors being recorded.

5.10.5 Investigate using the Object Troubleshooting dashboard

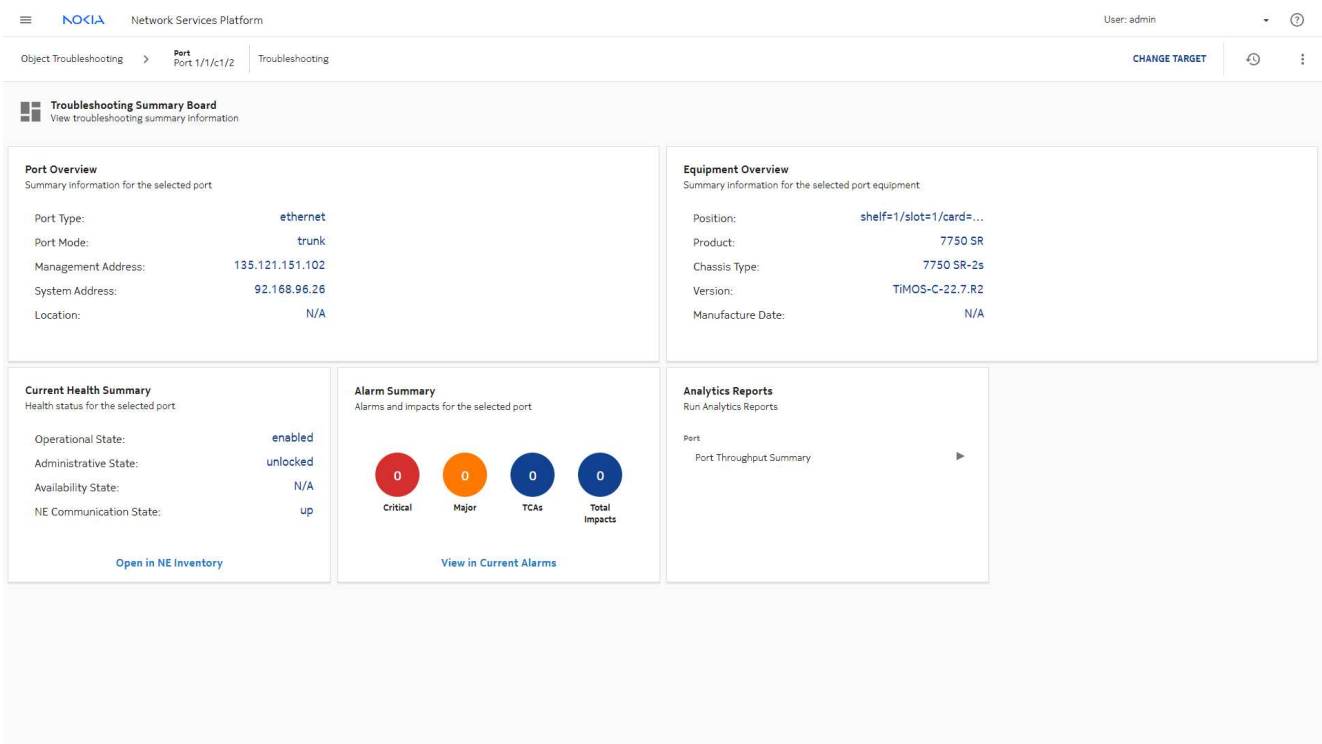
1

You can cross-launch the **Object Troubleshooting** dashboard in context from the **Ports** data page in the **Network Map and Health** dashboard.

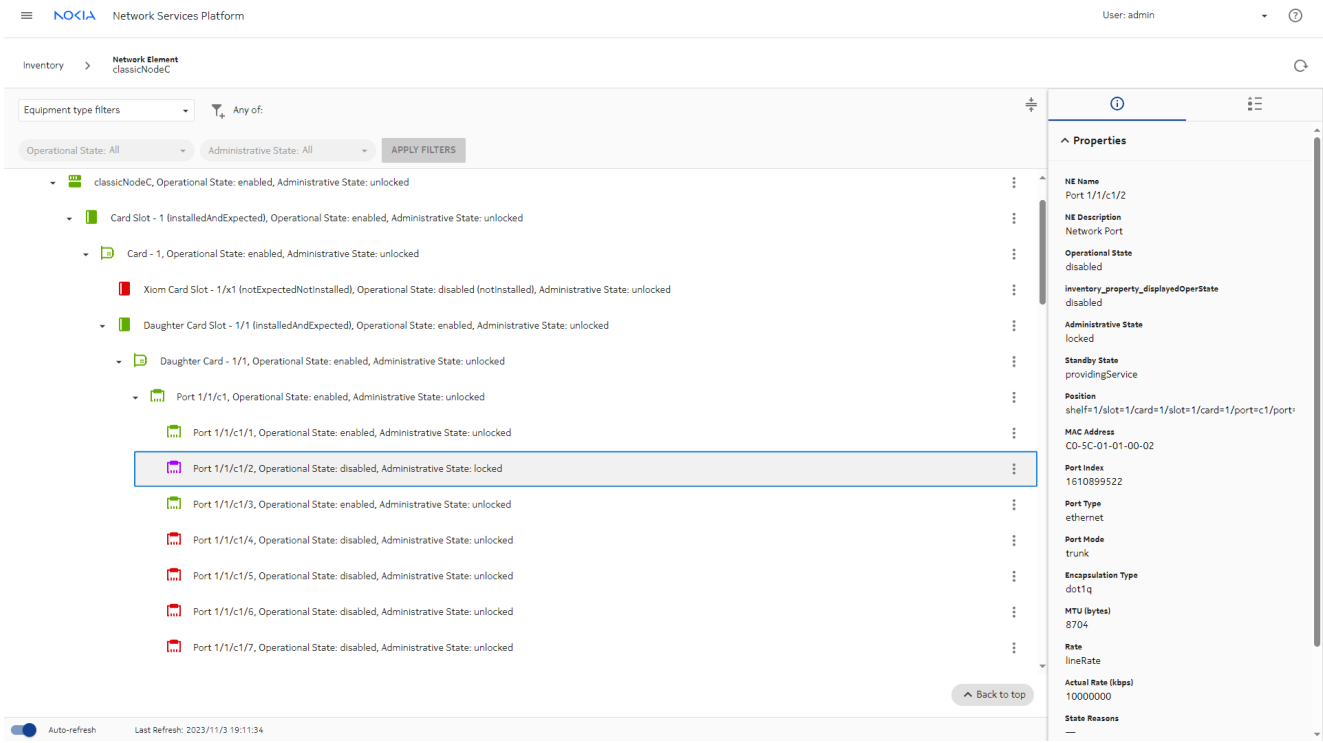


2

From the Current Health Summary dashlet in the Object Troubleshooting dashboard, click **Open in NE Inventory**.



The port is selected, and additional information is shown in the **Info** panel regarding the operational state and administrative state of the port.

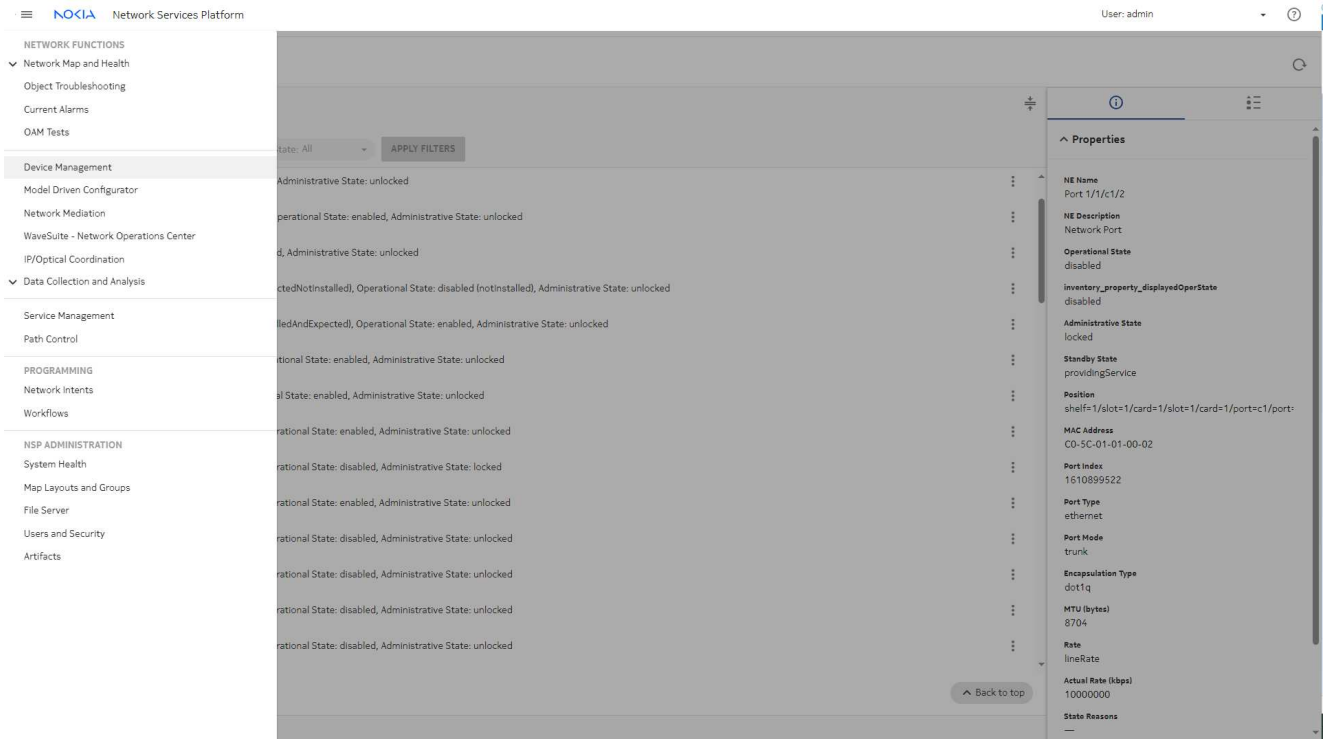


5.10.6 Check infrastructure configuration management details

1

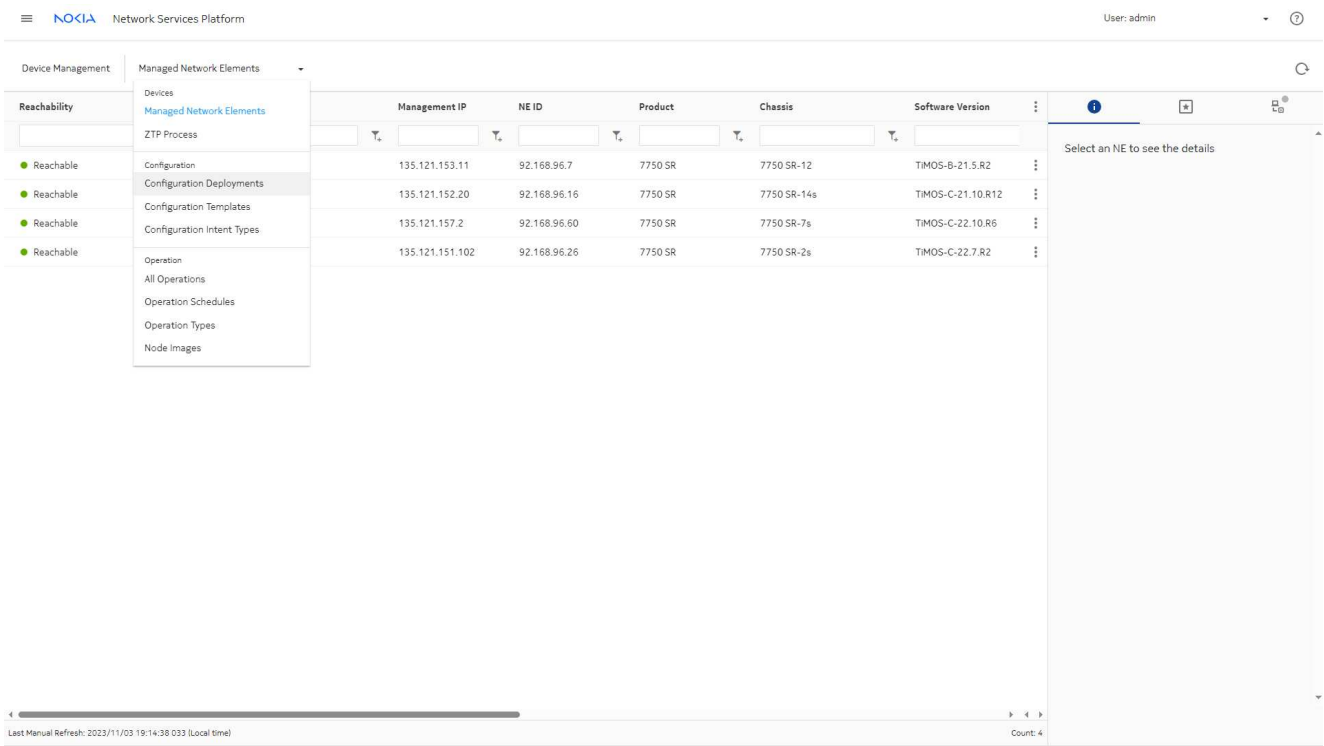
If the NE was configured using Infrastructure Configuration Management, we can check for a misalignment in the **Device Management**, **Configuration Deployments** view.

Navigate to **Device Management**.



