iMaster NCE
V100R023C10
REST NBI User Guide

Issue	03
Date	2024-07-31

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

About This Document

Product Version

Product Name	Version
iMaster NCE (referred to as NCE)	V100R023C10

Purpose

This document describes the functions, architecture, technical principles, and configuration and maintenance methods of the REST NBI provided by iMaster NCE (referred to as NCE). **Table 1** includes references for frequently asked questions (FAQs) to help you better utilize this document.

Table 1 Reading guide

No.	Question	Where to Find the Answer
1	Where is the REST NBI positioned on the network?	**1.1 System Structure**
2	What functions does the REST NBI provide?	**1.2 Functions**
3	What is the general process of interconnecting the REST NBI with OSSs?	**1.4 Interconnection Process**
4	How do we interconnect the REST NBI with OSSs in practice?	Consult the related *iMaster NCE Northbound REST API Guide* about secondary development of the REST NBI. This guide provides NBI interconnection guidance and related API reference to help you develop the REST NBI.
5	How do I test connectivity between the REST NBI and OSSs?	

No.	Question	Where to Find the Answer
6	What configurations must be performed to export inventory data to a server?	**3.6.1 Configuration Policy** **3.6.3 Configuring the Export Function**
7	How can I perform secondary development on the REST NBI to meet specific requirements?	Secondary development involves a wide array of operations. This document (**1.2 Functions**) only describes the open functions provided by the system without elaborating the development methods. Consult the related *iMaster NCE Northbound REST API Guide* about secondary development of the REST NBI. This guide provides NBI interconnection guidance and related API reference to help you develop the REST NBI.

Intended Audience

This document describes the overview, configuration, and maintenance operations of the REST NBI.

This document is intended for:

- Network planning engineers
- Data configuration engineers
- Application development engineers
- Maintenance engineers

  To resolve common problems, maintenance engineers must be able to perform:

  - Basic operations on EulerOS
  - Routine NBI maintenance operations, such as configuring, enabling, and disabling NBIs

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.

Symbol	Description
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. A maximum of all or none can be selected.

GUI Conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, windows, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Change History

Issue	Date	Description
03	2024-07-31	This issue is the third official release, which incorporates the following changes: • **8.1 How Do I Customize the REST NBI?**: Changed the default value of **Number of iterators** to **200** at **Table 8-1**.
02	2024-03-31	This issue is the second official release, which incorporates the following changes: • **8.2 How Do I Enable the Domain-based Function for New Users?**: Added a constraint —"The domain-based function can be used only when **Scenario name** is **COMMON** (default value)."—to Step 2.
01	2023-12-30	This issue is the first official release. Compared with V100R023C00, it incorporates the following changes: • **8.8 How Do I Configure Fingerprint Authentication for the SFTP Server?**: Added fingerprint survival configurations.

Contents

1 Overview

REST NBIs provide the inventory text export capability based on FTP or SFTP to help you quickly synchronize network-wide resources, reduce the interaction process and synchronization time, and improve the reliability and stability of network-wide resource synchronization. They provide alarm and notification reporting capabilities based on WebSocket or Server-Sent Events (SSE), helping you obtain reported alarms in real time. They also provide REST inventory query, alarm clearance, acknowledgment, and unacknowledgement capabilities, helping you quickly query and handle alarms for a specific resource.

1.8 Security Capabilities
NCE ensures secure interconnection of the REST NBI through token authentication, user authentication, and HTTPS.

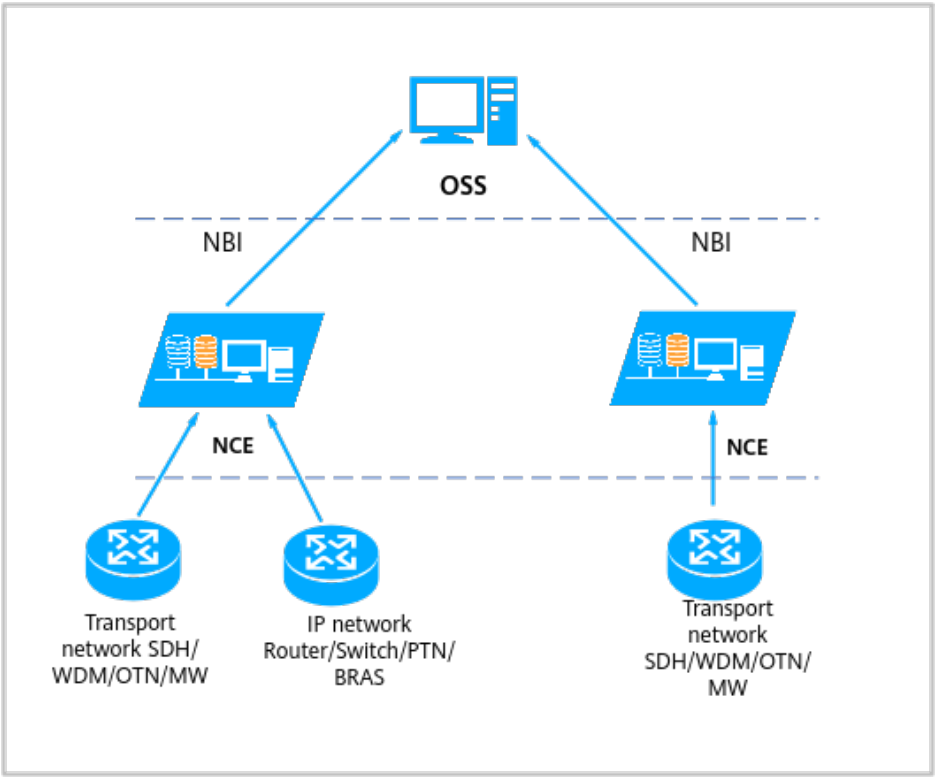
1.1 System Structure

This section describes the system structure of the REST NBI.

Network Position

Figure 1-1 shows the position of the REST NBI on the network.

Figure 1-1 Position of the REST NBI on the network



Software Architecture

Figure 1-2 shows the architecture of the REST NBI.

Figure 1-2 Software architecture

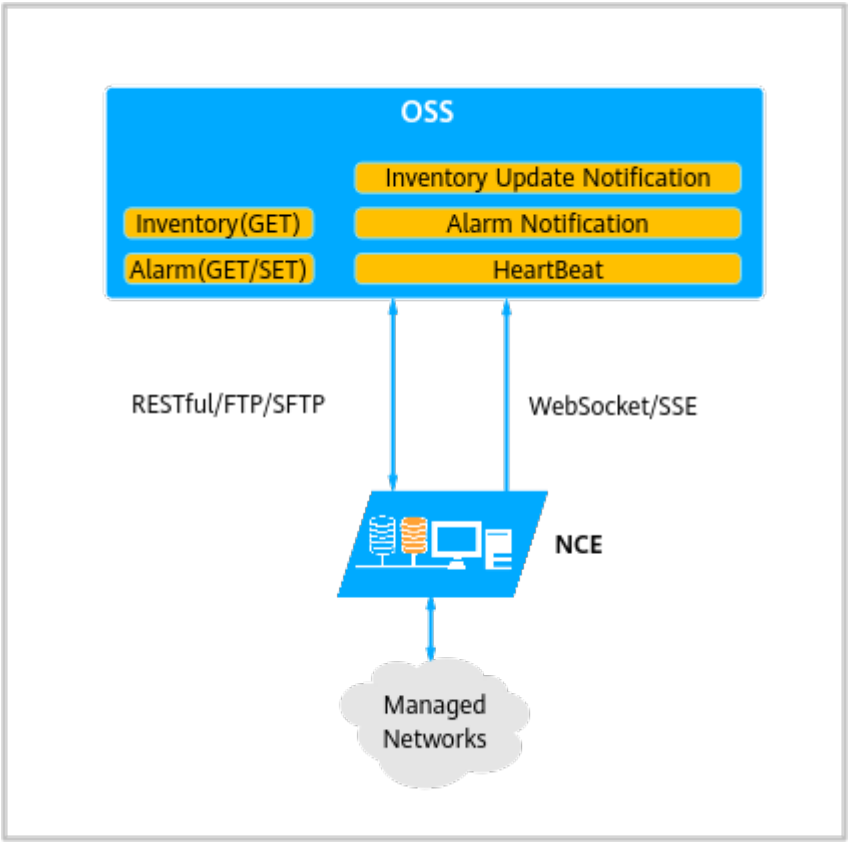


Table 1-1 REST NBI components

Component	Description
NCE	NCE server used to manage networks and provide the REST NBI.
OSS	OSS that performs operations on networks through the REST NBI provided by NCE.

1.2 Functions

The REST NBI provides the inventory, alarm, and notification functions.

- Inventory: network-wide inventory text export, resource-based batch query, and single record query
- Alarm: alarm reporting, query, filtering, acknowledgment, and additional information update
- Notification: reporting of incidents and resource changes

Table 1-2 and Table 1-3 describe the functions provided by the REST NBI.