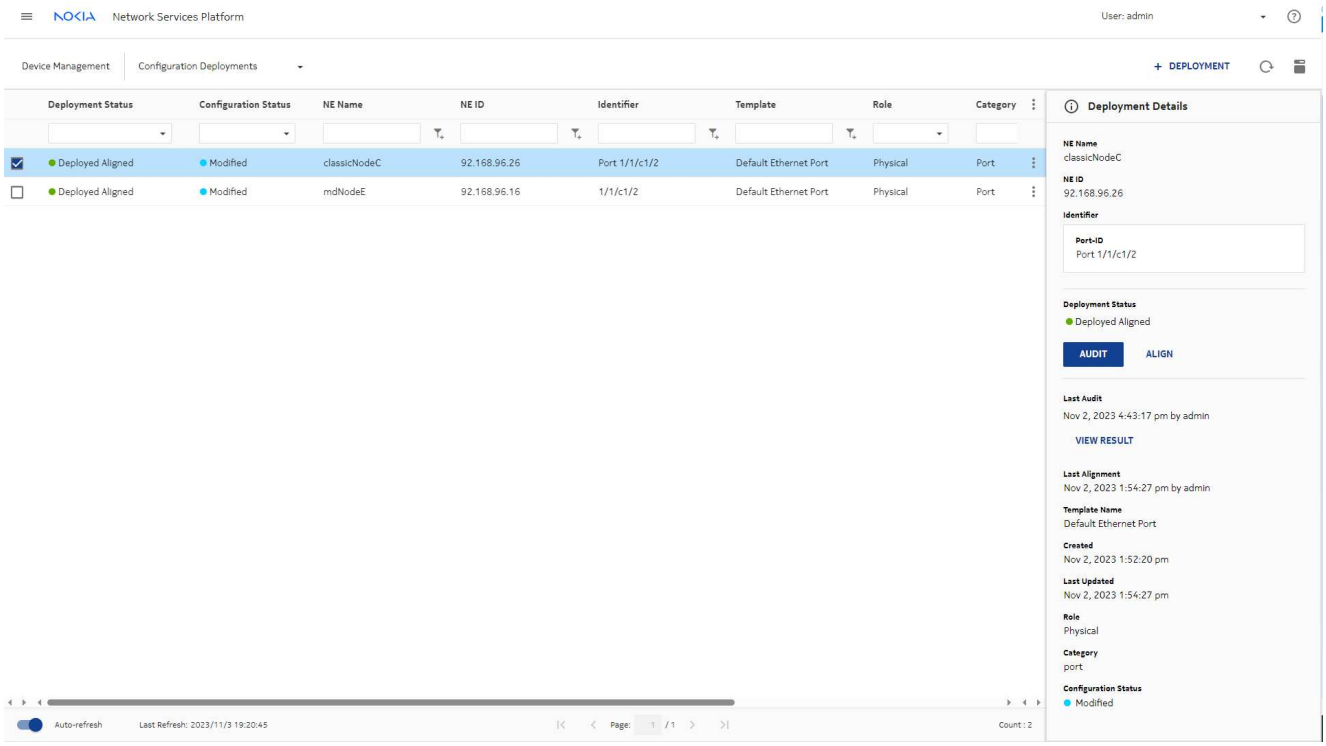
2

In **Device Management**, select **Configuration Deployments** to view the deployed configurations.



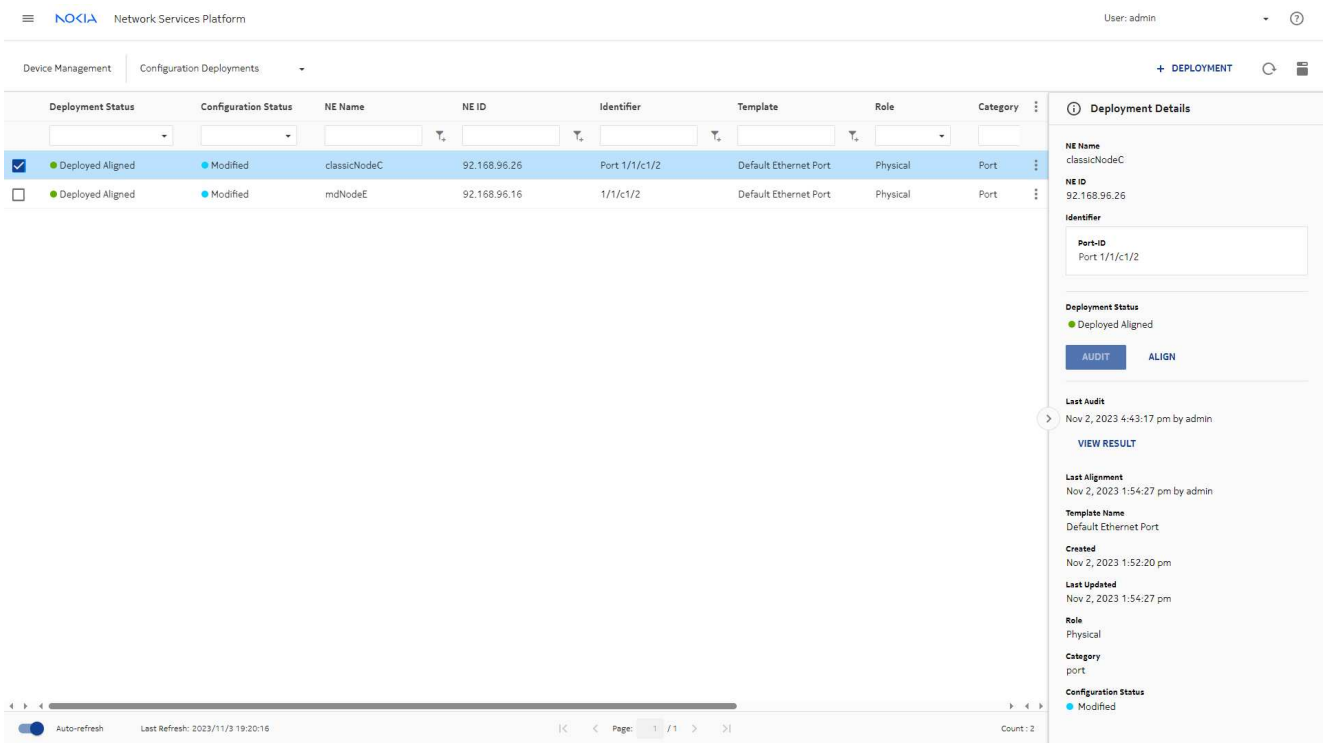
3

Configuration Deployments opens. Click on the port to see information about the port deployment. The Deployment Status column shows the status after the last alignment performed.



4

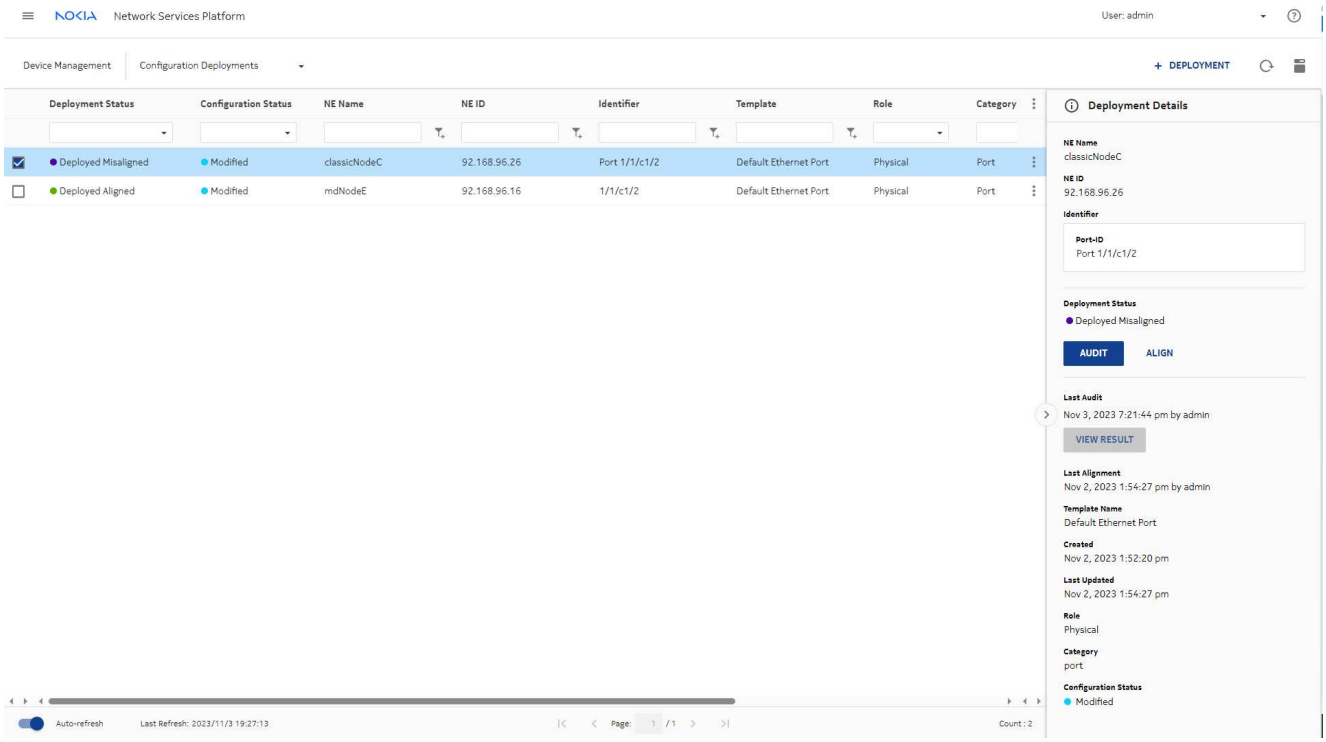
Let’s audit the configuration to compare the configuration of the port in the NSP to the configuration that is present in the network. Click **AUDIT** in the Deployment Details panel.



5

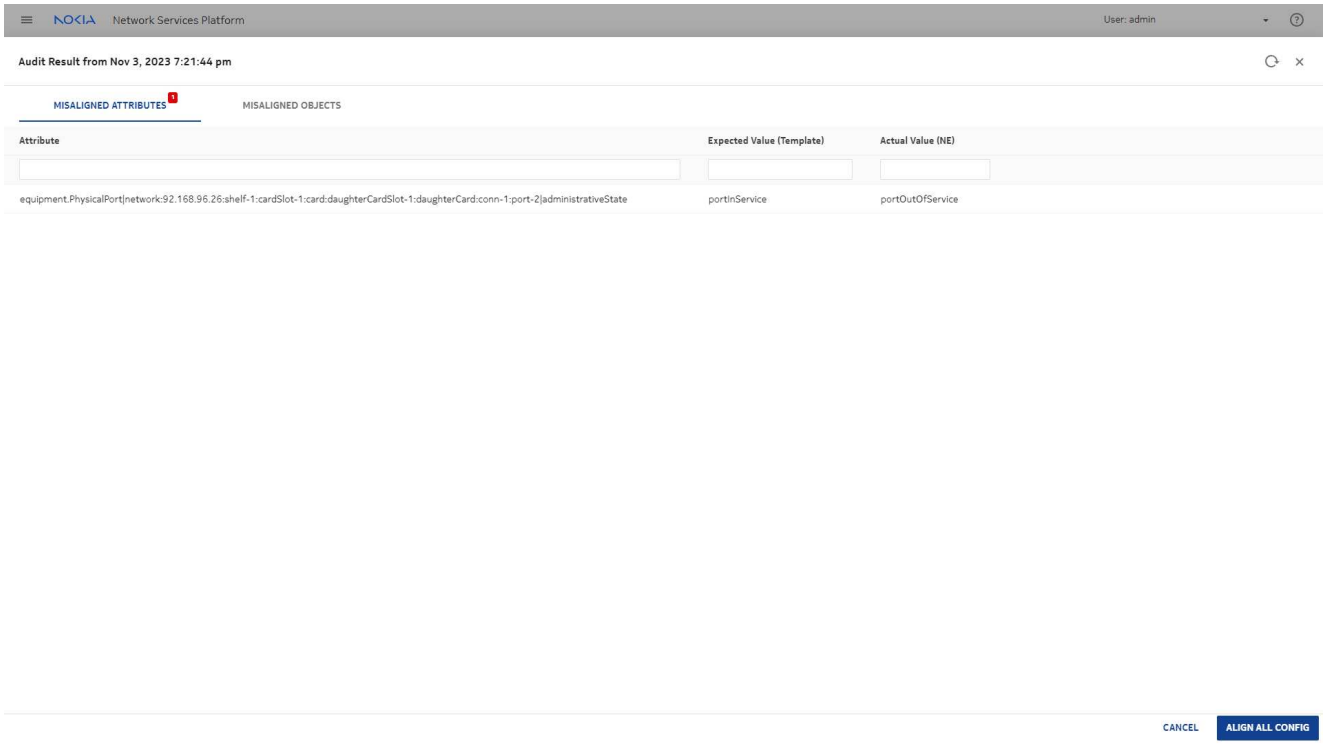
When the audit completes, we see that the deployment is misaligned. The configuration on the port is different from the configuration in **Device Management**.

Click **VIEW RESULT** for more details.



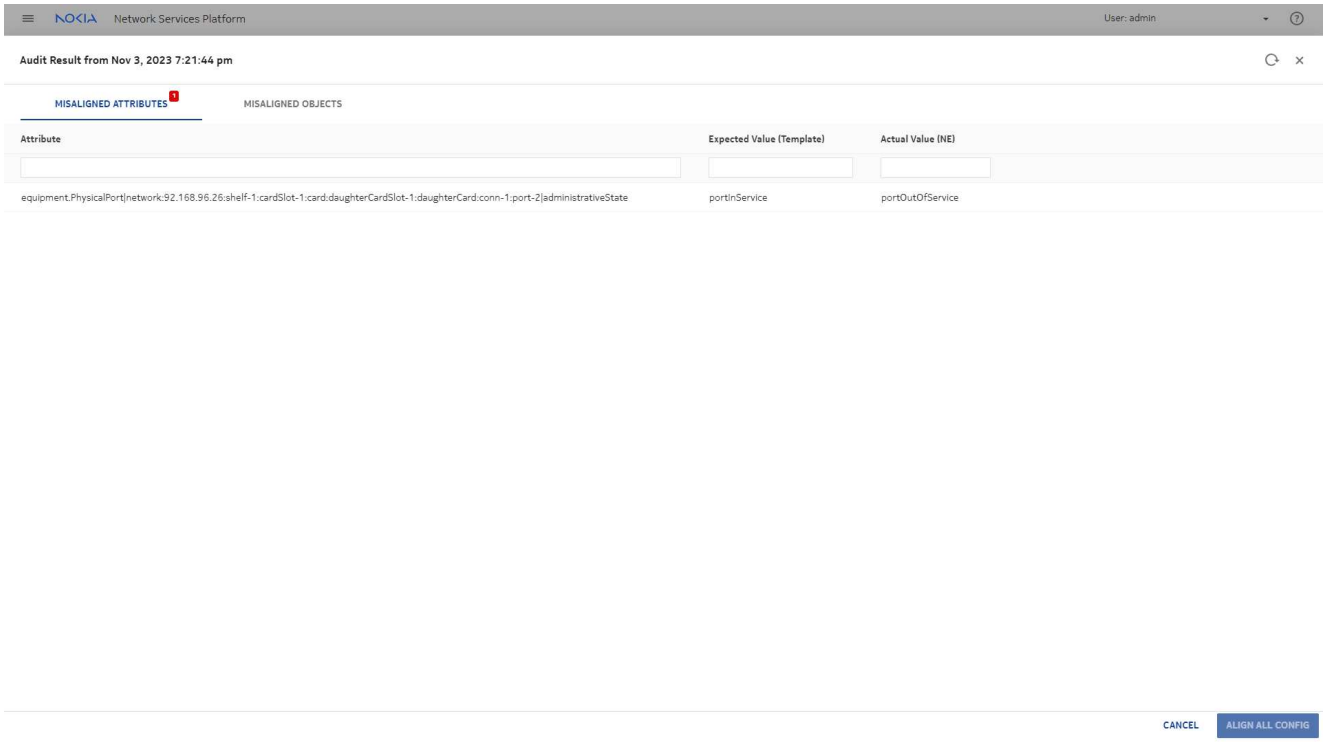
6

The audit results show a state mismatch for the port.



7

The port configuration can be aligned by clicking on **ALIGN ALL CONFIG** in the audit result.

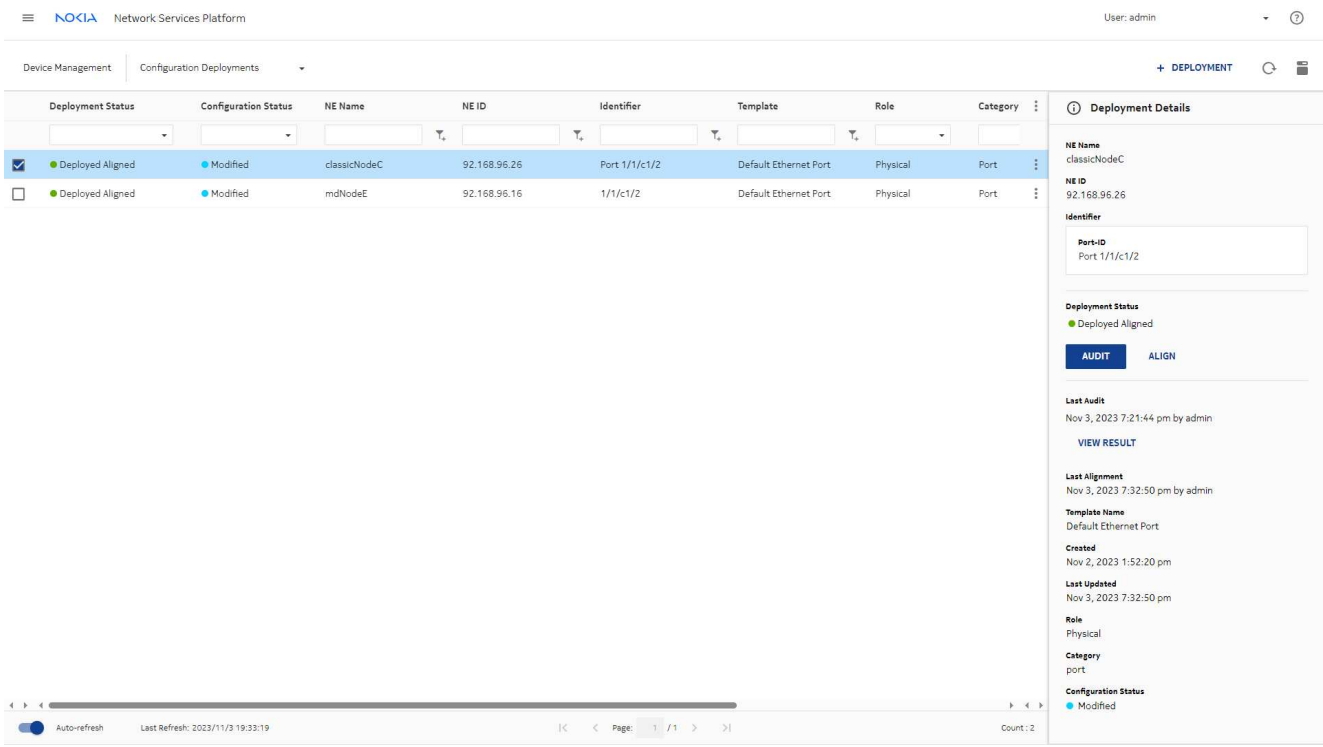


5.10.7 Verify the results

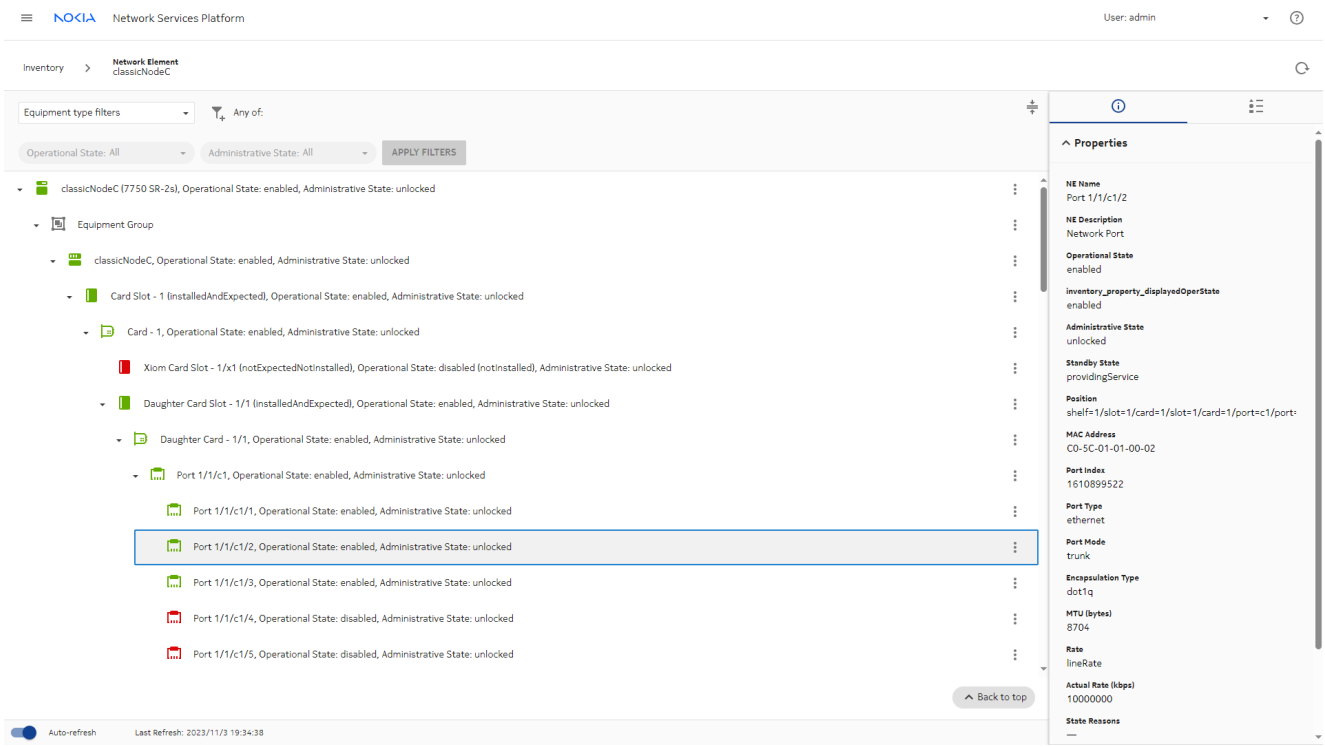
1

After the audit is completed, we can check that the problem has cleared.

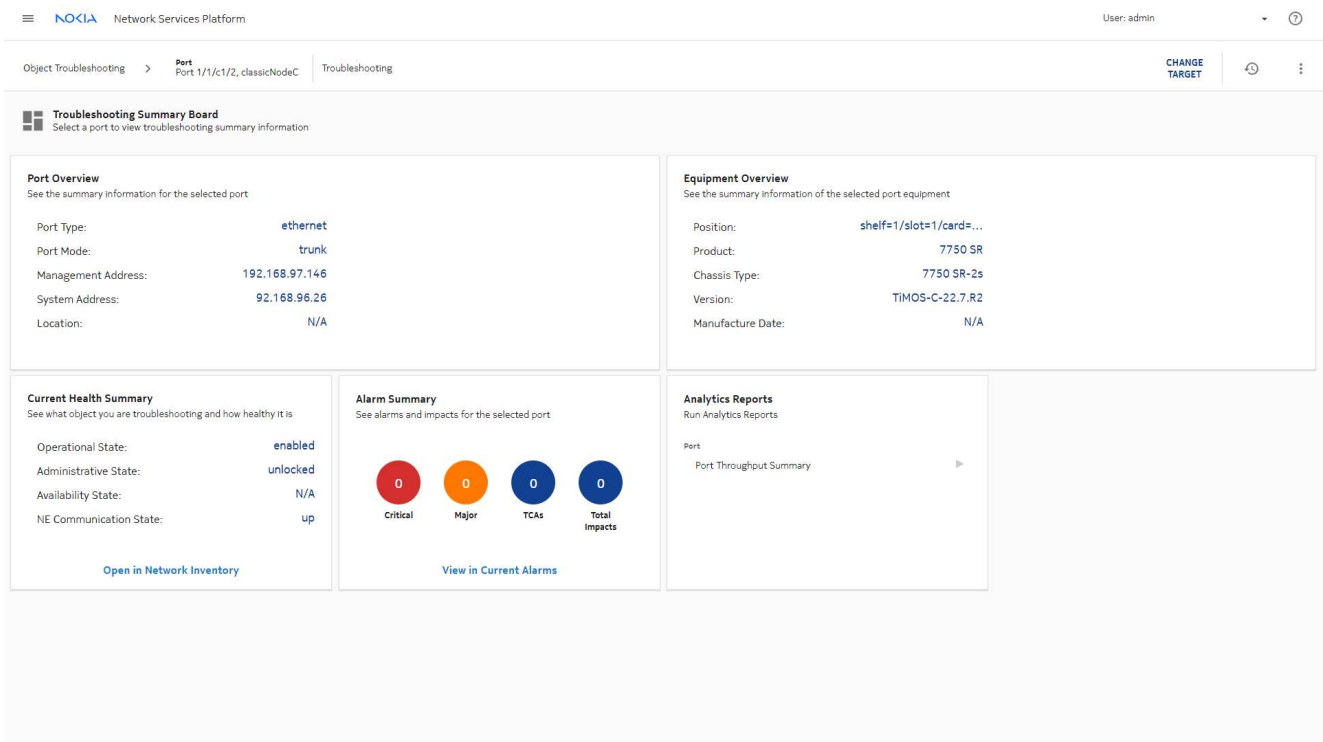
Device Management shows that the configuration is now aligned:



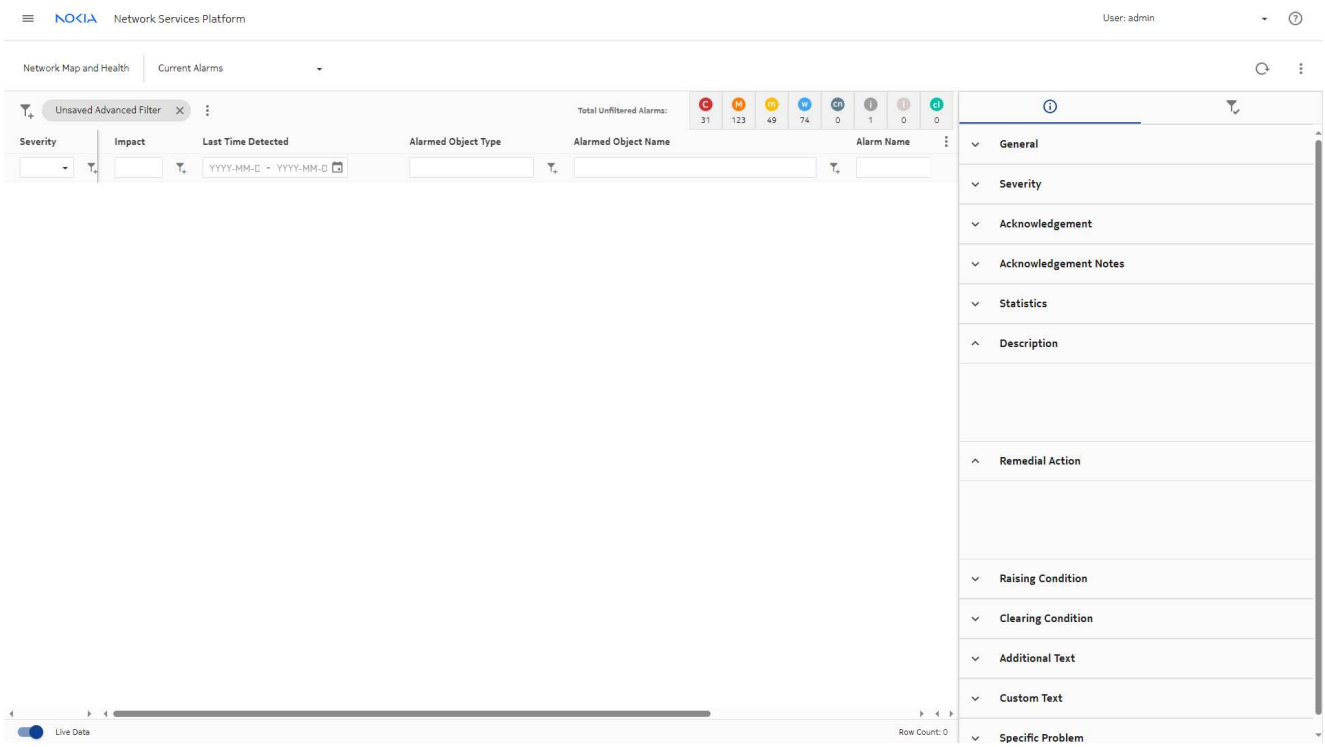
Inventory shows the port in green, with Operational State enabled and Administrative State unlocked:



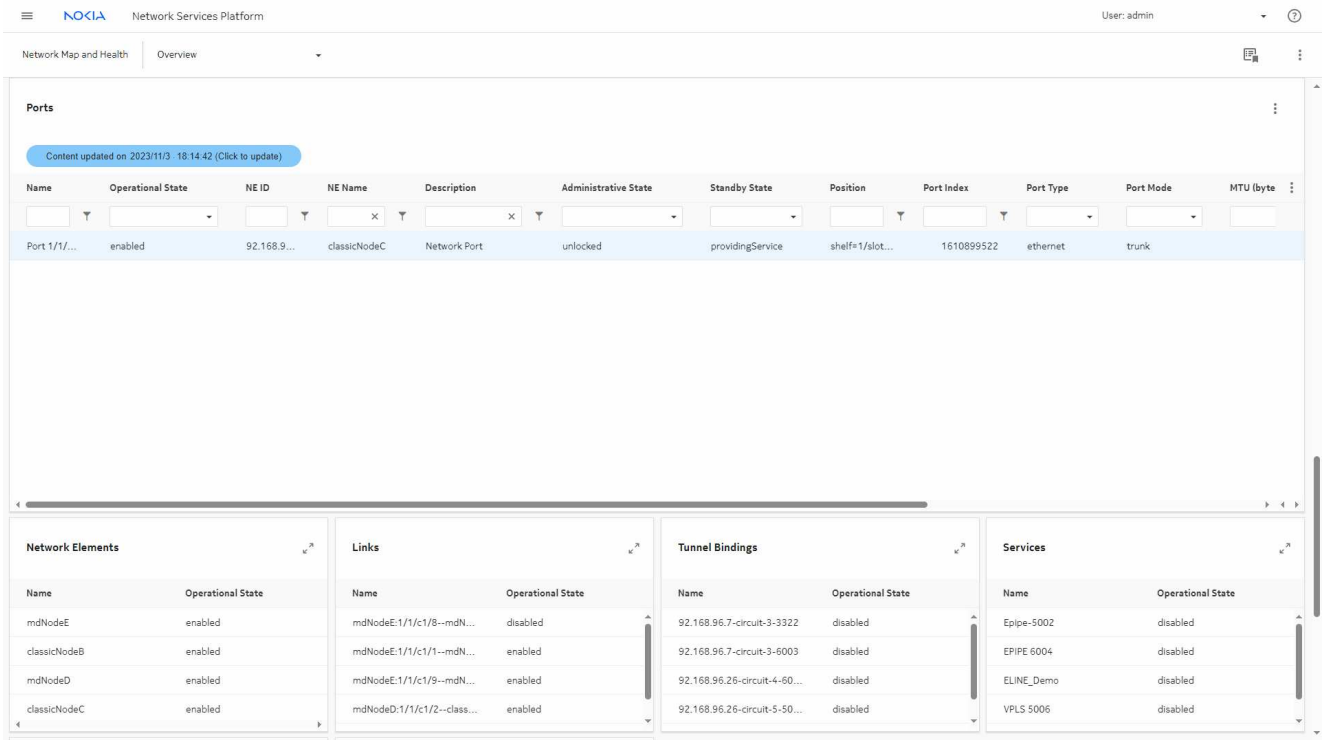
The **Object Troubleshooting** dashboard shows the Major alarm cleared and Operational and Administrative states as expected:



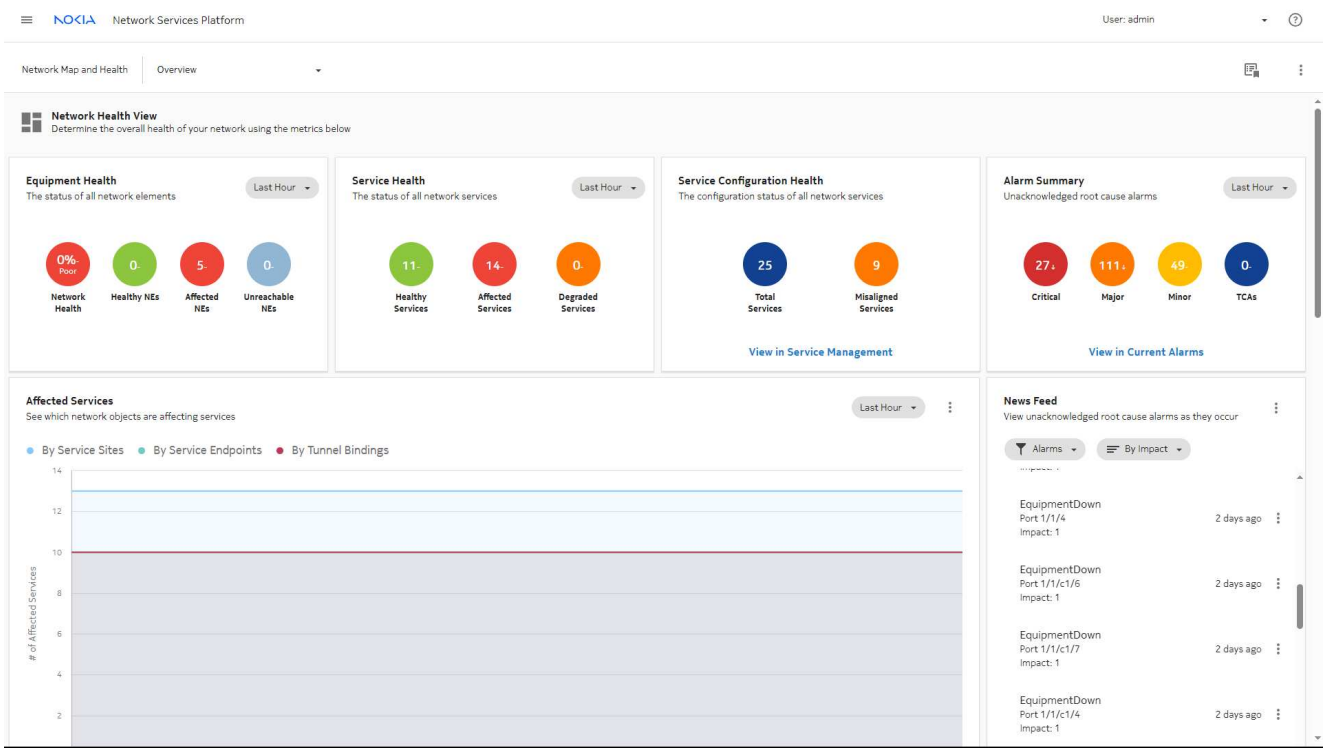
Clicking **View in Current Alarms** from the **Object Troubleshooting** dashboard takes you to the alarm list, where the Equipment Down alarm no longer appears.



The **Ports** list in the **Network Map and Health** dashboard shows the updated port states:



The **News Feed** also shows that the Equipment Down alarm has cleared:



Returning to **Data Collection and Analysis Visualizations**, we can also see that the traffic on the port has resumed.

Troubleshooting using Analytics

5.11 Analytics troubleshooting overview

5.11.1 Troubleshooting

An effective troubleshooting model for solving Analytics report problems includes the following tasks:

- Eliminate the possibility of a hardware or network problem. For example, if you are having trouble with a Port Throughput report, verify that the port is up.
- Check the report description in this guide for the report-specific requirements, such as statistics, aggregation, or policies that must be in place.
- Verify that the NE is generating the required files. For example, if the report requires a statistic, verify that counters for that statistic are being generated.
- Categorize the problem.

  The following are the most common categories of problems affecting reports:
  - Data collection issues
  - Data storage issues
  - Report generation issues
- Plan corrective action and resolve the problem.
- Verify that the problem is resolved.

5.12 Troubleshooting data collection

5.12.1 Statistics collection for Application Assurance reports

A blank report may be due to a statistics collection issue, or a prompt selection that excludes all available data.

The description of the report shows the statistics type required for the report, and whether NSP flow collection is required. Table 5-1, “Troubleshooting statistics collection for Application Assurance reports ” (p. 320) describes options for checking statistics collection.

Table 5-1 Troubleshooting statistics collection for Application Assurance reports

Statistics type	Items to verify	See
AA accounting	• Are required policies in place? • Are statistics being collected? • What is the accounting retrieval status of the NE? • Is additional information available from server performance statistics?	"Workflow for accounting statistics collection" in the *NSP NFM-P Statistics Management Guide* "Workflow for server performance statistics collection" in the *NSP NFM-P Statistics Management Guide* "To view the accounting statistics collection status of an NE" in the *NSP NFM-P Classic Management User Guide*
AA Cflowd	• Has AA Cflowd sampling been configured? • Are required policies in place?	"To enable and configure global Cflowd sampling on an NE" in the *NSP NFM-P Classic Management User Guide* "To configure Cflowd collectors on an ISA-AA group or partition" in the *NSP NFM-P Classic Management User Guide* "To configure an AA Cflowd group policy" in the *NSP NFM-P Classic Management User Guide* "Workflow to configure flow statistics collection" in the *NSP NFM-P Statistics Management Guide* If the report requires special study statistics collection, see "Workflow to configure AA Cflowd special study statistics collection" in the *NSP NFM-P Statistics Management Guide*
Subscriber	• Are required policies in place? • Are statistics being collected?	"To configure AA subscriber statistics collection on an ISA-AA group or partition" in the *NSP NFM-P Classic Management User Guide*

5.12.2 Statistics and data collection for Network and Service reports and NSP reports

A blank report may be due to a statistics collection issue, or a prompt selection that excludes all available data.

The description of the report shows the statistics or data type required for the report, and any other prerequisites that may apply. Table 5-2, "Troubleshooting statistics and data collection for Network and Service reports and NSP reports " (p. 321) describes options for checking collection.

Table 5-2 Troubleshooting statistics and data collection for Network and Service reports and NSP reports

Statistics type	Items to verify	See
Accounting (also known as XML statistics)	• Are required policies in place? • Are statistics being collected? • Are required aggregators configured?	"Workflow for accounting statistics collection" in the *NSP NFM-P Statistics Management Guide* "How do I configure analytics aggregation?" in the *NSP Analytics Report Catalog*
Performance (SNMP) data	• Are required policies in place? • Is SNMP connectivity established between the NE and the NFM-P? • Are required statistics being collected? • Are required aggregation rules enabled? • Alarms: if the system cannot collect and process all performance statistics in the specified polling period, the PollerDeadlineMissed alarm will be raised.	"How do I configure analytics aggregation?" in the *NSP Analytics Report Catalog*
IPFIX (also called System Cflowd or Netflow v10)	• Has IPFIX sampling been configured? • Are required policies in place?	"Workflow to configure flow statistics collection" in the *NSP NFM-P Statistics Management Guide*
OAM data	• Is OAM testing configured in the NFM-P? • Are required policies in place? • Are OAM aggregation rules enabled?	"How do I configure analytics aggregation?" in the *NSP Analytics Report Catalog*
Event data for Uptime reports	• Is an event log policy in place with an appropriate retention time for assurance events? • Are maintenance windows configured appropriately?	"To configure an event log policy" in the *NSP NFM-P Classic Management User Guide* "To create and manage custom auxiliary database table attributes" in the *NSP System Administrator Guide*

5.12.3 NSP auxiliary database

If you suspect an auxiliary database problem, you can run the following script on an auxiliary database station to collect log files for technical support:

/opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh getDebugFiles

5.12.4 NFM-P main database

For Inventory reports, the NFM-P main database must be operational and able to receive files from NEs.

To confirm that files are being received and stored, monitor the following folder on the standalone or primary main server to ensure that new statistics files are being generated:

/opt/nsp/nfmp/server/xml_output

5.13 Troubleshooting data storage

5.13.1 OAM test result storage

For OAM test reporting, the OAM test results must be stored in the auxiliary database, which requires that the oam-test-results parameter is enabled in the samauxdb section of each NFM-P main server configuration. See the *NSP Installation and Upgrade Guide* for information about using the samconfig utility to modify the NFM-P configuration.

5.13.2 Statistics retention policy

Verify that the statistics retention policy is appropriate; data is unavailable for reporting if statistics are removed prematurely.

5.13.3 Auxiliary database log locations

Logs for each NE can be found in the following directory on an NSP auxiliary database station:

/opt/nsp/nfmp/auxdb/catalog/samdb/*member_ID*_catalog/vertica.log

where member_ID is the ID of the auxiliary database station, for example, v_samdb_node0002

The following log file contains basic auxiliary database status information:

/opt/nsp/nfmp/auxdb/install/proxy/log/EmsAuxDbProxy.log

5.13.4 Assurance event logging

If an NSP auxiliary database is present, assurance events are recorded in the following auxiliary database table:

samdb.assurance_assuranceevent

If no auxiliary database is present, assurance events are recorded in the following main database table:

PsoAssuranceEvent obj_199a4deb

5.14 Troubleshooting Analytics reporting

5.14.1 Configuring NSP Analytics logging

By default, NSP Analytics logs only errors, but additional logging options are available. For example, the SQL log shows the data table names so that you can verify that the table for your report is requesting and receiving timed frame data to generate reports.

See “How do I manage NSP Analytics logging?” in the *NSP System Administrator Guide* for information about enabling various NSP Analytics log levels.

5.14.2 Additional troubleshooting options

The following may assist with troubleshooting Analytics reporting:

- See “Using Analytics” in the *NSP Analytics Report Catalog* to ensure that the reporting criteria are correctly specified. For example, all data for a report must be collected using the same collection interval.
- Verify the connectivity between the NSP cluster, NSP auxiliary database, and other system elements.
- If a report takes a long time to create, or generates errors, try reducing the number of objects in the data set.

Troubleshooting using NSP workflows

5.15 Evaluating failed or slow workflow executions

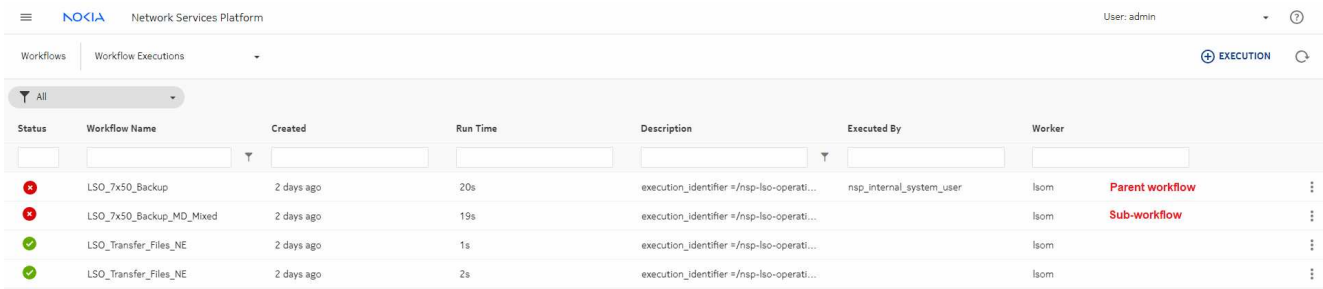
5.15.1 Purpose

This article shows you how to evaluate failed or slow workflow executions and troubleshoot the source of workflow errors.

5.15.2 Parent workflows and sub-workflows

Workflows may call other workflows as part of their execution. Both the parent workflow and the sub-workflow appear in the Workflow Execution list.

If a workflow execution's **Executed by** parameter is blank, the workflow was executed by another workflow, as shown in the following figure.



Note the Created field for these example executions. The `LSO_7x50_Backup_MD_Mixed` sub-workflow execution was created at the same time as the `LSO_7x50_Backup` workflow execution. The `LSO_7x50_Backup` may be the parent workflow that created this failed execution.

Start your troubleshooting with a parent workflow to ensure that you see all the relevant information.