NOTE

If you need to collect network-wide inventory data, it is advisable to export the data through the inventory text interface.

Table 1-2 Inventory functions of the REST NBI

NBI Type	Function	Applicable Domain
Query customer information	• Query details about all customers • Query details about one customer	All
Export inventory data	• Create inventory export tasks for one or more types of resources at the same time • Create incremental inventory export tasks for one or more types of resources in a particular period • Query the status of inventory export tasks • Download the exported inventory files	All
Query equipment protection groups	• Query details about all equipment protection groups • Query details about one equipment protection group	Transport
Query ports	• Query details about all ports • Query details about one port • Notify OSSs of port creation, deletion, or attribute changes	All
Query optical NEs	• Query details about all optical NEs • Query details about one optical NE	Transport
Query NEs	• Query details about all NEs • Query details about one NE • Notify OSSs of NE creation, deletion, or attribute changes	All
Query equipment rooms	• Query details about all equipment rooms • Query details about one equipment room	All
Query racks	• Query details about all racks • Query details about one rack	All

NBI Type	Function	Applicable Domain
Query chassis	• Query details about all chassis • Query details about one chassis • Notify OSSs of chassis creation, deletion, or attribute changes	All
Query boards	• Query details about all boards • Query details about one board • Notify OSSs of board creation, deletion, or attribute changes	All
Query slots	• Query details about all slots • Query details about one slot	All
Query links	• Query details about all links • Query details about one link • Notify OSSs of link creation, deletion, or attribute changes	All
Query IGP links	• Query details about all IGP links • Query details about one IGP link • Notify OSSs of IGP link creation, deletion, or attribute changes	IP
Query TE links	• Query details about all TE links • Query details about one TE link • Notify OSSs of TE link creation, deletion, or attribute changes	Super
Query topology information	• Query the topology information of all subnets or the subnets of NEs • Query the topology information of one subnet or the subnet of one NE	All
Query IGPs	• Query details about all IGPs • Query details about one IGP	IP
Query ONUs	• Query details about all ONUs • Query details about one ONU • Notify OSSs of ONU creation, deletion, or attribute changes	Access
Query slices	• Query details about all slices • Query details about one slice • Notify OSSs of slice creation, deletion, or attribute changes	IP

NBI Type	Function	Applicable Domain
Query signal types	Query the signal types supported by ports on multiple NEs	Transport
Query port availability	Query whether ports are occupied	Transport
Query SRLGs	• Query details about all SRLGs • Query details about one SRLG	All
Query system information	Query NCE system information, such as the ID, system name, software version, IP address, and license	All
Query transceivers	• Query details about all transceivers • Query details about one transceiver	All
Query IP fabrics	• Query details about all IP fabrics • Query details about one IP fabric • Notify OSSs of IP fabric creation or deletion	IP
Query lldp-neighbor	• Query details about all lldp-neighbor • Query details about one lldp-neighbor	Transport
Query OTN Protection Groups	• Query details about all OTN Protection Groups • Query details about one OTN Protection Groups	Transport
Query L2VPN and L3VPN VE groups	• Query details about all L2VPN and L3VPN VE groups • Query details about one L2VPN or L3VPN VE group • Notify OSSs of the creation, deletion, or attribute changes of L2VPN and L3VPN VE groups	IP
Query OTN trails	• Query details about all OTN trails • Query details about one OTN trail	Transport
Query the client or server trail of an OTN trail	Query the client or server trail of an OTN trail	Transport
Query the relationships between links and OTS trails	Query the OTS trails carried by a link or the links carrying an OTS trail	Transport

NBI Type	Function	Applicable Domain
Query VLANs	• Query details about all VLANs • Query details about one VLAN	Access
Query service ports	• Query details about all service ports • Query details about one service port	Access
Query the routing information of an OTN trail	Query the routing information of an OTN trail	Transport
Query VRF	• Query details about all VRF • Query details about one VRF	IP
Report forwarding domain notifications	Notify OSSs of forwarding domain creation, deletion, or attribute changes	Super
Report network control domain notifications	Notify OSSs of the creation, deletion, or attribute changes of network control domains	Super
Report IETF network notifications	Notify OSSs of IETF network creation, deletion, or attribute changes	Super

Table 1-3 Incident and alarm functions of the REST NBI

NBI Type	Function	Applicable Domain
Query incidents	• Query incidents based on specific criteria • Query the alarms associated with an incident • Notify OSSs of incident generation, deletion, or attribute changes	Transport and IP
Report alarm events	Report alarm events through SSE or WebSocket	All
Query alarms	• Query static alarm information • Query active alarms and historical alarms • Query statistics on the alarms reported from NCE • Query the alarms masked by NCE or the NBI • Query all the active alarms associated with a service	All

NBI Type	Function	Applicable Domain
Filter alarms	Filter alarms by time, ID, severity, SN, and more	All
Acknowledge alarms	Acknowledge or unacknowledge alarms	All
Update the additional information of alarms	Update the additional information of alarms	All

1.3 Technical Principles

REST APIs use the microservice architecture and REST technologies. The microservice architecture is a new technique of deploying applications and services on the cloud. It provides capabilities through lightweight web services, defines services and data structures through Yet Another Markup Language (YAML) and JavaScript Object Notation (JSON), uses protocols such as HTTPS, SSE, and WebSocket to transmit data, and uses the REST style to manage network resources. This section describes the fundamentals of REST APIs by describing the features and typical communication scenarios of REST APIs.

Related Technologies

The following description helps you understand the technologies and concepts involved in this chapter.

- HTTP(S)

  Hypertext Transfer Protocol (HTTP) is a communication protocol used to transmit information on the World Wide Web. HTTP is a request/response protocol between the client and server. A client that proposes an HTTP request (such as web browser, spider, or other terminal user tools) is called a user agent. The response server (saving or creating resources, such as HTML files and images) is called the original server.
- WebSocket

  WebSocket is a new network protocol based on TCP. It implements full-duplex communication between the browser and server. It allows the server to actively send information to the client. The server and client use HTTP to set up a TCP connection through a three-way handshake, and transmit and receive data frames at the TCP layer. REST APIs proactively send notifications and alarms to customers through WebSocket.
- SSE

  Similar to WebSocket, SSE is a protocol that allows the client and server to keep long connections. However, an SSE channel is a unidirectional channel and allows only the server to push messages to the client. In essence, the server declares that the data to be sent is flow information to the client, and then pushes the message to the client.

- RESTful

  Representational State Transfer (REST) is a software architectural style that defines a set of constraints to be used for creating web services. An architecture that conforms to the REST architectural style is called a RESTful architecture. The RESTful architecture is a resource-oriented architecture where resources are identified by their uniform resource locators (URLs). Resources are the core of the REST system, and all designs center on resources.

- JSON

  JavaScript Object Notation (JSON) is a lightweight data exchange format. It was derived from the ECMAScript Programming Language Standard (JavaScript specification developed by the European Computer Association) and uses a text format completely independent of the programming language to store and represent data. The simple and clear hierarchy makes JSON an ideal data exchange language. It is easy to read and write and can be easily parsed and generated by machines, effectively improving network transmission efficiency.

- YAML

  YAML Ain't Markup Language (YAML) is a markup language similar to XML and JSON. It focuses on data instead of language markup. Therefore, YAML is simple in definition and is called "a human-readable data serialization language".

Using YAML to Define Alarm Services and Data Structures

- The YAML text defines service URLs and request methods (such as POST, GET, PUT, and DELETE).
- It provides a complete description of the alarm data structure and supports free extension.
- It describes how to transmit data through HTTP or HTTPS.

Using JSON Messages for Communication

- JSON is independent of programming languages and protocols and can transmit information between two systems.
- The JSON data can be transmitted through HTTP or HTTPS.

Using HTTP or HTTPS as the Main Protocol to Transmit Interface Requests and Responses

- The development costs of HTTP or HTTPS on the client and server sides are lower than those of other transport protocols.
- HTTP or HTTPS is mature and supported by most systems.
- Generally, a firewall does not block HTTP or HTTPS packets.
- HTTPS packets can be transmitted in encrypted mode.

Using WebSocket or SSE as the Notification Bus

- Different notification topics (such as inventory and alarm) can be subscribed to or unsubscribed from.

One or multiple themes can be subscribed to independently.

- One-to-many notification sending is allowed.

  A theme can be subscribed to by multiple users. In other words, notifications can be sent to multiple parties at the same time.