5.15.3 Check the information page of a successful execution

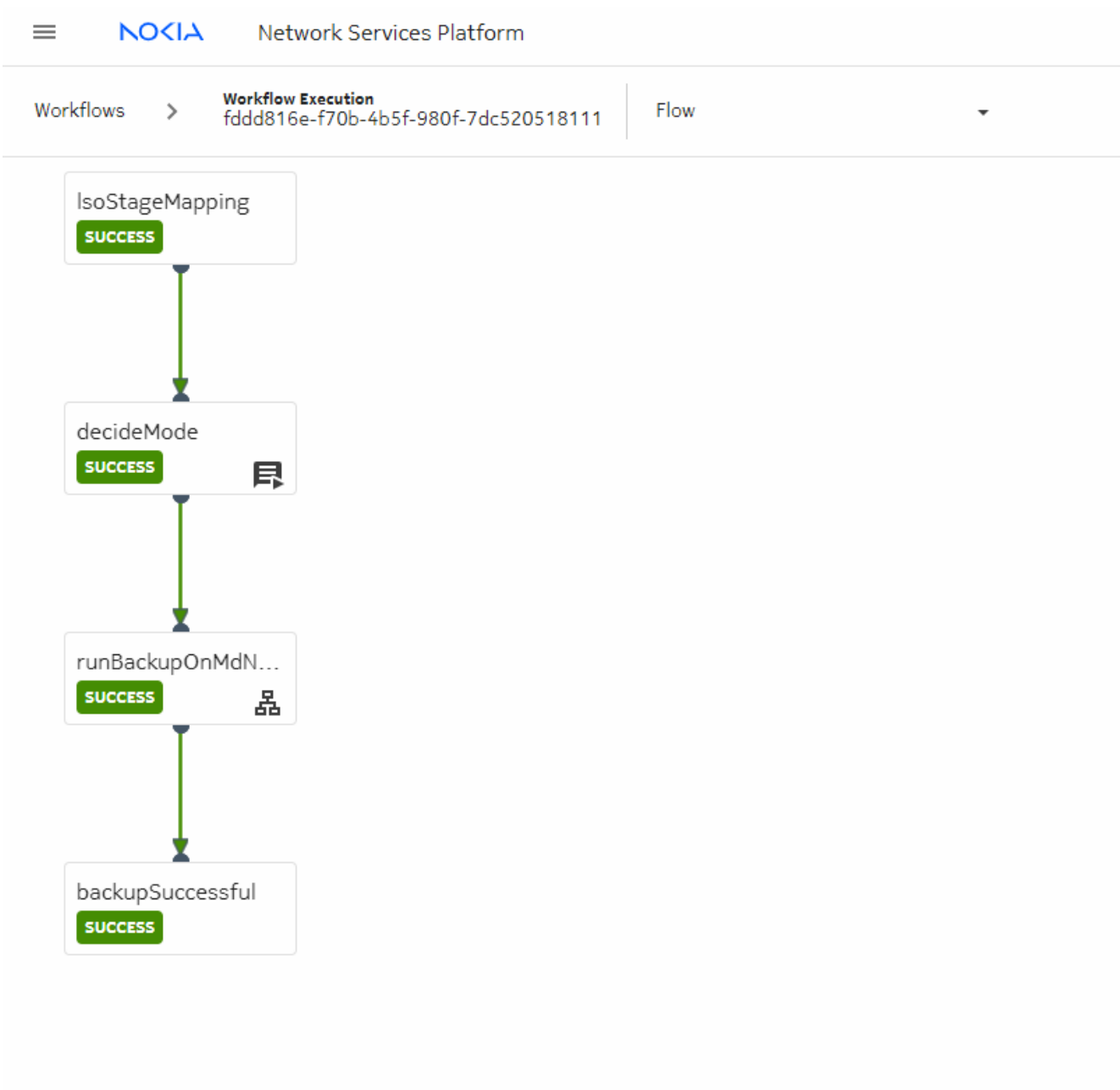
If you have an example of a successful execution of the workflow, it can help you narrow your search for the source of issues with slow or failing workflows.

1

Double click on a successful workflow execution. The Execution info page displays.

2

Choose **Flow** from the **Info** drop-down. The Flow diagram shows the sequence of tasks performed when the workflow was executed.



Hover over the icons on each task for more information on the task type. In this example, `decideMode` is a message action, and `runBackupOnMdNode` is a sub-workflow.

3

Expand the panel at the right of the screen for further details:

- Click Run Time to see the run time for each task.

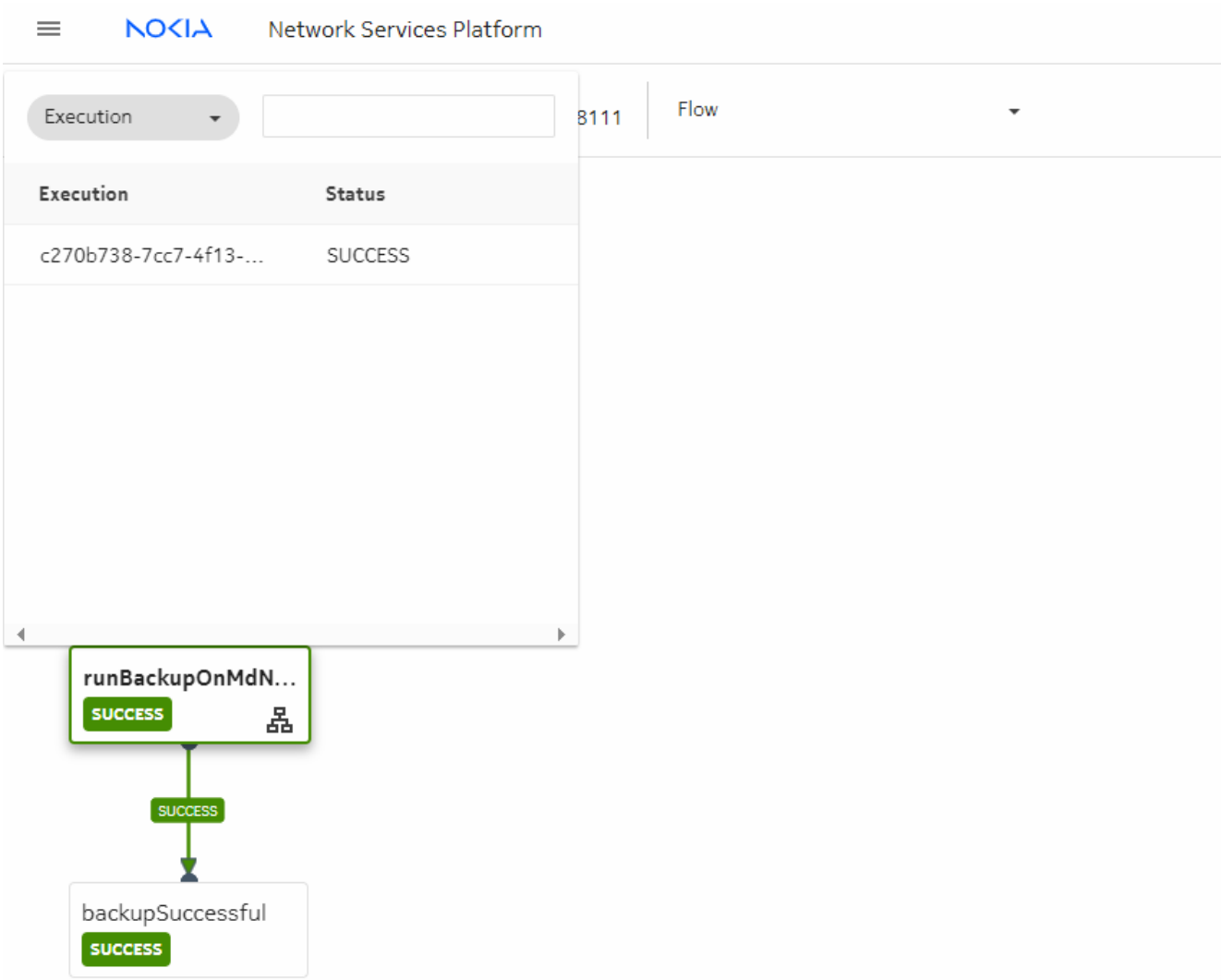
- Select a task and click Action Executions to see the list of actions executed by the task.

For this example, `runBackupOnMdNode` represents most of the runtime of the workflow, and it took 16 seconds to run. This provides expected behavior to compare to a workflow that may be running slowly.

The list of actions performed also shows whether the workflow is transferring files, calling APIs, or communicating with other applications. Problems with any of these could be the cause of a slowdown or failure.

4

Double-click on a sub-workflow task to see the execution status.



Double click on the execution status to open the info page for the sub-workflow execution in a new tab, and investigate actions and tasks executed by the sub-workflow.

END OF STEPS

5.15.4 Check the process of a slow workflow

1

Double-click on a workflow execution, and select **Tasks** from the Info drop-down. The Tasks list shows the time stamps when each task was created, and each task's run time.

The Created column shows the time since the task was created. Hover over a time in the Created column to see the precise time of creation.

2

Check for delays in the sequence of tasks. For example, if one task was created at midnight and had a run time of 2 seconds, the following task should be created at 2 seconds after midnight.

3

If there are delays, NSP is experiencing slowness due to memory usage. When database usage is high, it takes longer than expected to query the database for the next action.

If you are experiencing these delays, your cleanup policy may need to be adjusted. For more information, see the *NSP Network Automation Guide*.

END OF STEPS

5.15.5 Check concurrency

If a workflow is experiencing slowdowns or API errors, check for tasks with loops and ensure the concurrency is set correctly. If NSP is creating too many actions at one time, the workflow database could be impacted, causing slowdowns, or APIs could be overwhelmed with too many simultaneous calls.

1

From the Workflows page, double click on a workflow to open the Info page. Choose **Definition** from the Info drop-down.

2

In the YAML panel, search for a task with a `with-item` statement. The `with-item` statement provides the number of times the task will initiate the action.

3

Verify that any task with a `with-item` statement also has a `concurrency` property set.

The `concurrency` property sets a limit on the number of times the task will create the action concurrently. For example, if the `concurrency` is set to 1, the task will create the action once and wait for it to complete before executing it again.

4

Ensure that the concurrency value and the size of the with-items loop are appropriate for the task. For example, if the task is an API call, ensure that the concurrency is low enough to prevent the resource from being overwhelmed with simultaneous API calls. Remember that this workflow may not be the only entity calling the API at the time you execute it.

END OF STEPS

5.15.6 Check task output

If a workflow is experiencing slowdowns or getting stuck in a Running state, resource usage may be impacted by large amounts of output.

1

From the Workflows page, double click on a workflow to open the Info page. Choose **Definition** from the Info drop-down.

2

In the YAML panel, search for the `output` statements for the tasks and the workflow itself, as applicable.

3

Ensure that output for all tasks is as minimal as possible. This minimizes the database usage of each task execution and helps to prevent resource overload. For more information; see the Mistral documentation and the Best Practices section in the Network Automation tutorial on the Network Developer Portal.

END OF STEPS

5.15.7 Heartbeat errors

A `Heartbeat not received` error occurs when a workflow attempts to contact an API or NSP and no response is received within ten minutes. Check logs to verify the source of the error.

1

Check the logs for the Mistral executor to see whether responses were received from the other entity.

2

Check logs for the RabbitMQ messaging bus to see whether there was an interruption to monitoring, which may have caused Mistral to miss a response.

END OF STEPS

6 Network troubleshooting using NFM-P

6.1 Overview

6.1.1 Purpose

This chapter provides information about troubleshooting a managed network using the NFM-P.

6.1.2 Contents

Troubleshooting services and connectivity

6.2 Service and connectivity diagnostics

6.2.1 STM OAM diagnostics for troubleshooting

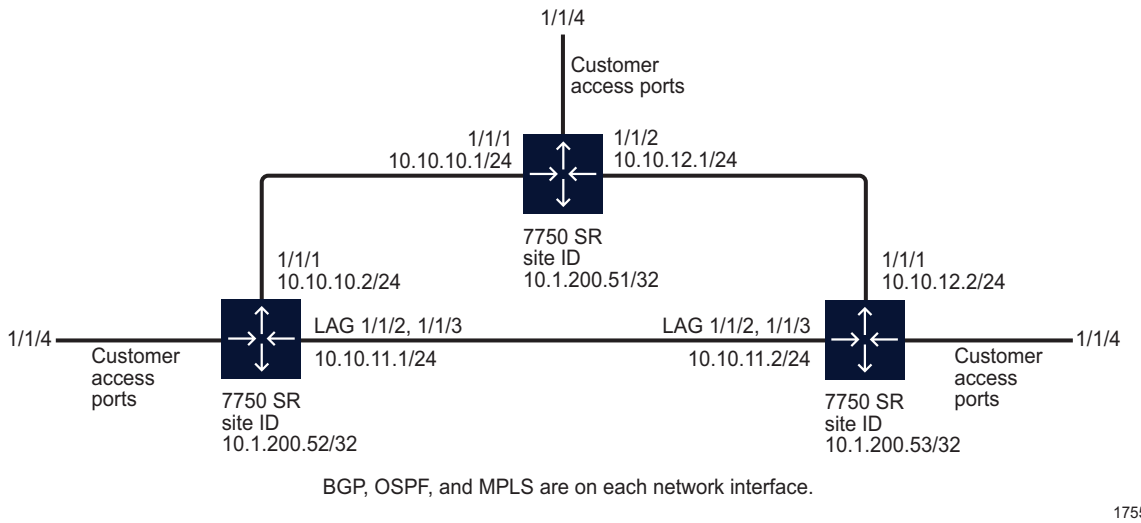
This chapter documents how to troubleshoot service and general connectivity problems when there is no associated alarm condition.

You can use the NFM-P Service Test Manager, or STM, OAM diagnostic tools for network troubleshooting and for verifying compliance with SLAs. The STM provides the ability to group OAM diagnostic tests into test suites for more comprehensive fault monitoring and troubleshooting. A test suite can perform end-to-end testing of a customer service and the underlying network transport elements. The use of test suites is especially valuable when multiple objects of the same type require testing. Test suites can be scheduled to run on a regular basis to provide continual network performance feedback. See the *NSP NFM-P Classic Management User Guide* for information about using the STM and creating scheduled tasks.

6.2.2 OAM diagnostics sample network

The configuration below shows a network that is used as an example for the OAM diagnostics procedures in this chapter.

Figure 6-1 Sample network



6.3 Workflow to troubleshoot a service or connectivity problem

6.3.1 Purpose

Perform the following tasks in sequence until you identify the root cause of the problem.

6.3.2 Stages

1

Verify that there are no alarms associated with the service by clicking on the Faults tab in the Service form.

a. If there are no alarms that affect the service, see Stage 2.

2

If you are troubleshooting a VPLS service, determine whether it is part of an H-VPLS configuration. See 6.4 “To identify whether a VPLS is part of an H-VPLS” (p. 335).

3

Verify whether the administrative and operational states of each component of the service are Up; see 6.5 “To verify the operational and administrative states of service components” (p. 336).

4

Verify the connectivity of the customer equipment using the entries in the FIB; see 6.6 “To verify the FIB configuration” (p. 337).

5

Verify that the NFM-P service configuration aligns with the customer requirements. For example, ensure that NFM-P configuration uses the correct service type and SAP configuration, and that the circuit and site are included in the service.

6

Verify the connectivity of all egress points in the service:

a. using MAC Ping and MAC Trace; see 6.7 “To verify connectivity for all egress points in a service using MAC Ping and MAC Trace” (p. 338).

b. using MEF MAC Ping; see 6.8 “To verify connectivity for all egress points in a service using MEF MAC Ping” (p. 340).

7

Use the results from the MAC Ping and MAC Trace diagnostics to choose one of the following options:

a.

If the MAC Ping, MEF MAC Ping, or MAC Trace diagnostics returned the expected results for the configuration of your network:

1. Measure the frame transmission size on all objects associated with the service such as the service sites, access and network ports, service tunnels, and circuits; see 6.9 “To measure frame transmission size on a service using MTU Ping” (p. 342).
2. Review the ACL filter policies to ensure that the ACL filter for the port is not excluding packets that you want to test; see 6.14 “To review ACL filter properties” (p. 350).