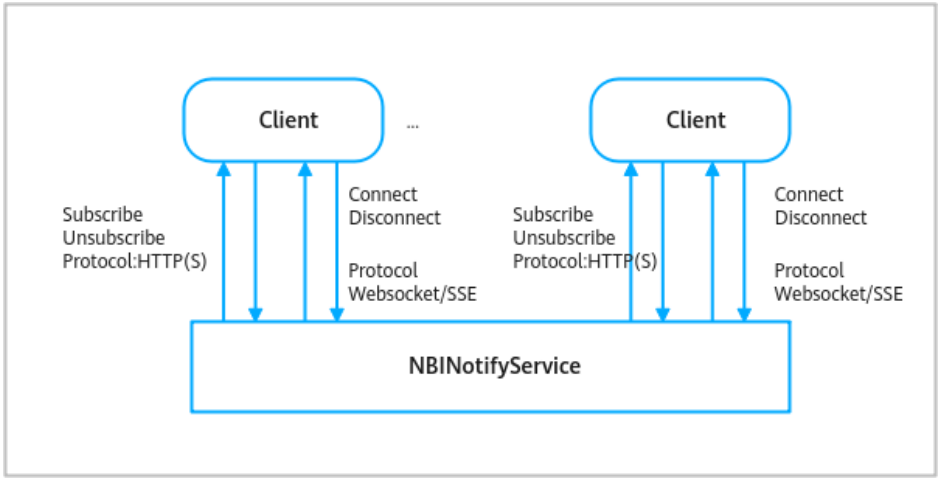
- Notification persistency is supported.

  Notification persistence means that the message middleware can store notification information on the physical medium. If an OSS goes offline due to a fault after it subscribes to a notification theme, the OSS can receive notifications after the fault is rectified.

- Filter criteria can be flexibly set.

  Filter criteria can be set during notification subscription. Currently, only alarms support filtering. After the filter criteria are set, only notifications meeting the filter criteria will be sent to subscribers.

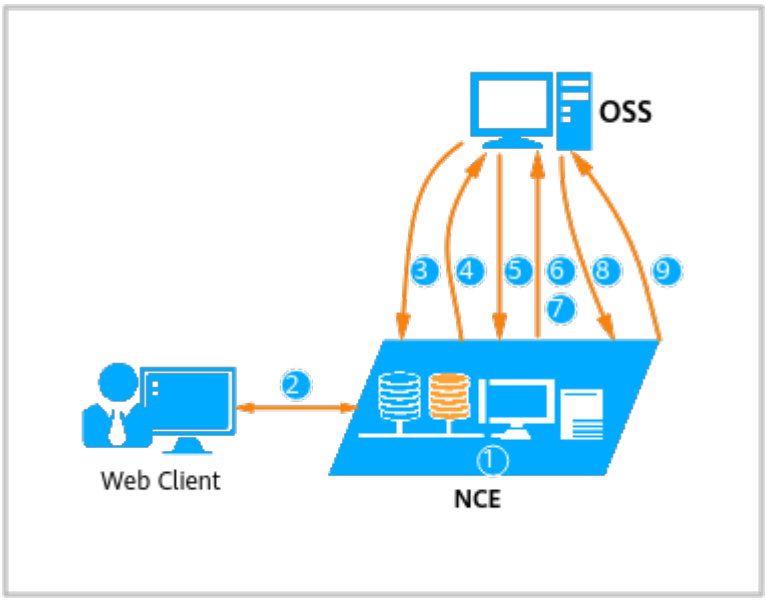
Figure 1-3 Schematic diagram of notification



1.4 Interconnection Process

Figure 1-4 shows the interconnection process of the REST NBI.

Figure 1-4 REST NBI interconnection process



Step	Description
1	Start the northbound REST inventory service and alarm & notification service.
2	Log in to the NCE O&M plane, create a northbound user, and configure the corresponding operation permissions.
3	The OSS calls NCE's authentication interface to initiate third-party user authentication with NCE.
4	NCE returns the token information required for accessing the application interface.
5	The OSS subscribes to notifications and alarms and establishes a WebSocket or SSE connection.
6	When the inventory resources of NCE change, NCE reports a resource change notification to the OSS.
7	When an alarm is generated on NCE, NCE reports the alarm to the OSS.
8	The OSS sends REST requests, such as inventory query, inventory text export, alarm query, alarm acknowledgment, and alarm clearance, to NCE.
9	NCE returns a response message through its northbound interface.

- Scenario 1: system startup

  Start the northbound REST inventory service and alarm & notification service.
- Scenario 2: notification and alarm subscription and reporting

a. The OSS uses a REST NBI to subscribe to notifications and alarms from NBINotifyService.

b. The OSS accesses NBINotifyService through SSE or WebSocket. NBINotifyService pushes notifications and alarms to the OSS.

- Scenario 3: inventory text export

  a. The OSS calls the third-party login authentication interface. NCE returns the token required for communication between the OSS and NCE. All subsequent interface calling requests must include this token in their headers.

  b. The OSS calls the inventory export interface and sets the required resource type and model version number in the delivered parameters, such as the NE, LTP, and link parameters. NCE returns the task ID of the export task.

  c. The OSS calls the northbound inventory task status query interface of NCE to obtain the task status based on the task ID. After the task is successfully completed, NCE returns the list of inventory files to be downloaded in the northbound response.

  d. The OSS calls the inventory file download interface to download the inventory files based on the task ID and inventory file list.

- Scenario 4: inventory query

  a. The OSS calls the third-party login authentication interface. NCE returns the token required for communication between the OSS and NCE. All subsequent interface calling requests must include this token in their headers.

  b. The OSS calls an inventory query interface, for example, the NE query interface. If a single resource is queried, the query is performed once. If the query is performed in batches, for example, all NEs are queried, pagination is allowed.

  c. In a batch query scenario, if **is-truncated** is **true** in the header of an NCE response, the next page is followed. In this case, the **next-page** attribute in the header provides the URL for obtaining the next page. The OSS can continue to obtain the next page data based on the URL until **is-truncated** changes to **false**, which means that all data has been queried.

1.5 Technical Specifications

This section describes the performance specifications of REST NBIs for reference during interconnection with an OSS.

Table 1-4 shows the performance specifications of REST NBIs.

Table 1-4 Performance indicators of the REST NBI

Indicator	Specifications
Request response timeout interval	5 minutes

Indicator	Specifications
Request packet size limit	2 MB
Response packet size limit	10 MB
Notification reporting capability	≤ 500 per second
Notification and alarm reporting delay	< 10 seconds
Number of notification (WebSocket&SSE) connections	≤ 100
Alarm reporting capability	Continuous reporting: ≤ 500 alarms per second; peak: 1000 alarms per second (without loss in 15 seconds) **NOTE** If 500 alarms are reported per second, none of them will be lost. However, if 1000 alarms are reported per second, for the first 15 seconds there will be no loss of alarms. From the 16th second, some alarms may be lost. Persistence: When the number of persistent data (alarm notifications) reaches 500,000 or the persistence duration reaches 7 days, data will be wrapped.

1.6 Standards and Protocols Compliance

NCE complies with IETF standards. The upper-layer integrated NMS or OSS can manage Huawei transport, IP, and access devices and their alarms in a centralized manner through REST NBIs.

Service Standards Compliance

Table 1-5 Service standards

IETF Standard	Version	Description
RFC8632	--	--

Technical Standards Compliance

Table 1-6 Technical standards

Standard	Version
Websocket	RFC 6455
YAML	2.0
HTTP (S)	1.1
SSE	1.1

1.7 Devices Supported

This section describes the types of devices that can be managed through the REST NBI.

Transport devices include MSTP, WDM, OTN, RTN, PTN (V5), VRP, and so on. IP devices include PTN (V8) series, NE (V8) series, CX (V5) series, ATN (V5) series, BRAS (V5) series, and so on. Access devices include OLTs, MxUs, and DSLAMs. Different types of devices support different attributes in the model. For details, see *NBI Inventory Attribute Support Summary* in the related **iMaster NCE REST NBI Documents** folder.

1.8 Security Capabilities

NCE ensures secure interconnection of the REST NBI through token authentication, user authentication, and HTTPS.

Authentication Modes

NCE supports three authentication modes: token authentication, username/password authentication, and basic authentication. Token authentication is recommended.

Authentication Mode	Request Header	Description
Token authentication (recommended)	X-Auth-Token	Token used to authenticate APIs. This parameter is not required for the API used to obtain the token. Token authentication is available on the O&M plane.

Authentication Mode	Request Header	Description
Username/password authentication (not recommended)	• username • password	The username and password parameters are used to authenticate APIs. The username and password parameters are valid only when they are used at the same time. **NOTE** This authentication mode is provided only for compatibility with earlier versions. It may involve security risks related to password transmission. Therefore, do not use it to protect sensitive or valuable information.
Basic authentication (not recommended)	Authorization	Base64-encoded **Basic** *username:password*. Basic authentication is available on the O&M plane. **NOTE** This authentication mode is provided only for compatibility with earlier versions. It may involve security risks related to password transmission. Therefore, do not use it to protect sensitive or valuable information.

User Authentication

The following measures are taken to ensure that appropriate permissions are assigned to northbound interconnection users:

- Create a dedicated third-party user for interconnecting with REST NBIs.

  The third-party user is used only for third-party system access. It cannot log in to NCE clients.
- Configure the default role **NBI User Group**.

  The default role **NBI User Group** is assigned to the third-party user. As shown in **Table 1-7**, **NBI User Group** has permission to call all REST NBIs. You can add one or more roles to the third-party user based on service needs. For example, NCE-Super has planned multiple service-specific roles in addition to the default role **NBI User Group**. (See **Table 1-8**.) This helps control user permissions by service.