3. Verify the QoS configuration.

b.

If the MAC Ping and MAC Trace diagnostics did not return the expected results for the configuration of your network:

1. Verify the end-to-end connectivity on the service using the Service Site Ping diagnostic; see 6.10 “To verify the end-to-end connectivity of a service using Service Site Ping” (p. 343).
2. Verify the end-to-end connectivity on the service tunnel using the Tunnel Ping diagnostic; see 6.11 “To verify the end-to-end connectivity of a service tunnel using Tunnel Ping” (p. 345).
3. Verify the end-to-end connectivity of an MPLS LSP using the LSP Ping diagnostic; see 6.12 “To verify end-to-end connectivity of an MPLS LSP using LSP Ping” (p. 347).

c.

If the MAC Ping diagnostic returned the expected results for the configuration of your network, and the MAC Trace diagnostic did not return the expected results for the configuration of your network:

1. Verify that the correct service tunnels are used for the service.
2. Correct the service tunnel configuration, if required.
3. Review the route for the MPLS LSP using the LSP Trace OAM diagnostic. (For MPLS encapsulation, only.) If the LSP Trace results do not meet the requirements of your network, review the resource availability and configurations along the LSP expected routes; see 6.13 “To review the route for an MPLS LSP using LSP Trace” (p. 349).

8

As required, perform one or more of the following.

a. Review ACL filter properties; see 6.14 “To review ACL filter properties” (p. 350).

b. View anti-spoof filters; see 6.15 “To view anti-spoof filters” (p. 351).

c. Retrieve MIB information from a GNE using the snmpDump utility; see 6.16 “To retrieve MIB information from a GNE using the snmpDump utility” (p. 352).

9

Contact your technical support representative if the problem persists; see Chapter 1, “NSP troubleshooting overview” .

6.4 To identify whether a VPLS is part of an H-VPLS

6.4.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu.

2

Choose the service associated with the service problem.

3

Click Properties. The Service form opens.

4

Click on the Mesh SDP Bindings or Spoke SDP Bindings tab.

5

Drag and drop the Service ID, VC ID, and Service Type columns to first three positions on the left side of the form.

6

Sort the list by VC ID.

If a VC ID has more than one unique Service ID, these services are involved in an H-VPLS relationship.

a. If there are no alarms on the H-VPLS service, go to Stage 3 in 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

END OF STEPS

6.5 To verify the operational and administrative states of service components

6.5.1 Steps

1

Open the service properties form.

2

On the navigation tree, click on the site on which you want to verify the operational and administrative states of service components; expand the entries for that site.

3

Click on the site. The *service* (Edit) form opens. Review the states for the site using the Operational State and Administrative State parameters.

4

On the navigation tree, click on the L2 Access Interfaces, L3 Access Interfaces, and Mesh SDP Bindings or Spoke SDP bindings objects to review the operational and administrative states for the remaining components of the service.

5

Use the operation and administrative states of the service components to choose one of the following options:

a. If the operational and administrative states for all service components are Up, go to Stage 4 in 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333) .

b. If the operational state is Down and the administrative state is Up for one or more service components, the NFM-P generates an alarm. You must investigate the root problem on the underlying object.

c. If the administrative state is Down for one or more service components, change the administrative state to Up. Go to Step 7 .

6

If the service problem persists, another type of service problem may be present. Perform the steps of the 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333) troubleshooting workflow.

7

If the workflow does not identify the problem with your service, contact your technical support representative. See Chapter 1, “NSP troubleshooting overview” for more information.

END OF STEPS

6.6 To verify the FIB configuration

6.6.1 Purpose

This procedure describes how to verify the connectivity of customer equipment on the service tunnel.

6.6.2 Steps

1

Click on the L2 Access Interfaces tab on the Services (Edit) form. A list of L2 access interfaces appears.

2

Double-click on a row in the list. The L2 Access Interface form appears.

3

Click on the Forwarding Control tab.

4

Click on the FIB Entries tab.

5

Click Resync.

a. If there is a list of FIB entries, confirm the number of entries with the customer configuration requirement. If the configuration meets the customer requirement, go to Stage 5 in 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

b. If there are no FIB entries, there is a configuration problem with the customer equipment or the connection from the equipment to the service tunnel.

   1. Confirm that the NFM-P service configuration aligns with the customer requirements.
   2. Confirm that there are no problems with the customer equipment and associated configuration.

6

If the service problem persists, another type of service problem may be present. Perform the steps of the 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333) troubleshooting workflow.

7

If the workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, “NSP troubleshooting overview”.

END OF STEPS

6.7 To verify connectivity for all egress points in a service using MAC Ping and MAC Trace

6.7.1 Steps

1

Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears.

2

Click Create.

3

Choose L2 Service→Create MAC Ping from the Create contextual menu. The MAC Ping (Create) form appears.

4

Clear the results from the previous diagnostic session from the Results tab, if necessary.

Note: You must use the MAC Ping and MAC Trace diagnostic to test the service in both directions for the connection.

5

Configure the required parameters for the diagnostic session and run the diagnostic.

a. You can target the MAC broadcast address of FF-FF-FF-FF-FF-FF in the data plane to flood the service domain and receive a response from all operational service access ports. Enter the service ID for the VPLS or VLL service between the sites, and the sites you want to ping, in this case, from site ID 10.1.200.51/32 to site IDs 10.1.200.52/32 and 10.1.200.53/32 using the network in Figure 6-1, “Sample network” (p. 333).

   Click on the Results tab to view the list of ping responses. Double-click on a row in the list to view its details.

b. You can target the specific MAC address of a service site. Enter the target MAC address of the specific site in the service that you want to ping, in this case, from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 6-1, “Sample network” (p. 333).

   Click on the Results tab to view the list of ping responses. Double-click on a row in the list to view its details.

6

Review the results and assess whether the configuration meets the network requirements.

In particular, review the results in the Return Code column. The table below lists the displayed messages.

Table 6-1 MAC Ping OAM diagnostic results

Displayed message	Description
notApplicable (0)	The OAM diagnostic message does not apply to the OAM diagnostic performed.
fecEgress (1)	The replying router is an egress for the FEC. The far-end egress point exists and is operating correctly. No action required.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.
downstreamNotMacFlood (7)	The replying router is a downstream router, but it does not have the specified MAC address and cannot flood the request to other routers.
malformedEchoRequest (8)	The received echo request is malformed.
tlvNotUnderstood (9)	One or more TLVs were not understood.

7

Click Create.

8

Choose L2 Service→Create MAC Trace from the Create contextual menu. The MAC Trace (Create) form appears.

9

Configure the required parameters for the diagnostic session and run the diagnostic. A MAC Trace shows the path, protocol, label, destination SAP, and hop count to the location of the destination MAC. Enter the service ID for the VPLS or VLL service between the sites, and the sites you want to trace, in this case, from site ID 10.1.200.51/32 to site IDs 10.1.200.52/32 and 10.1.200.53/32 using the network in Figure 6-1, “Sample network” (p. 333) .

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details.

10

Review the diagnostic results and assess whether the configuration meets the network requirements.

a. If MAC Ping and MAC Trace diagnostics returned the expected results for the configuration of your network, go to Stage 7 a in 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

b. If MAC Ping and MAC Trace diagnostics did not return the expected results for the configuration of your network, go to Stage 7 b in 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

c. Go to Stage 7 c in 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333) if:

- MAC Ping diagnostic returned the expected result for the configuration of your network
- MAC Trace diagnostic did not return the expected result for the configuration of your network

END OF STEPS

6.8 To verify connectivity for all egress points in a service using MEF MAC Ping

6.8.1 Steps

1

Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears.

2

Click Create.

3

Choose L2 Service→Create MEF MAC Ping from the Create contextual menu. The MEF MAC Ping (Create) form appears.

4

Clear the results from the previous diagnostic session from the Results tab, if necessary.

Note: MEF MAC Ping must run simultaneously in both directions between the source and destination VPLS sites.

5

Configure the required parameters for the diagnostic session and run the diagnostic.

You can target the specific MAC address of a service site. Enter the target MAC address of the specific site in the service that you want to ping.

Click on the Results tab to view the list of ping responses. Double-click on a row in the list to view its details.

6

Review the results and assess whether the configuration meets the network requirements.

In particular, review the results in the Return Code column. The table below lists the displayed messages.

Table 6-2 MEF MAC Ping OAM diagnostic results

Displayed message (return code)	Description
responseReceived (1)	A response was received on the device to the OAM diagnostic performed.
requestTimedOut (5)	The OAM diagnostic could not be completed because no reply was received within the allocated timeout period.

7

Review the diagnostic results and assess whether the configuration meets the network requirements.

a. If MEF MAC Ping diagnostics returned the expected results for the configuration of your network, go to Stage 7 a in 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

END OF STEPS

6.9 To measure frame transmission size on a service using MTU Ping

6.9.1 Steps

1

Record the maximum frame transmission size for the service.

2

Choose Manage→Service Tunnels from the NFM-P main menu. The Manage Service Tunnels form appears.

3

Filter to list only the source and destination routers of the service tunnel and click Search. The list of service tunnels appears.

4

Double-click on a service tunnel from the list. The Tunnel (Edit) form appears.

5

Click on the Tests tab.

6

Click on the MTU Ping tab and click Create. The MTU Ping (Create) form appears with the General tab selected. The form displays information about the service tunnel being tested and the originating tunnel ID.

Note: You must use the MTU Ping diagnostic to test the service in both directions for the connection.

7

Configure the required parameters for the diagnostic session. Click on the Test Parameters tab and enter the MTU value recorded in Step 1 for the MTU End Size (octets) parameter.

8

Run the diagnostic. The MTU Ping increments the datagram size until it fails to pass through the SDP (service tunnel) data path, in this case, an MTU Ping from site ID 10.1.200.52/32 to site ID 10.1.200.53/32 using the network in Figure 6-1, “Sample network” (p. 333).

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. The number of responses is determined by the incremental increase in datagram size.

9

Review the diagnostic results and assess whether the configuration meets the network requirements. Click on the Packets tab.

a. If the Status column displays Response Received for all circuits, the service tunnel supports the configured frame transmission size for the circuit. Go to Stage 7 a 2 in 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

b. If the Status column displays Request Timed Out for any of the circuits, the transmission failed at that frame size. If the frame size for the failure point is below the MTU value configured for the service, the packets are truncating along the service route. Investigate the cause of the truncated packets.

10

If the service problem persists, another type of service problem may be present. Perform the steps of the troubleshooting workflow in this chapter.

11

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, “NSP troubleshooting overview”.

END OF STEPS

6.10 To verify the end-to-end connectivity of a service using Service Site Ping

6.10.1 Steps

1

Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears.

2

Click Create.

3

Choose Service→Create Service Site Ping from the Create contextual menu. The Service site ping (Create) form appears.

Note: You must use the Service Site Ping diagnostic to test the service in both directions for the connection.

4

Configure the required parameters for the diagnostic session and run the diagnostic.

The originating service tunnel for the Service Site Ping is from site ID 10.1.200.51/32 to site ID 10.1.200.53/32, the other end of the service using the network in Figure 6-1, “Sample network” (p. 333).

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details.

5

Review the diagnostic results and assess whether the configuration meets the network requirements. The table below lists the displayed messages.

Table 6-3 Service Site Ping OAM diagnostic results

Displayed message	Description
Sent - Request Timeout	The request timed out with a reply.
Sent - Request Terminated	The request was not sent because the diagnostic was terminated by the operator.
Sent - Reply Received	The request was sent and a successful reply message was received.
Not Sent - Non-Existent Service-ID	The configured service ID does not exist.
Not Sent - Non-Existent SDP for Service	There is no SDP for the service tested.
Not Sent - SDP For Service Down	The SDP for the service is down.
Not Sent - Non-Existent Service Egress Label	There is a service label mismatch between the originator and the responder.

a. If the Service Site ping passes, the routes between the two sites are complete and in an operational state. If the MAC Ping performed in 6.7 “To verify connectivity for all egress points in a service using MAC Ping and MAC Trace” (p. 338) failed:

1. Investigate the status of the two SAPs used for the circuit.
2. Correct the configuration issue related to the SAPs, if required.

   If there is no configuration problem with the SAPs, the service problem is related to the MAC addresses.

   The MAC address problem could be caused by the:
   - ACL MAC filter excluding the required MAC address
   - external customer equipment

b. If the Service Site Ping fails, there is a loss of connectivity between the two sites.

1. Log in to one of the sites using the CLI.
2. Enter the following command:

   `ping <destination_site_ip_address>` ↵

   where <*destination_site_ip_address*> is the address of the other site in the route

   If the CLI IP ping passes, go to Stage 7 b 2 of 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

6

Use the CLI to verify that the IP address of the destination site is in the routing table for the originating site by entering:

show router route-table ↵

If the IP address for the destination site is not in the routing table for the originating site, there is an L3 or L2 problem.

1. Verify that the appropriate protocols are enabled and operational on the two sites.
2. Verify the administrative and operational states of the underlying L2 equipment, for example, ports and cards.

7

If the service problem persists, another type of service problem may be present. Perform the steps 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

8

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, “NSP troubleshooting overview”.

END OF STEPS

6.11 To verify the end-to-end connectivity of a service tunnel using Tunnel Ping

6.11.1 Steps

1

Choose Manage→Service Tunnels from the NFM-P main menu. The Manage Service Tunnels form appears.

2

Filter to list only the source and destination routers of the service tunnel and click Search. The list of service tunnels appears.

3

Double-click on a service tunnel from the list. The Tunnel (Edit) form appears.

4

Click on the Tests tab.

5

Click on the Tunnel Ping tab and click Create. The Tunnel Ping (Create) form appears with the General tab displayed. The form displays information about the circuit being tested, including the originating tunnel ID.

Note: You must use the Tunnel Ping diagnostic to test the service in both directions for the connection.

6

Configure the required parameters for the diagnostic session as follows.

- The Return Tunnel parameter must specify the return tunnel ID number, because the tunnels are unidirectional.
- From the Test Parameters tab, the Forwarding Class parameter must specify the forwarding class for the service tunnel. Make sure that the forwarding classes for the service tunnels map to the QoS parameters configured for customer services, such as VLL.
- The Number of Test Probes and Probe Interval parameters must be configured to send multiple probes.

7

Run the diagnostic. Set the diagnostic configuration for a Tunnel Ping from site ID 10.1.200.51/32 to site ID 10.1.200.53/32 using the network in Figure 6-1, “Sample network” (p. 333) , by specifying the return ID of the tunnel you want to test.

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. Double-click on the entry in the Tunnel Ping results form to view the diagnostic details.

8

Review the diagnostic results and assess whether the configuration meets the network requirements.

The table below lists the displayed messages.