  Table 1-7 Mapping between roles and permissions

Role Name	Category	Permission	Description
NBI User Group	API Management	GET	Permission for calling GET APIs.
		POST	Permission for calling POST APIs.

Role Name	Category	Permission	Description
		PUT	Permission for calling PUT APIs.
		DELETE	Permission for calling DELETE APIs.
		PATCH	Permission for calling PATCH APIs.

Table 1-8 Mapping between NCE-Super services, roles, and permissions

Service	Role Name (Recommended)	Permission
WebSocketGW Service	websocket_api	Subscribe to Event
UnderlayVPNAPIService	underlayvpn_api	• Create IP WAN Service • Delete IP WAN Service • Modify IP WAN Service • Query IP WAN Service
VPNDesignAPI Service	vpndesign_api	• Create VPN Design • Delete VPN Design • Modify VPN Design • Query VPN Design
BaseResAPIService	baseresource_api	• Configure Basic Resources • Manage Basic Resources • Query Basic Resources • Manage Recycle Bin

HTTPS

By default, RESTful APIs use HTTPS v1.1 for transmission. HTTPS v1.1 is more secure than HTTP.

NOTICE

HTTP is insecure and not recommended.

2 Checking the License

NCE controls the functions and available resources of a REST NBI by a license. Before using a REST NBI, ensure that you have obtained its license and that the REST NBI configurations in the license meet requirements.

Prerequisites

- NCE has been installed.
- The NCE license has been loaded.
- NCE has NE management licenses and functions properly.

Context

NOTICE

- An REST NBI can be used when NCE has a northbound license and the license consumption does not exceed the threshold.
- When NCE has a northbound license but the consumption reaches the alarm threshold, the system reports a northbound license threshold alarm. Open the System Settings app and choose **System Settings** > **License Management** from the main menu, the alarm is reported successfully only when **Sending Alarms** is set to **Yes** in **License Information** on the NCE O&M plane.
- When the northbound license consumption of NCE exceeds the threshold, the grace period is not supported. An error is reported when the REST NBI is invoked. The device alarms of the REST are stopped, and the notifications and system-level alarms (non-device alarms) can be reported.
- In the NCE-Super separated deployment scenario, the REST NBI of the Super is not under license control.
- In NCE capacity expansion, NBI licenses need to be expanded.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the System Settings app and choose **System Settings** > **License Management** from the main menu.

Step 4 On the **License Information** page, click the **Sales Information Items** tab of the current product.

Step 5 On the **Sales Information Items** tab page, check whether **Sales Item** contains the license sales item corresponding to the NBI. If the results can be found, NCE has the authority to use the REST NBI. For the relations between the sales items in the License file and the REST sale items, see **Table 2-1** and **Table 2-2**.

Table 2-1 Carriers License sale items

License Sale Item	Abbreviation	Value	Domain
NCE-FAN Unified Northbound API Suite (per Equivalence), Perpetual License	NSSS0FANAPI1	0–20000	NCE-FAN
NCE-FAN Unified Northbound API Suite (per 50 equivalent NEs), Perpetual License	NSSSCOMMON15	0–20000	NCE-FAN
Value-added open APIs (Includes REST, Kafka, etc.),per 1 equivalent NEs,Perpetual License	NSSSIPNBIAPIPER1	0–20000	NCE-IP
Value-added open APIs (Includes REST, Kafka, etc.), per 50 equivalent NEs, Perpetual License	NSSSTRANIPNBIPL02	0–20000	NCE-IP
NCE-T Value-added open APIs (Includes REST, Kafka, etc.),per 50 equivalent NEs,Perpetual License	NSSSTRANOTNNBIPL02	0–20000	NCE-T
NCE-T Value-added open APIs (Includes REST, Kafka, etc.),per 1 equivalent NEs,Perpetual License	NSSSTRANOTNNBIPLL02	0–20000	NCE-T
NCE-RTN Value-added open APIs (Includes REST, Kafka, etc.),per 50 equivalent NEs,Perpetual License	NSSSTRANMWNBIPL02	0–20000	NCE-T

License Sale Item	Abbreviation	Value	Domain
NCE-RTN Value-added open APIs (Includes REST, Kafka, etc.),per equivalent NEs,Perpetual License	NCEMICROWAVE29	0–20000	NCE-T

Table 2-2 Enterprises License sale items

License Sale Item	Abbreviation	Value	Domain
NCE-FAN Unified Northbound API Suite (per Equivalence), Perpetual License	NSSSEFANAPI1	0–20000	NCE-FAN
Access Network Unified Northbound API Suite (per 5 equivalent NEs), Perpetual License	NSSSANUNAS04	0–20000	NCE-FAN
Access Network Unified Northbound API Suite (per 20 equivalent NEs), Perpetual License	NSSSANUNAS01	0–20000	NCE-FAN
NCE-FAN Unified Northbound API Suite (per 50 equivalent NEs), Perpetual License	NSSSENUNAS01	0–20000	NCE-FAN
Value-added open APIs (Includes REST, Kafka, etc.), per 5 equivalent NEs, Perpetual License	NSSSTENPNBIPLS08	0–20000	NCE-IP
Value-added open APIs (Includes REST, Kafka, etc.),per 5 equivalent NEs,Perpetual License	NSSSTRANIPNBIPL72P5Eq	0–20000	NCE-IP
Value-added open APIs (Includes REST, Kafka, etc.), per 20 equivalent NEs, Perpetual License	NSSSTRANSENPNBIPL08	0–20000	NCE-IP
Value-added open APIs (Includes REST, Kafka, etc.), per 50 equivalent NEs, Perpetual License	NSSSTRANIPNBIPL72	0–20000	NCE-IP
Value-added open APIs (Includes REST, Kafka, etc.), per 1 equivalent NE, Perpetual License	NSSSNORTH102	0–20000	NCE-T

License Sale Item	Abbreviation	Value	Domain
NCE-T Value-added open APIs (Includes REST, Kafka, etc.),per 5 equivalent NEs,Perpetual License	NSSSTRANOTNNORTHL02	0–20000	NCE-T
Transport domain Value-added open APIs (Includes REST, Kafka, etc.),per 50 equivalent NEs,Perpetual License	NCEENTNORTH004	0–20000	NCE-T
NCE-RTN Value-added open APIs (Includes REST, Kafka, etc.), per 5 equivalent NEs, Perpetual License	NSSSTRANMWNLITEL04	0–20000	NCE-T

Step 6 If the license does not support the functions or resources needed, contact Huawei engineers to apply for the license. For the license introduction and information on how to apply for a license, see *iMaster NCE License Instructions* of the corresponding version.

----End

3 Configuring the REST NBI

Prerequisites

The REST NBI services are running.

- In the single-site scenario, the REST NBI processes are in the manual startup mode and stopped by default. To use the REST NBI, start the REST NBI processes and change their startup modes to automatic. For details, see **8.9 How Do I Change the Startup Modes of NBI Processes?**
- In other scenarios, the REST NBI processes are in the automatic startup mode and started by default, entailing no additional operations.

Configuration Instructions

Table 3-1 Configuration instructions

Operation	Mandatory	Description
3.1 Configuring the Security Certificates of APIGWService	Yes	When NCE interconnects with a third-party system, it is necessary to configure security certificate authentication to ensure successful communications between the two systems.
3.2 Setting Common Parameters	No	The REST NBI component is automatically deployed during NCE installation. You need to manually set some parameters to enable the NBI.
3.3 Configuring an IP Address Access Policy and Port	No	The default port number is 26335. If you need to change the port number, refer to this section.
3.4 Configuring a Global Traffic Control Policy	No	This operation helps protect NCE against DoS attacks and Challenge Collapsar (CC) attacks.

Operation	Mandatory	Description
3.5 Configuring the HTTP or HTTPS Protocol	No	NCE uses the HTTPS protocol by default. If you need to use the HTTP protocol, refer to this section. **NOTICE** HTTP is insecure and not recommended.
3.6 Configuring Inventory Export	No	NCE supports periodic inventory export and inventory export through APIs. If you want to export inventory data at a fixed period, follow this section to configure periodic inventory export. Otherwise, follow the related *iMaster NCE Northbound REST API Guide* to export data through APIs.
3.7 Configuring Alarm Reporting	No	NCE alarms are reported to the OSS in real time. To configure the reporting rules (for example, whether to report acknowledgment/unacknowledgement notifications or correlative alarms), refer to this section.
3.8 Configuring Incident Export	No	In coordination with real-time incident reporting, the OSS synchronizes network-wide incident information as needed during NCE fault O&M. If the intelligent incident export period is fixed, you can export data periodically by referring to this section.
3.10 Creating a REST NBI User for an OSS	No	In addition to normal work of the REST NBI and successful network communication, create a user on NCE for each OSS and assign the REST NBI permissions to it so that OSSs can access NCE through the REST NBI.
3.11 Configuring RESTful Callback	No	If the RESTful protocol is chosen to report service data, related RESTful protocol, alarm, alarm acknowledgment/ unacknowledgement, event, and notification parameters need to be set.

Precautions

Before configuring the REST NBI, familiarize yourself with the precautions and policy of the configuration, and collect required information. Modifications to certain configuration items may restart NBI services, necessitating advance application. Before configuring the REST NBI, read the following precautions:

- After NCE is installed, NBI services are started by default; therefore, you can directly configure the REST NBI.
- If NBI services are redeployed, reconfigure the REST NBI.
- When the IP address of NCE changes, reconfigure the REST NBI.
- Each NIC allows only one IP address. Do not configure multiple IP addresses for one NIC. If you need multiple IP addresses, configure multiple NICs.
- To ensure successful interconnection with the NBI, the OSS must be able to communicate with NCE. If the NCE server has multiple NICs in different network segments, select the NIC connected to the OSS and set its IP address as NCE's IP address.

3.1 Configuring the Security Certificates of APIGWService
When NCE interconnects with a third-party system, it is necessary to configure security certificate authentication to ensure secure communications between the two systems. To prevent system security risks caused by certificate expiration or private key leak, it is advisable to periodically update certificates.

3.2 Setting Common Parameters
The REST NBI is automatically deployed during NCE installation. You need to manually set some parameters to enable the NBI.

3.3 Configuring an IP Address Access Policy and Port

3.4 Configuring a Global Traffic Control Policy
After service is deployed, modify **Max. northbound OpenAPI connection requests** and **Max. northbound OpenAPI connection requests from one IP address** on NCE to protect client against DoS and Challenge Collapsar (CC) attacks.

3.5 Configuring the HTTP or HTTPS Protocol

3.6 Configuring Inventory Export
REST NBIs provide the function to export inventory data. You can configure parameters appropriately on NCE to export inventory data to a server. In addition, NCE opens inventory data query and export NBIs for call and development. For details about how to call or develop such an NBI, see *iMaster NCE Northbound REST API Guide* of the corresponding version.

3.7 Configuring Alarm Reporting

3.8 Configuring Incident Export
NBI components are automatically deployed during NCE installation. Scheduled incident export through the REST NBI, however, still needs to be manually enabled.

3.9 Obtaining Text Files
The REST NBI supports full export and incremental export of inventory resources, and export tasks can be created for one or more types of inventory resources at a time. In addition, multiple tasks can be created for text export of incident data. After a user creates an export task, only that user can query the task status and download the files generated by the task.

3.10 Creating a REST NBI User for an OSS
In addition to normal work of the REST NBI and successful network communication, create a user on NCE for each OSS and assign the REST NBI permissions to it so that OSSs can access NCE through the REST NBI.

3.1 Configuring the Security Certificates of APIGWService

When NCE interconnects with a third-party system, it is necessary to configure security certificate authentication to ensure secure communications between the two systems. To prevent system security risks caused by certificate expiration or private key leak, it is advisable to periodically update certificates.

You can update certificates in either of the following methods:

- Manually importing certificates: This involves applying for security certificates from a third-party CA and manually importing them to the NCE O&M plane. For details, see **3.1.1 Importing and Updating Security Certificates**.
- Applying for certificates online: This involves creating a certificate update task on the NCE O&M plane to apply for and update certificates online. For details, see **3.1.2 Updating Certificates Online**.

3.1.1 Importing and Updating Security Certificates

When using this method, you need to apply for security certificates from a third-party CA and manually import the certificates to the NCE O&M plane.

NOTICE

For security purposes, do not copy the temporary certificates as the security certificates of the OSS.

Applying for Security Certificates

When applying for security certificates from a third-party CA, select those in the PEM, PKCS12, JKS, or DER format. Because certificates have multiple encoding formats, you are advised to select an encoding format that matches your OSS.

Prerequisites

- The services that require certificate management have been deployed.
- You have the **Query Certificate**, **Import Certificate**, and **Delete Certificate** permissions.
- You have obtained new certificates and relevant information, such as file passwords, certificate types, and the public key file, private key file, private key password, and certificate chain of the identity certificate.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the System Settings app and choose **System Settings** > **Certificate Management** from the main menu. Then click **Administrator Certificate Management**.

Step 4 In the navigation pane, choose **Service Certificate Management**.

Step 5 Search for "APIGWService" in the service list.

Step 6 Click the **APIGWService** card displayed.

Step 7 Configure different types of certificates on their respective tab pages.

- Identity certificate
  a. On the **Identity Certificate** tab page, click **Import**.
  b. On the **Import Identity Certificate** page, set certificate parameters based on **Table 3-2**.

  NOTE

  Only one identity certificate is allowed. If an identity certificate already exists, importing a new certificate will overwrite the existing certificate. Be sure to import a correct certificate. If the identity certificate is incorrect, communications may be interrupted.

Table 3-2 Parameters for importing an identity certificate for APIGWService

Parameter	Description
Certificate alias	User-defined alias of the certificate to be imported. Setting an alias helps you distinguish and find this certificate.
Public key file	Click to upload a .pem, .der, .cer, or .crt certificate file not larger than 50 KB.
Private key file	Click to upload an encrypted *.pem certificate file not larger than 50 KB.
Private key password	Password for the certificate file. **NOTICE** ■ For security purposes, the password must be 8–64 characters long and contain at least three of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ ■ For security purposes, change the password in a timely manner, update it periodically, and keep it secure.
(Optional) Certificate chain	Click to upload a .pem or .p7b certificate file not larger than 50 KB.

Parameter	Description
(Optional) Remarks	Remarks on the certificate. Setting remarks helps you distinguish and maintain this certificate.

c. Click **Submit**.

- Trust certificate
  a. On the **Trust Certificate** tab page, click **Import**.
  b. On the **Import Trust Certificate** page, set certificate parameters based on **Table 3-3**.

Table 3-3 Parameters for importing a trust certificate for APIGWService

Parameter	Description
Certificate alias	User-defined alias of the certificate to be imported. Setting an alias helps you distinguish and find this certificate.
Certificate format	▪ PKCS12(.p12) ▪ JKS(.jks) ▪ PEM(.pem/.der/.cer/.crt) ▪ DER(.der/.cer/.crt)
Certificate file	Click to upload a certificate file in the selected format (not larger than 50 KB).
Certificate password	Password for the certificate file. This parameter appears only when **Certificate format** is **PKCS12(.p12)** or **JKS(.jks)**. **NOTICE** ▪ For security purposes, the password must be 8–64 characters long and contain at least three of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ ▪ For security purposes, change the password in a timely manner, update it periodically, and keep it secure.
(Optional) Remarks	Remarks on the certificate. Setting remarks helps you distinguish and maintain this certificate.

c. Click **Submit**.

- Certificate revocation list (CRL)
  a. On the **Certificate Revocation List** tab page, click **Import**.
  b. On the **Import Certificate Revocation List** page, set certificate parameters based on **Table 3-4**.

Table 3-4 Parameters for importing a CRL for APIGWService

Parameter	Description
Certificate alias	User-defined alias of the certificate to be imported. Setting an alias helps you distinguish and find this certificate.
Certificate file	Click to upload a *.crl certificate file not larger than 50 KB.
(Optional) Remarks	Remarks on the certificate. Setting remarks helps you distinguish and maintain this certificate.

c. Click **Submit**.

Step 8 The service automatically restarts, which takes about 1 minute. Within this period, the service is unavailable. It is advisable to perform the preceding operations in off-peak hours.

----End

Related Tasks

- See "Importing and Updating Certificates > Related Tasks" in the Information Center.
- Querying shared CRLs

  In the navigation pane, choose **Shared CRLs**. In the right pane, view **Certificate Revocation Lists**.

  NOTE

  APIGWService does not automatically restart upon CRL updates. Therefore, you need to restart APIGWService for the updates to take effect.

3.1.2 Updating Certificates Online

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the System Settings app and choose **System Settings** > **Certificate Management** from the main menu. Then click **Administrator Certificate Management**.

Step 4 In the navigation pane, choose **Online Certificate Update** > **Certificate Update Tasks**.

Step 5 Perform subsequent operations by referring to the Information Center.

----End

3.2 Setting Common Parameters

The REST NBI is automatically deployed during NCE installation. You need to manually set some parameters to enable the NBI.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 4 In the navigation pane, choose **REST NBI** > **Common Settings**. Set parameters based on **Table 3-5**.