Table 6-4 Tunnel OAM diagnostic results

Displayed message	Description
Request Timeout	The request timed out with a reply.
Orig-SDP Non-Existent	The request was not sent because the originating SDP does not exist.
Orig-SDP Admin-Down	The request was not sent because the originating SDP administrative state is Down.
Orig-SDP Oper-Down	The request was not sent because the originating SDP operational state is Down.
Request Terminated	The operator terminated the request before a reply was received, or before the timeout of the request occurred.
Far End: Originator-ID Invalid	The request was received by the far-end, but the far-end indicates that the originating SDP ID is invalid.
Far End: Responder-ID Invalid	The request was received by the far-end, but the responder ID is not the same destination SDP ID that was specified.
Far End:Resp-SDP Non-Existent	The reply was received, but the return SDP ID used to respond to the request does not exist.
Far End:Resp-SDP Invalid	The reply was received, but the return SDP ID used to respond to the request is invalid.

Table 6-4 Tunnel OAM diagnostic results (continued)

Displayed message	Description
Far End:Resp-SDP Down	The reply was received, but the return SDP ID indicates that the administrative or operational state of the SDP is Down.
Success	The tunnel is in service and working as expected. A reply was received without any errors.

a. If the Tunnel Ping passes, the network objects below the tunnel are operating with no performance issues.

b. If the Tunnel Ping fails, go to Stage 7 b 3 of 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333) to verify the end-to-end connectivity of services using MPLS LSP paths, if required.

9

If the service problem persists, another type of service problem may be present. Perform the steps of 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333) .

10

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, “NSP troubleshooting overview”.

END OF STEPS

6.12 To verify end-to-end connectivity of an MPLS LSP using LSP Ping

6.12.1 Steps

1

Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears.

2

Click Create.

3

Choose MPLS→Create LSP Ping from the Create contextual menu. The LSP Ping (Create) form appears.

Note: You must use the LSP Ping diagnostic to test the service in both directions for the connection.

4

Configure the required parameters for the diagnostic session and run the diagnostic. Target an LSP or an LSP path. Choose the MPLS site for the test, then configure the LSP you want to

ping that is associated with the MPLS site, in this case, an LSP Ping from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 6-1, “Sample network” (p. 333).

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. Double-click on the entry in the LSP Ping results form to view the diagnostic details.

5

Review the diagnostic results and assess whether the configuration meets the network requirements.

The table below lists the displayed messages.

Table 6-5 LSP Ping OAM diagnostic results

Displayed message	Description
notApplicable (0)	The OAM diagnostic message does not apply to the OAM diagnostic performed.
fecEgress (1)	The replying router is an egress for the FEC. The far-end egress point exists and is operating correctly. No action required.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.
downstreamNotMacFlood (7)	The replying router is a downstream router, but it does not have the specified MAC address and cannot flood the request to other routers.
malformedEchoRequest (8)	The received echo request is malformed.
tlvNotUnderstood (9)	One or more TLVs were not understood.

a. If the LSP Ping passes, you have completed the workflow for troubleshooting services. Contact your technical support representative if the problem persists; see Chapter 1, “NSP troubleshooting overview”.

b. If the LSP Ping fails, verify the administrative and operational status of the underlying L2 equipment.

6

If the service problem persists, another type of service problem may be present. Perform the steps of 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

7

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, “NSP troubleshooting overview”.

END OF STEPS

6.13 To review the route for an MPLS LSP using LSP Trace

6.13.1 Steps

1

Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears.

2

Click Create.

3

Choose MPLS→Create LSP Trace from the Create contextual menu. The LSP trace create form appears.

Note: You must use the LSP Trace diagnostic to test the service in both directions for the connection.

4

Configure the required parameters for the diagnostic session and run the diagnostic. Target an LSP, any LSP or an LSP path. Choose the MPLS site for the test, then configure the LSP or LDP you want to trace that is associated with the MPLS site, in this case, an LSP Ping from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 6-1, “Sample network” (p. 333).

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. Double-click on the entry in the LSP Trace results form to view the diagnostic details.

5

Review the diagnostic results and assess whether the configuration meets the network requirements.

a. If the LSP Trace returned the expected results for the configuration of your network, the troubleshooting is complete.

b. If the LSP Trace did not return the expected results for the configuration of your network, verify that the correct MPLS LSP is used for the service.

6

If the service problem persists, another type of service problem may be present. Perform the

steps of 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

7

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, “NSP troubleshooting overview”.

END OF STEPS

6.14 To review ACL filter properties

6.14.1 Steps

1

Click on the L2 Access Interfaces or L3 Access Interfaces tabs on the Services (Edit) form. A list of interfaces appears.

2

Double-click on a row in the list. The L2 or L3 Interface configuration form appears.

3

Click on the ACL tab.

4

Review the ingress and egress filter configurations to ensure that ACL filtering configurations do not interfere with the service traffic.

a. If there are no ACL filtering configurations that interfere with the service traffic, go to Stage 7 a 2 in 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

b. If there are ACL filtering configurations that interfere with the service traffic, implement and verify the solution for the service problem.

5

If the service problem persists, another type of service problem may be present. Perform the steps of 6.3 “Workflow to troubleshoot a service or connectivity problem” (p. 333).

6

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, “NSP troubleshooting overview”.

END OF STEPS

6.15 To view anti-spoof filters

6.15.1 Purpose

If a host is having a problem connecting to the network, one possibility for the problem is dropped packets as a result of anti-spoofing filters on the SAP. The NFM-P allows you to view the anti-spoof filters currently in effect on a SAP.

Anti-spoof filters are frequently created and deleted in the network. As a result, the NFM-P does not keep synchronized with the anti-spoof filters on the managed devices. However, the NFM-P allows you to retrieve, on demand, the current anti-spoof filters for a SAP.

6.15.2 Steps

1

Select Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Select the service for which you want to view the anti-spoof filters.

3

Click Properties. The Service (Edit) form opens.

4

Click on the L2 Access Interfaces or L3 Access Interfaces tab, depending on the service that you selected.

5

Select an interface from the list and click Properties. The Access Interface (Edit) form opens.

6

Click on the Anti-Spoofing tab.

7

Click on the Filters tab.

8

Click Search to retrieve the current anti-spoof filters for the SAP. The Filters tab refreshes with a list of the current anti-spoof filters.

END OF STEPS

6.16 To retrieve MIB information from a GNE using the snmpDump utility

6.16.1 Purpose

Perform this procedure to export all object values from the NFM-P-supported SNMP MIBs on a GNE. The exported information may help with troubleshooting the GNE configuration on the device or in the NFM-P.

6.16.2 Steps

1

Log in to an NFM-P main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

4

Enter the following:

`./snmpDump.bash option_list` ↵

where *option_list* is one or more of the options listed in Table 6-6, “snmpDump .bash options” (p. 351)

Note: Each option must be separated by a space, as shown in the following example:
snmpDump.bash -v 3 -h 192.168.18.77 -u jsmith -apw mypass -ppw yoda
If an option has a default value, the default value is included in the option description.

Table 6-6 snmpDump .bash options

Option	Description
-v *version*	The SNMP version in use on the GNE Default: 2
-f *file_name*	The output filename Default: *host*-snmpDump.out in the current directory
-h *host*	The IP address or hostname of the GNE Default: localhost
-c *community*	The SNMP community
-u *v3_user*	The SNMPv3 user name
-e *snmp_engine_ID*	The SNMP engine ID

Table 6-6 snmpDump .bash options (continued)

Option	Description
-ap *v3_auth_protocol*	The SNMPv3 authorization protocol, which can be MD5 or SHA Default: MD5
-apw *v3_auth_password*	The SNMPv3 authorization password
-ppw *v3_privacy_password*	The SNMPv3 privacy password
-cn *v3_context_name*	The SNMPv3 context name
-ci *v3_context_ID*	The SNMPv3 context ID
-p *port*	The TCP port on the main server that snmpDump must use to reach the GNE Default: 161
-t *timeout*	A communication timeout value
-r *retries*	The number of times to retry connecting to the GNE

The utility displays status messages similar to the following as it initializes:

```
Init Products ...
Init ProductFamilyDefs ...
Init PollingDirectiveDefs ...
Start reading from Node ...
```

The utility then begins to retrieve the MIB tables. As It processes a MIB table, it lists the table name and the number of entries the table contains, as shown below:

```
IF-MIB.ifEntry : 21
IP-MIB.ipAddrEntry : 5
MPLS-LSR-STD-MIB.mplsInterfaceEntry : 8
MPLS-TE-STD-MIB.mplsTunnelEntry : 0
MPLS-TE-STD-MIB.mplsTunnelHopEntry : 0
MPLS-TE-STD-MIB.mplsTunnelARHopEntry : 0
MPLS-TE-STD-MIB.mplsTunnelCHopEntry : 0
MPLS-LDP-STD-MIB.mplsLdpEntityEntry : 3
MPLS-LDP-STD-MIB.mplsLdpEntityStatsEntry : 3
MPLS-LDP-STD-MIB.mplsLdpPeerEntry : 3
```

The utility is finished when the command prompt is displayed.

5

To view the utility output, open the file using a MIB browser or a text editor.

END OF STEPS

Troubleshooting using the NE resync audit function

6.17 NE resync auditing overview

6.17.1 Functional description

The NE resync audit function detects and reports differences between the NFM-P database version of the NE configuration and the version stored on the NE. The NE resync audit manager displays a list of misaligned parameters and values as represented in the NE and NFM-P databases, and provides quick navigation to the affected object. A resync audit polls the NE in the same manner as a standard full resynchronization, but instead of updating the objects in the NFM-P database, the NFM-P compares the NE configuration retrieved by the resync with the NE configuration in the NFM-P. See 6.20 “To perform an NE resync audit” (p. 356) for information about performing an NE resync audit.

Differences identified during the audit are displayed in the Show Difference manager. In this manager, you can navigate to the associated NE object that contains the difference and perform a resync on that object to resolve the difference. You can access the results of one audit per NE in the NE audit result list.

You can specify whether to include or ignore read-only parameters in a resync audit. Some read-only parameters are set by the NE after a configuration change. Other read-only parameters, such as temperature measurements and time stamps, change frequently on the NE and will often differ from the values in the NFM-P database. Disabling the inclusion of read-only parameters can help prevent cluttered audit results.

The difference entries that an NE resync audit returns are categorized as follows:

- Property Change—the value of a specific parameter is different in the NFM-P and NE databases
- Missing—the object and contained parameters exist in the NFM-P, but not on the NE
- Added—the object and contained parameters exist on the NE, but not in the NFM-P

6.17.2 Additional information

Consider the following information about NE resync audits:

- The NFM-P limits the audit result to 1 000 differences.
- NE resync audits only compare parameters that are synchronized with the NFM-P database. Parameters that are stored in the NE database only and are not managed by the NFM-P are not included in the audit report.
- NE resync audit results do not include statistics.
- NE resync audits cannot be used to deploy changes to an NE.
- You cannot perform a full resync from the NE audit manager or Show Differences form.
- Dynamic read-only objects and dynamic parameters are excluded from NE resync audits. For example, the following objects are excluded: LDP session, RSVP session, MPLS In Segment, Out Segment, Cross Connect, MPLS Actual Hop and Actual Path, ISIS SPF Log.

6.18 Workflow for NE resync auditing

6.18.1 Stages

1

Perform NE resync auditing to identify specific object and parameter misalignment between an NE and the NFM-P; see 6.20 “To perform an NE resync audit” (p. 356) .

2

View the results of NE resync audits and manage audit results; see 6.21 “To view NE resync audit results using the NE audit manager” (p. 357) .

3

Clear the SDP binding Frame Size Problem alarm; see 6.19 “To clear a Frame Size Problem (MTU Mismatch) alarm” (p. 354) .

6.19 To clear a Frame Size Problem (MTU Mismatch) alarm

6.19.1 Purpose

This procedure describes how to clear the SDP binding Frame Size Problem alarm.

6.19.2 Steps

1

Choose Manage→Service→Services from the NFM-P main menu.

2

Choose the service identified by the Alarmed Object Id in the Alarm Info form for the alarm that you are trying to clear.

3

Click Properties. The Service form opens.

4

Click on the Sites tab. The list of available sites for the service appears.

5

Choose the site identified by the Site Id in the Alarm Info form for the alarm that you are trying to clear.

6

Click Properties. The Site form opens.

7

Change the MTU to a value less than 1492, for example, 1000.

8

Save your changes. The MTU configuration change is applied to customer, service, and site objects. The SDP binding and related service alarms clear automatically.

END OF STEPS

6.20 To perform an NE resync audit

6.20.1 Steps

1

Choose Equipment from the navigation tree view selector. The managed NEs are displayed.

2

Right-click on an NE and choose NE Resync Audit.

3

Enable the check box if you want to include read-only attributes in the audit and click Yes. The NE Audit Result form appears and displays the NE Audit State as “in progress”.

Note: The NFM-P displays an error message and does not begin the resync audit if the NE in unreachable.

4

When the audit completes, choose one of the following based on the NE Audit State:

a. If the NE Audit State displays “succeeded” and the NE Audit Result displays “misaligned”, go to Step 5 .

b. If the NE Audit State displays “succeeded” and the NE Audit Result displays “aligned”, then no further action is required.

c. If the NE Audit State displays “failed”, information about the failure is displayed in the Error Messages panel. Click to expand the panel.

5

Click Show Difference. The Show Difference form opens with a list of difference entries displayed.

6

To resync a missing or added object, perform a full resync.

7

To resync a property change for a single object with the NFM-P:

1. Select a difference entry from the list. The panes at the bottom of the form display the misaligned data for the entry.
2. Click Properties for the SAM Object. The Properties form of the object is displayed.
3. Click Resync.
4. Click Yes and wait for the object to resync with the NFM-P. The value of the misaligned parameter changes if the resync operation is successful.

8

To save the results of the resync audit to an HTML or CSV file:

1. Right-click on a column header in the differences list and choose Save to File. The Save As form is displayed.
2. Navigate to the required location on the client workstation and specify a file name.
3. Choose a file type and click Save.

9

Close the forms.

END OF STEPS

6.21 To view NE resync audit results using the NE audit manager

6.21.1 Purpose

You can use the NE audit manager to view the results of previous NE audits and delete audit results.

6.21.2 Steps

1

Choose Administration→NE Maintenance→NE Audit Results from the NFM-P main menu. The NE Audit Manager list form opens.

2

To view an entry, select an entry from the list and click Show Difference. If there are results to display, the Show Difference form opens.

3

To delete an entry:

1. Select an entry from the list and click Delete.

2. Click Yes. The entry is deleted.

4

Close the NE Audit Manager list form.

END OF STEPS

Troubleshooting network management LAN issues

6.22 Problem: All network management domain stations experience performance degradation

6.22.1 Steps

1

Verify that there is sufficient bandwidth between the elements of the network management domain.

Bandwidth requirements vary depending on the type of management links set up, and the number of devices in the managed networks. For information about network planning expertise, contact your technical support representative.