Table 3-5 Common parameters

Parameter	Mandatory	Description	Value Range	Default Value
Time format	Yes	Time format in inventory, notifications, and alarms. **NOTE** Modifying **Time format** will trigger the message "Modifying this configuration item will affect Kafka packets. Are you sure you want to continue?" If you are sure that no adverse impact will be caused, click **OK**. Otherwise, click **Cancel**.	UTC time, Local time	UTC time
MD name	Yes	ID of NCE on the OSS. If you configure multiple sets of NCE in a network as planned, configure a unique name for each NCE. **NOTE** Modifying **MD Name** will trigger the message "Modifying this configuration item will affect Kafka packets. Are you sure you want to continue?" If you are sure that no adverse impact will be caused, click **OK**. Otherwise, click **Cancel**.	0–300 bytes	Huawei/ NCE

Parameter	Mandatory	Description	Value Range	Default Value
Scenario name	Yes	Name of the scenario. If there is no custom scenario, retain the default value **COMMON**. **NOTE** If this parameter is set to **COMMON_WITH_DN**, the **distinguished-name** field will be added to the responses of the NE, board, port, and link inventory export and query interfaces.	--	COMMON

----End

3.3 Configuring an IP Address Access Policy and Port

Configure an IP address access policy to control access to client. That is, users can access the REST NBI only through clients within the configured IP address range.

Obtain the port of client and IP address of the node where client resides, and provide them for third-party systems before interconnection.

Prerequisites

The default port of client is 26335.

Procedure

Step 1 Query the IP address.

When the REST NBI is interconnected, external connections need to be established with the IP address of the node where client resides.

NOTE

- In Manager, it is the NorthAPIAccessIP address of the NMS_Server node.
- In Manager+Controller+Analyzer without IP address convergence, it is the NorthAPIAccessIP4 address of the Common_Service node.
- In Manager+Controller+Analyzer with IP address convergence, it is the LVS-apimlb IP address of the GW node.

For details about how to find these IP addresses, see **6.1 Checking the Northbound IP Address**.

Step 2 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 3 Enter a username and password, and click **Log In**.

Step 4 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 5 (Optional) Modify the port number.

1. In the navigation pane, choose **API Gateway** > **General Configuration**.
2. In the **Port** area, modify **Listening port**.
3. Click **Apply** in the lower right corner. The configuration takes effect after the page is refreshed.

   NOTE

   To avoid conflicts, do not use port numbers between 1 and 1024.

Step 6 Configure an IP address access policy.

1. In the navigation pane, choose **API Gateway** > **Access Configuration**.
2. Click > **IP Address Access Policy**.
3. Click **Create**.
4. In the **Create IP Address Access Policy** dialog box, select an IP address type and set the start and end IP addresses.
5. Click **OK**. The configuration takes effect after the page is refreshed.

Step 7 On third-party systems, configure interconnection using the preceding port number and IP addresses.

----End

3.4 Configuring a Global Traffic Control Policy

After service is deployed, modify **Max. northbound OpenAPI connection requests** and **Max. northbound OpenAPI connection requests from one IP address** on NCE to protect client against DoS and Challenge Collapsar (CC) attacks.

Prerequisites

You have obtained the management IP addresses of all Common_Service nodes, including Common_Service_01, Common_Service_02, and Common_Service_03. The number of nodes depends on the node protection scheme and management scale. For details, see **8.3 How Do I Query the IP Address of a Node?**

Precautions

By default, NCE does not limit the connection frequency of IP addresses. You are advised to set a frequency not lower than 20 times per second.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 4 In the navigation pane, choose **API Gateway** > **Access Configuration**.

Step 5 In the **Global Traffic Control Policy** area, set the maximum number of connection requests and connection frequency.

NOTE

Max. API gateway connection requests indicates the maximum number of concurrent connections allowed to the northbound IP address. Setting **Max. API gateway connection requests** to **0** (meaning no limit) or a large value may lead to security risks. For security purposes, select a proper value within the supported range (0–6000).

Step 6 Click **Apply** in the lower right corner.

Step 7 In the **High Risk** dialog box, read the message displayed and determine whether to apply the global traffic control policy.

- If yes, select **I understand the risks and want to continue**, click **OK**, and go to **Step 8**.
- If no, click **Cancel**.

Step 8 Click **OK**.

----End

3.5 Configuring the HTTP or HTTPS Protocol

By default, the HTTPS protocol (which is recommended because it is more secure) is used to communicate with third-party systems. If you need to use HTTP, follow this section to configure the protocol.

NOTICE

HTTP is an insecure protocol and nullifies the certificate authentication function. This will pose security risks in data transmission, resulting in data leakage or tampering. Configure the protocol based on site requirements.

Prerequisites

- You have obtained the IP address of the node (Common_Service by default) where NCE O&M plane client resides.
- HTTP is required for interconnecting with third-party systems.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 4 In the navigation pane, choose **API Gateway** > **General Configuration**.

Step 5 In the **Secure Connection** area, disable **Enable HTTPS**.

Step 6 In the **Warning** dialog box, read the message displayed and determine whether to use HTTP. If yes, click **OK**.

Step 7 Click **Apply** in the lower right corner. The configuration takes effect after the page is refreshed.

----End

3.6 Configuring Inventory Export

REST NBIs provide the function to export inventory data. You can configure parameters appropriately on NCE to export inventory data to a server. In addition, NCE opens inventory data query and export NBIs for call and development. For details about how to call or develop such an NBI, see *iMaster NCE Northbound REST API Guide* of the corresponding version.

3.6.1 Configuration Policy

Before configuring the export function of the REST NBI, you need to understand the configuration policy and collect related information.

Selecting an Export Server

The export server stores inventory data for a specified period. Considering the large data volume, you are advised to select a server with sufficient storage space.

Table 3-6 Planning of the export server

Server Type	Description	Upload Directory
Local server	When specifying the local server, select the node where the northbound network communication IP address has been configured. Under this setting, the system stores inventory data on that node. For details about the northbound network communication IP address, see **6.1 Checking the Northbound IP Address**. When you need inventory data, use FileZilla to log in to the server as the **ftpuser** user and download data from the upload directory.	/hfs_public/nbi
Third-party FTP/SFTP server prepared by the customer	When selecting a third-party SFTP server, ensure that: • The server supports FTP/SFTP. • You have obtained the server username and password required for transferring files through FTP/SFTP. • The server supports the following data encryption algorithms: AES128-CTR, AES192-CTR, and AES256-CTR. • The server supports the following signature algorithms: HMAC-SHA2-512 and HMAC-SHA2-256. Under this setting, the system stores inventory data on the third-party FTP/SFTP server. When you need inventory data, use FileZilla to log in to the server and download data from the upload directory.	Depends on the site plan. Ensure that the user who logs in to the server in FTP/SFTP mode has permission to read and write the FTP/SFTP shared directory.

Configuring Inventory Data Export

Table 3-7 describes the inventory export functions provided by the REST NBI.

Table 3-7 Inventory export functions

Type	Description	Usage Scenario
Scheduled export	Once configured on the GUI, the system exports inventory data at scheduled times.	Inventory data needs to be periodically exported to a server, which will keep the data for the number of days set in **3.6.3 Configuring the Export Function**. When you need inventory data, download it from the server.
	Once configured on the GUI, the system exports incremental inventory data at scheduled times. **NOTE** Inventory data export takes a long time and consumes system resources. To ensure the "freshness" of inventory data on the server and reduce the impact of frequent full inventory data export, the system provides the function to periodically export incremental data. In incremental inventory export, only the data that is added or modified after the previous full or incremental export is exported.	Inventory data needs to be periodically updated on the storage server, so that the inventory data is always up-to-date.
Inventory export by calling an NBI	The REST NBI can be called or customized to export data.	In case that you need more than what has been provided in terms of inventory export, the REST NBI is open further development and integration. For details about how to call or customize the NBI, see *iMaster NCE Northbound REST API Guide*.

3.6.2 Collecting Export Server Parameters

Before configuring inventory export, you need to plan and collect the export server parameters to ensure that inventory data will be successfully exported to the server.

Table 3-8 lists the information to be collected.

Table 3-8 Export server parameters

No.	Parameter	Mandatory	Description
1	Exported to	Yes	Type of the server that receives inventory data. Set it to the actual plan. For details, see **Table 3-6**. If **Local server** is selected, you do not need to collect the 4th to 12th parameters.
2	Local inventory export directory	Yes	Local directory for storing inventory data.
3	Local increment export directory	Yes	Local directory for storing incremental inventory data.
4	FTP/SFTP mode	Yes	Transfer mode of inventory data. **NOTICE** SFTP is recommended, because it is more secure than FTP.
5	FTP/SFTP server IP address	Yes	IPv4 or IPv6 address of the FTP/SFTP server that receives inventory data.
6	FTP/SFTP server port	Yes	Port of the FTP/SFTP server that receives inventory data.
7	Inventory FTP/SFTP upload directory	Yes	Directory on the FTP/SFTP server for receiving inventory data.
8	Increment FTP/SFTP upload directory	Yes	Directory on the FTP/SFTP server for receiving incremental inventory data.
9	FTP/SFTP username	Yes	Name of the user who can transfer files through FTP/SFTP.

No.	Parameter	Mandatory	Description

10	Authentication mode	Yes	Authentication mode, which can be **Password** or **Public Key Authentication**.
			• If **FTP/SFTP mode** is **FTP**, **Authentication mode** can only be **Password**.
			• If **FTP/SFTP mode** is **SFTP**, **Authentication mode** can be **Password** or **Public Key Authentication**.
			NOTE
			• **Password**: The SFTP user password is required during first-time authentication. To change the password, select **Change Password**.
			• **Public Key Authentication**: An SFTP private key file needs to be uploaded for authentication. For details about how to generate a private key file, see **8.6 How Do I Generate a Private Key File?** After uploading an SFTP private key file:
			  • If the private key file is encrypted, set **Encrypt private key** to **Yes** and enter the correct file password in the **Enter the private key password** dialog box.
			  • If the private key file is not encrypted, set **Encrypt private key** to **No** and click **OK** in the **Enter the private key password** dialog box.

11	FTP/SFTP password	Yes	Password for the user who can transfer files through FTP/SFTP. **NOTICE** • The password is expected to meet the following rules: 1) Differ from the username and the reverse of the username. 2) Consist of at least eight characters. 3) Contain at least three types of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (=~@#^*-_+[{}];:./?). 4) Not be composed of repeated strings of any length, for example, aaaaaaaa, abababab, or abcdabcd. • For security purposes, change the password upon the first login, update it periodically, and keep it secure.
12	Confirm FTP/SFTP password	Yes	Confirm password.

Before configuring the export function of the REST NBI, read the following precautions:

- Configuring the inventory export function of the REST NBI may affect other NCE components and the OSS. Modifying certain configuration items (**Table 3-9**) may also depend on other NCE components. Before configuring the REST

NBI, check whether these configuration items will cause such impact and seek advance consent from customers.

- Scheduled inventory export and incremental inventory export are disabled by default, but you can enable them as needed.

Table 3-9 Key configuration items

Configuration Item	Description	Impact
Scheduled inventory export	Whether to export inventory data at scheduled times.	Inventory data will be exported at scheduled times. This function is disabled by default.
Inventory export resource range	Which resources will be exported.	By default, the recommended resource range is used. The OSS can modify the range as required, and then the NCE NBI will export inventory data according to the modified range.
Scheduled increment export	Whether to export incremental inventory data at scheduled times.	Incremental inventory data will be exported at scheduled times. This function is disabled by default.
Increment export resource range	Which resources will be exported incrementally.	By default, the recommended resource range is used. The OSS can modify the range as required, and then the NCE NBI will export inventory data according to the modified range.

3.6.3 Configuring the Export Function

Although NBI components are automatically deployed during NCE installation, you still need to manually enable and configure scheduled inventory data export.

Prerequisites

- All databases are running.
- The installation directory has more than 20 GB free space. On EulerOS, you can run the **df -hk /opt** command to check the remaining space in the **/opt** directory.

- You have obtained the values of all the involved configuration items from the OSS vendor.

Procedure

Step 1 Open a browser, enter **https://***IP address of the NCE O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

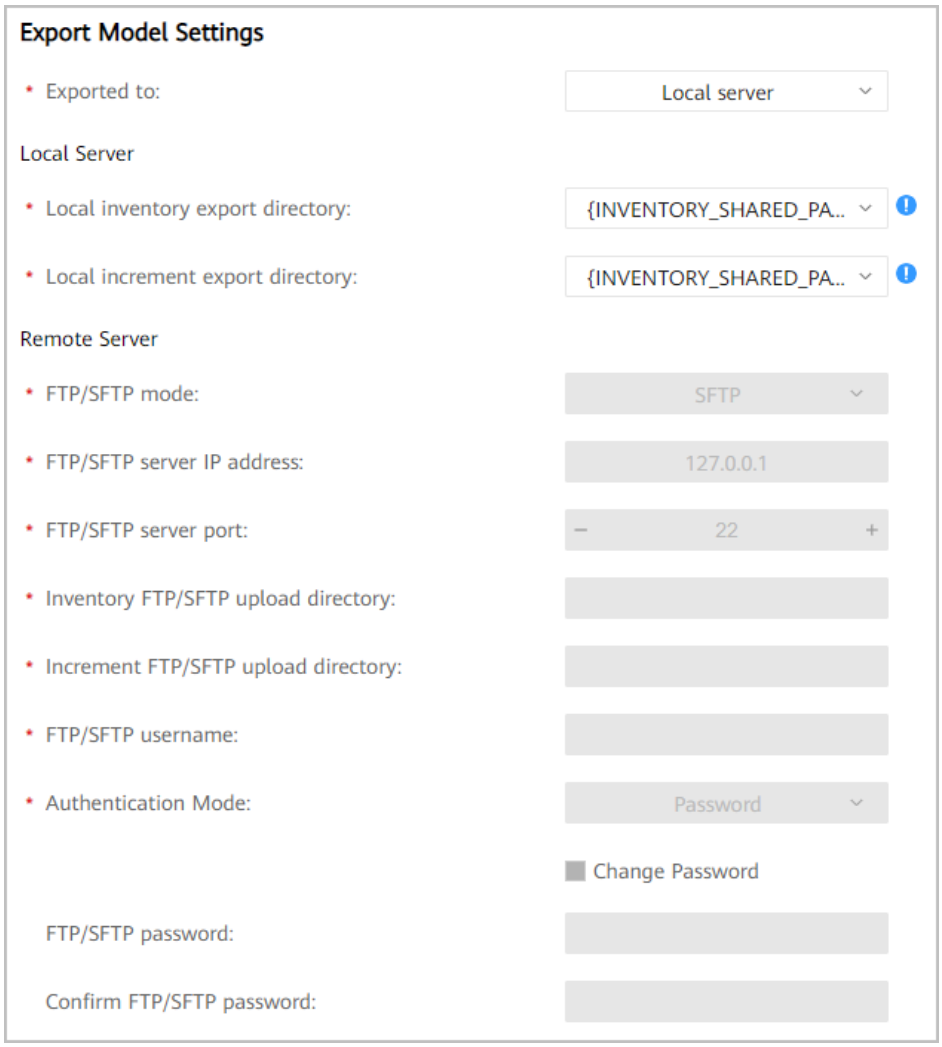
Step 3 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 4 In the navigation pane, choose **REST NBI** > **Inventory Task Settings**.

Step 5 On the **Inventory Task Settings** page, click **Create**.

Step 6 Determine whether to use a third-party server to store the exported inventory data. (By default, the system stores inventory data on the local server.)

- If yes, set parameters in the **Export Model Settings** area by referring to **Table 3-10**.



- If no, proceed to **Step 7**.

Table 3-10 Common parameters

No.	Parameter	Mandatory	Description	Example
1	Exported to	Yes	Type of the server that receives inventory data. Set it to the actual plan. – If you select **Local server**, directly start from **Step 7**. – If you select **Remote FTP server**, set the remaining parameters in this table.	Local server
2	Local inventory export directory	Yes	Local directory for storing inventory data. **NOTE** Use FileZilla to log in as **ftpuser**.	/hfs_public/nbi/inv/export
3	Local increment export directory	Yes	Local directory for storing incremental inventory data. **NOTE** Use FileZilla to log in as **ftpuser**.	/hfs_public/nbi/inv/incexport
4	FTP/SFTP mode	Yes	Transfer mode of inventory data. **NOTICE** SFTP is recommended, because it is more secure than FTP.	SFTP
5	FTP/SFTP server IP address	Yes	IPv4 or IPv6 address of the FTP/SFTP server that receives inventory data.	10.10.10.10
6	FTP/SFTP server port	Yes	Port through which the FTP/SFTP server receives inventory data.	22
7	Inventory FTP/SFTP upload directory	Yes	Directory where the FTP/SFTP server places the inventory data received.	/tmp/export
8	Increment FTP/SFTP upload directory	Yes	Directory where the FTP/SFTP server places the incremental inventory data received.	/tmp/incexport
9	FTP/SFTP username	Yes	Name of the user who can transfer files through FTP/SFTP.	sopuser

No.	Parameter	Mandatory	Description	Example
10	Authentication Mode	Yes	Authentication mode, which can be **Password** or **Public Key Authentication**. – If **FTP/SFTP mode** is **FTP**, **Authentication mode** can only be **Password**. – If **FTP/SFTP mode** is **SFTP**, **Authentication mode** can be **Password** or **Public Key Authentication**. **NOTE** – **Password**: The SFTP user password is required during first-time authentication. To change the password, select **Change Password**. – **Public Key Authentication**: An SFTP private key file needs to be uploaded for authentication. To generate this file, refer to **8.6 How Do I Generate a Private Key File?** After uploading an SFTP private key file: ■ If the private key file is encrypted, set **Encrypt private key** to **Yes** and enter the correct file password in the **Enter the private key password** dialog box. ■ If the private key file is not encrypted, set **Encrypt private key** to **No** and click **OK** in the **Enter the private key password** dialog box.	Password

No.	Parameter	Mandatory	Description	Example
11	FTP/SFTP password	Yes	Password for the user who can transfer files through FTP/SFTP. **NOTICE** – The password must meet the following complexity requirements: (1) Not be the same as or the reverse of the username. (2) Contain at least eight characters. (3) Contain at least three of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (=~@#^*-_+ [{}];:./?). (4) Not be repetitive strings of any length, for example, aaaaaaaa, abababab, or abcdabcd. – For security purposes, change the password in a timely manner, update it periodically, and keep it secure.	--
12	Confirm FTP/SFTP password	Yes	Confirm password.	--

Step 7 Set parameters in the **Scheduled Inventory Export Settings** area.