See the *NSP Planning Guide* for more information about the bandwidth requirements.

2

When you are using in-band management, ensure that the network devices used to transport the management traffic are up. Ping each of the devices to ensure the management traffic can flow along the in-band path.

In-band management uses a connection provided by a customer service, such as a VLL. The management traffic is sent in-band along with the customer payload traffic. The packets with the management data arrive at the device using one of the virtual interfaces.

END OF STEPS

6.23 Problem: Lost connectivity to one or more network management domain stations

6.23.1 Purpose

Perform this procedure on a RHEL or Windows station to check the reachability of another station.

6.23.2 Steps

1

Log in to the station.

2

Open a console window.

3

Enter the following:

`ping` *`station`* ↵

where *station* is the station hostname or IP address

4

To interrupt the ping operation, press Ctrl+C.

5

Review the output, which resembles the following when connectivity is good:

```
PING station: 56 data bytes
64 bytes from station (192.168.106.169): icmp_seq=1, time=1.0 ms
64 bytes from station (192.168.106.169): icmp_seq=2, time=0.3 ms
64 bytes from station (192.168.106.169): icmp_seq=3, time=0.2 ms
----station PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
rtt (ms) min/avg/max = 0.2/0.7/1.0
```

6

If the packets arrive out of order, if some packets are dropped, or if some packets take too long to complete the round trip, LAN congestion may be a problem. Contact your IT department or check the physical LAN connectivity.

7

If you can ping the station, but are unable to connect to the station to perform a function, there may be a problem with access to a function on the station.

If the NFM-P deployment includes a firewall, the firewall log entries are in the /var/log/messages file on a RHEL station.

See 6.24.1 “Purpose” (p. 360) for information about how to verify the following:

- ports that need to be open across firewalls
- routing configuration

END OF STEPS

6.24 Problem: Another station can be pinged, but some functions are unavailable

6.24.1 Purpose

Perform this procedure to determine whether port availability or routing is the cause of a management domain LAN issue.

The NFM-P uses TCP and UDP ports for communication between components. Some of the ports, such as the SNMP trap port, are configured during installation. Other ports are configured automatically by the NFM-P software.

6.24.2 Steps

1

Log in as the root user on a station in the network management domain.

2

Verify that the required ports are open or protected by a firewall. See the *NSP Planning Guide* for a complete list of the ports that the NFM-P requires and the purpose of each port.

Note: If you modify the port configuration, ensure that you record the changes for future reference.

3

Perform the following steps to check the local routing configuration.:

1. Open a console window on a station in the management domain.
2. Use one of the following commands to determine the path to a destination:
   - on a Windows station—tracert
   - on a RHEL station—traceroute

   The command uses ICMP echo request messages to list the near-side interfaces that packets traverse between the source and destination stations. A near-side interface is the interface closest to the source host.
3. Use OS commands such as netstat -r and arp -a to display a list of active TCP connections, Ethernet statistics, the IP routing table, and the ports on which the station is listening.

END OF STEPS

6.25 Problem: Packet size and fragmentation issues

6.25.1 General information

Large packet sizes from the managed devices are being dropped by intermediate routers because the packets exceed the device MTU or the devices are not configured to forward fragmented packets, causing resynchronizations to fail. The managed devices are configured to send SNMP packets of up to 9216 bytes. The NFM-P can accept such large SNMP packets.

However, the typical L2 or L3 interface MTU on an NFM-P-managed device is likely configured to transmit smaller SNMP packets, usually in the 1500-byte range. This causes packet fragmentation. In order to handle these fragmented packets, intermediate devices between the NFM-P-managed device and NFM-P must be configured to handle or forward fragmented packets. When an intermediate network device, such as a router, cannot handle or forward fragmented packets, then packets may be dropped and resynchronization may fail.

Consider the following:

- The network infrastructure that carries traffic between the NFM-P main and auxiliary servers and the managed NEs must support fragmentation and reassembly of the UDP packets for NEs that

have an SNMP PDU size greater than the MTU configured for the network path between the NE and NFM-P. The 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, and 7950 XRS require an SNMP PDU size of 9216 bytes and fragmentation support in the network path between the NFM-P and the NE.

- Ensure that the CPM filters on managed devices are configured to accept fragmented packets, and that this filter policy is configured on each server in a redundant NFM-P deployment.
- Ensure that devices located between the managed devices, such as the 7750 SR, and the NFM-P can handle an MTU size of 9216 bytes, can fragment large SNMP packets, or can forward fragmented L2 or L3 packets.
- Verify the MTU packet sizes for all LAN devices.
- Verify that large packets can travel from the managed devices to the NFM-P by using CLI to ping the IP address of the NFM-P server, with a large packet.
- Ensure that the firewalls between the managed devices and the NFM-P server are configured to allow traceroute and ping packets.

6.25.2 Steps

1

Log in to the 7750 SR or another NFM-P-managed device.

2

Run the traceroute command:

> traceroute *SAM_server_IP_address* ↵

A list of hops and IP addresses appears.

3

Ping the first hop in the route from the managed device to the NFM-P server:

> ping *intermediate_device_IP_address* size 9216 ↵

A successful response indicates that the intermediate device supports large SNMP packets or packet fragmentation.

4

Repeat for all other hops until a ping fails or until a message indicates that there is an MTU mismatch. A failed ping indicates that the intermediate device does not support large SNMP packets or packet fragmentation.

5

Check the configuration of the intermediate device, and configure fragmentation or enable a larger MTU size.

END OF STEPS

Troubleshooting using NFM-P client GUI warning messages

6.26 Client GUI warning message overview

6.26.1 Warning message scenarios

Warning messages in the NFM-P client GUI provide an error recovery mechanism to inform you when:

- information has been entered incorrectly
- additional information is required
- the operation you are attempting cannot be completed
- a change to a configuration sub-form is not committed until the parent form is committed
- an operation that may result in service disruption is requested
- a configuration form for an object is open that can potentially conflict with a previously opened form

When an error condition is encountered that the NFM-P client has not anticipated, a Problems Encountered form is displayed. See 6.28 “Overview” (p. 366) for more information.

You can use the client GUI to suppress warning messages within containing windows. See the *NSP NFM-P Classic Management User Guide* for more information.

6.26.2 Incorrect data entry

When incorrect information is entered for a parameter, a warning message that describes the error is displayed. For example, when you configure a password for a site user, the value entered for the Password parameter and the Confirm Password parameter must match. If they do not match, a warning message is displayed.

6.26.3 Additional information required

When the value selected for a parameter has a condition that requires another parameter to be configured, a warning message indicates the missing information that is required. For example, when you configure a new or existing user with MD5 or SHA as the value for the Authentication Protocol parameter, a password must be configured. If you do not configure a password, a warning message is displayed.

The warning message indicates the information that is required. In this case, click OK to close the dialog box, and configure the New Authentication Password and Confirm New Auth Password parameters.

6.26.4 Unable to complete requested action

Warning messages are used to indicate that a specific action cannot be completed. These warnings may occur when you try to create a new object or modify an existing object that results in an unsupported configuration. For example, the message “Can't bind LSP to a non-mpls service tunnel“ indicates that you cannot bind an LSP to a service tunnel that is not configured with the MPLS protocol.

These errors can be difficult to resolve and may require that you retrace your steps to determine the cause of the warning. Check the documentation to ensure that you are following procedures correctly.

6.26.5 Commitment of changes from a form and its sub-forms

From a configuration form, you can open sub-forms that require completion before you continue with the parent form. For example, when you create a VLL service, the Create Service Site form opens during one of the configuration steps. After you configure parameters in this sub-form and click on the Finish button, a warning message is displayed.

Changes entered in the sub-form are not committed until you click OK or Apply on the parent form. When you click OK or Apply on the parent form, a final confirmation is displayed.

When you click Yes for the last confirmation, the changes to the parent or sub-forms are committed.

6.26.6 Service disruption warning

A service disruption dialog box is displayed when you perform an action that may be service-affecting. For example, if you attempt to shut down a daughter card, a warning message is displayed.

As indicated by the warning message, the action you are about to perform may cause a disruption to customer service because of a potential dependency that another object or service has on the current object. Click View Dependencies to indicate the number of services that may be affected by the action.

Verify that the requested action is appropriate. Click on the checkbox beside the statement “I understand the implications of this action” to continue with the action.

6.26.7 Duplicate configuration form conflicts

There are multiple ways to access a configuration form for the same object. For example, you can view the configuration form for a port by choosing Manage→Equipment, or you can access the port by clicking on the port object in the expanded navigation tree. When you try to perform both accesses, a warning message is displayed.

When this warning message is displayed, another form is open for the same object. When two forms are open concurrently for the same object, there may be unexpected results because changes committed from one form are not reflected in the other form.

6.27 To respond to a GUI warning message

6.27.1 Steps

1

Perform an action.

A warning message dialog box opens. For example, when you configure a site password policy, at least one authentication order must be specified as the default in order to configure the authentication order parameters. If at least one authentication order is not configured, a warning message is displayed.

2

After you read the warning message, click OK. The warning message dialog box closes.

3

Correct the problem based on the information provided.

4

If you cannot correct the problem and continue to get the same warning message:

a. Check the documentation to ensure that you are following the steps correctly.

b. Verify that you are trying to perform an action that is supported.

c. Review the general troubleshooting information in 1.2.4 “Checklist for identifying problems” (p. 16) .

d. If you cannot resolve the problem, collect the logs identified in 4.2 “To collect NFM-P log files” (p. 44) before you contact your technical support representative.

END OF STEPS

Troubleshooting with Problems Encountered forms

6.28 Overview

6.28.1 The Problems Encountered form

The Problems Encountered form reports error conditions on the client software for which there are no associated warning messages or when the client software cannot identify the problem.

Table 6-7 Problems Encountered form field descriptions

Field name	Description
Class	Specifies the object type that is the source of the problem
Operation	Specifies the type of operation that was attempted when the problem occurred.
Affected Object	Specifies the name of the affected object. Typically, if a Problems Encountered form appears when you are trying to create a object, this field contains N/A because the object has not been created.
Description	Specifies a short description of the problem, which may help you determine the cause of the problem and how to correct the problem. For additional information, click on the Properties button. The information may not be enough for you to correct the problem. The information can be used by your technical support representative to help resolve the problem.

6.29 To view additional problem information

6.29.1 Steps

1

Choose an entry in the Problems Encountered form and click Properties.

2

Try to correct the problem based on the information provided. If you cannot correct the problem, complete the procedure and perform 6.30 “To collect problem information for technical support” (p. 367) .

3

Close the details form.

4

If there is more than one problem, repeat Step 1 to Step 3 .

5

Close the form.

END OF STEPS

6.30 To collect problem information for technical support

6.30.1 Purpose

The following procedure describes what to do before you contact your technical support representative when you cannot resolve a problem on the Problems Encountered form.

6.30.2 Steps

1

Review the problem information in the Problems Encountered form, as described in 6.29 “To view additional problem information” (p. 366) .

2

Record the actions performed up to the point when the Problems Encountered form appeared. For example, if you were trying to create a VLL service, record the details about the service that you were trying to create.

3

Record the appropriate problem information, as described in Chapter 1, “NSP troubleshooting overview” .

4

Collect logs for your support representative, as described in 4.2 “To collect NFM-P log files” (p. 44) .

END OF STEPS

Troubleshooting using the NFM-P user activity log

6.31 User activity log overview

6.31.1 Logging user activity

The NFM-P user activity log allows an operator to view information about the actions performed by each NFM-P GUI and OSS user.

Note: An NFM-P operator with an Administrator scope of command role can view all user activity log records except records associated with LI management. Viewing LI management records requires the Lawful Intercept Management role.

You can use the User Activity form to do the following:

- List and view information about recent user activities.
- List and view information about recent user sessions and the actions performed during each session.
- Navigate directly to the object of a user action.
- View NFM-P client session information that includes connection, disconnection, and authentication failure events.
- View NFM-P server session information, that includes startup, shutdown, and access violation events.

Note: The NFM-P also raises an alarm for a security-related event such as an authentication failure or access violation.

You can navigate directly from an object properties form to a filtered list of the activities associated with the object. See the *NSP NFM-P Classic Management User Guide* for more information about the user activity log and using the User Activity form.

Note: The User Activity form and related list forms do not refresh dynamically. To view the latest log entries in a list form, you must click Search.

Each log entry has a request ID. There can be multiple log entries associated with a single request ID. For example, the creation of a discovery rule that has multiple rule elements creates one log entry for each rule element. You can use the request ID to sort and correlate the multiple log entries associated with a single client operation.

6.32 To identify the user activity for a network object

6.32.1 Steps

1

Open the User Activity form.

2

Click on the Activity tab.

3

Specify the filter criteria for the object and click Search. A list of user activity entries is displayed.

4

View the State column values for the activities associated with the object. A value of Failure or Timeout means that the action did not modify the object. A value of Success represents the successful deployment of the configuration action.

5

To view a suspect entry, such as a failed or incorrect configuration attempt, select the required entry and click Properties. The Activity form opens.

6

Use the activity information from one or more entries to determine whether a sequence of user actions is the source of the problem.

7

Close the forms.

End of steps

6.33 To identify the user activity for an NFM-P object

6.33.1 Steps

1

Open the User Activity form.

2

Click on the Activity tab.

3

Specify a Site Name of NONE as the filter criterion and click Search. A list of user activity entries is displayed.

4

Sort the entries to locate the affected NFM-P object.

5

View the State column values for the activities associated with the object. A value of Failure or Timeout means that the action did not modify the object. A value of Success means that the object modification succeeded.

6

To view an entry, select the required entry and click Properties. The Activity form opens.

7

Use the activity information from one or more entries to determine whether a sequence of user actions is the source of the problem.

8

Close the forms.

END OF STEPS

6.34 To navigate to the object of a user action

6.34.1 Steps

1

Open the User Activity form.

2

Click on the Activity tab.

3

Specify the filter criteria, if required, and click Search. A list of user activity entries is displayed.

4

Select an entry and click Properties. The Activity form opens.

5

Click View Object. The object properties form opens.

6

Close the forms.

END OF STEPS

6.35 To view the user activity records of an object

6.35.1 Steps

1

Open the required object properties form.

2

Click User Activity, or, if the button is not displayed, click More Actions and choose User Activity. The User Activity form opens and displays a filtered list of user activity records associated with the object.

3

To view an entry, select the entry and click Properties. The Activity form opens.

4

Close the forms.

END OF STEPS

6.36 To view the user activity performed during a user session

6.36.1 Steps

1

Open the User Activity form.

2

Specify the filter criteria, if required, and click Search. A list of user session entries is displayed.

3

Select an entry and click Properties. The Session form opens.

4

Click on the Activity tab.

5

Specify the filter criteria, if required, and click Search. A list of the actions performed by the user during the session is displayed.

6

To view an entry, select the entry and click Properties. The Activity form opens.

7

Close the forms.

END OF STEPS