- If you need scheduled inventory export, set **Scheduled inventory export** to **Enable** and set other parameters by referring to **Table 3-11**.

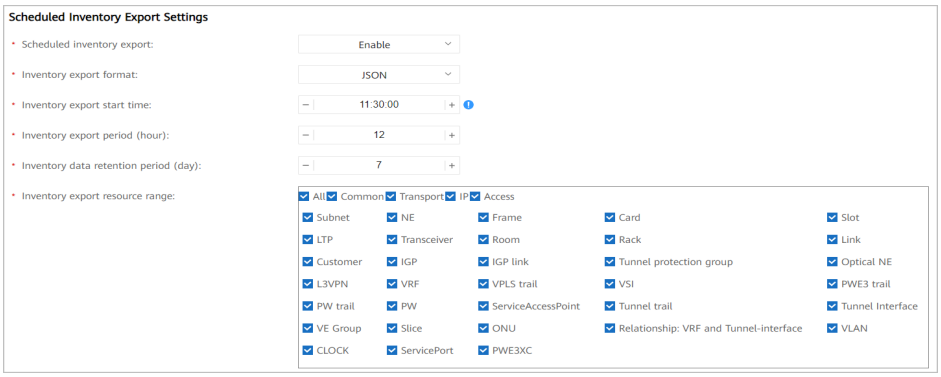


Table 3-11 Inventory export settings

Parameter	Description	Example
Inventory export format	Value range: – JSON (default value) – CSV **NOTICE** If Excel displays a security statement upon your attempt to open a CSV file exported from NCE, use a text editor to open the CSV file and check that no command injection risk is involved with the character strings starting with an equal sign (=), plus sign (+), minus sign (–), or at sign (@). Then, re-open the file with Excel.	JSON
Inventory export start time	Exporting network-wide inventory data is a resource- and time-consuming process. To avoid slowing down the system, it is advisable to select an off-peak time. **NOTE** If you want to change the start time, change it at least 30 seconds in advance.	12:00:00
Inventory export period (hour)	The recommended value is 12 hours or longer.	12
Inventory data retention period (day)	The recommended value is 3 days. **NOTE** This parameter takes effect only when **Exported to** is set to **Local server**.	3
Inventory export resource range	Recommended resource types are automatically selected. You can make changes as required. **NOTE** The resource item **Transceiver** is available only for the IP domain.	--

- If you do not need scheduled inventory export, set **Scheduled inventory export** to **Disable** and directly go to **Step 8**.

Step 8 Set parameters in the **Scheduled Inventory Increment Export Settings** area.

NOTE

Full inventory export consumes a large amount of system resources and affects the system speed. Therefore, incremental export is provided as a complementary approach to full export. This approach can export data in a timely fashion without affecting the system speed.

- If you need scheduled incremental inventory export, set **Scheduled increment export** to **Enable** and set other parameters by referring to **Table 3-12**.

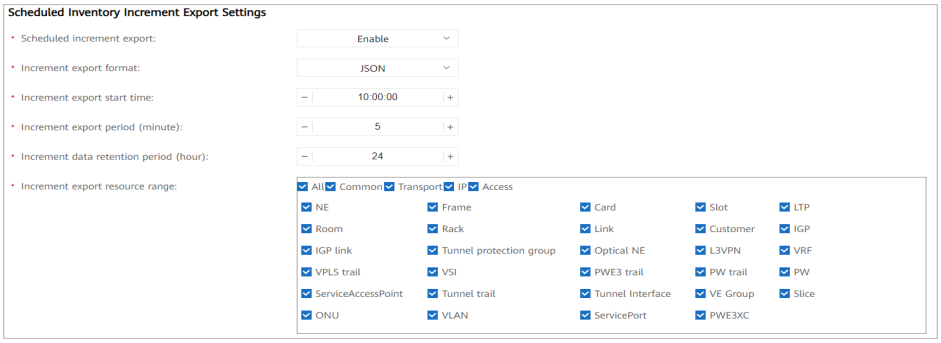


Table 3-12 Incremental inventory export settings

Parameter	Description	Example
Increment export format	Value range: – JSON (default value) – CSV **NOTICE** If Excel displays a security statement upon your attempt to open a CSV file exported from NCE, use a text editor to open the CSV file and check that no command injection risk is involved with the character strings starting with an equal sign (=), plus sign (+), minus sign (–), or at sign (@). Then, re-open the file with Excel.	JSON
Increment export start time	It is advisable to select an off-peak time.	12:00:00
Increment export period (minute)	The recommended value is 5 minutes or longer.	5
Increment data retention period (hour)	The recommended value is 24 hours or longer. **NOTE** This parameter takes effect only when **Exported to** is set to **Local server**.	24
Increment export resource range	Recommended resource types are automatically selected. You can make changes as required.	--

- If you do not need scheduled incremental inventory export, set **Scheduled increment export** to **Disable** and directly go to **Step 9**.

Step 9 Click **Save**.

Step 10 In the dialog box that is displayed, click **OK**.

----End

3.7 Configuring Alarm Reporting

NCE has the alarm reporting function. You can configure this function so that alarms will be correctly reported to the desired server.

Configuring the alarm reporting function of the REST NBI may affect other NCEcomponents and the OSS. Modifying certain configuration items (**Table 3-13**) may also depend on other NCE components. Before configuring the REST NBI, check whether these configuration items will cause such impact and seek advance consent from customers.

Table 3-13 Key configuration items

Configuration Item	Description	Impact
Report correlative alarms	Whether to report correlative alarms.	None
Report engineering alarms	Whether to query or report engineering alarms. This function is enabled by default.	• If disabled, NCE does not report some topics of notifications to the OSS. • If enabled, the OSS may receive unnecessary notifications.

NBI components are automatically deployed during NCE installation. Alarm reporting, however, still needs to be manually enabled.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 4 In the navigation pane, choose **REST NBI > Alarm Settings**. In the right pane, set parameters based on **Table 3-14**.

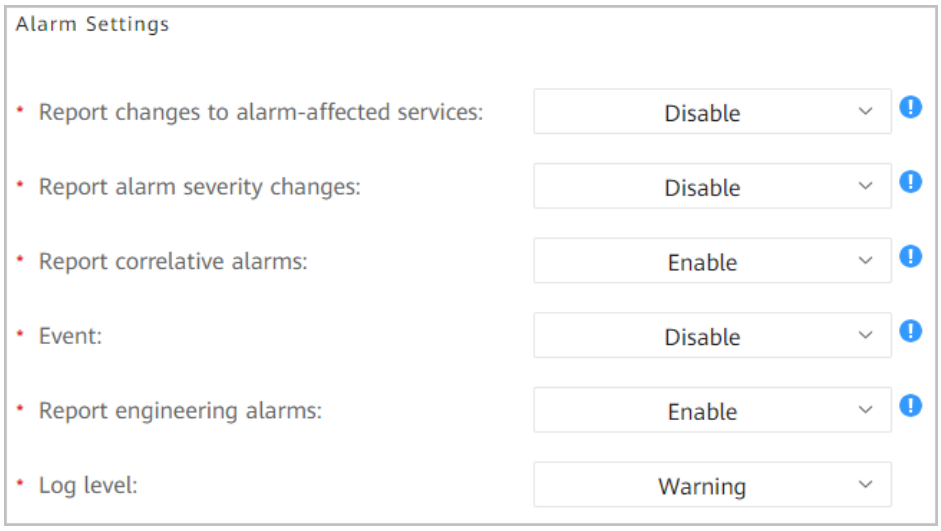


Table 3-14 Alarm parameters

No.	Parameter	Mandatory	Description	Example
1	Report changes to alarm-affected services	Yes	Whether to report alarm-affected services to the OSS. This function is disabled by default.	Disable
2	Report alarm severity changes	Yes	Whether to report alarm severity changes. This function is disabled by default.	Disable
3	Report correlative alarms	Yes	Whether to report correlative alarms. If enabled, correlative alarms can be queried or reported. This function is enabled by default.	Enable
4	Event	Yes	Whether to report events. This function is disabled by default.	Disable
5	Report engineering alarms	Yes	Whether to report engineering alarms. If enabled, engineering alarms can be queried or reported. This function is enabled by default.	Enable
6	Log level	Yes	Log level of the service.	Warning

Step 5 Click **Save**.

Step 6 In the dialog box that is displayed, click **OK**.

----End

3.8 Configuring Incident Export

NBI components are automatically deployed during NCE installation. Scheduled incident export through the REST NBI, however, still needs to be manually enabled.

Prerequisites

- All databases are running.
- The installation directory has more than 20 GB space available. On EulerOS, you can run the **df -hk /opt** command to view available space in **/opt**.
- You have obtained the values of all the involved configuration items from the OSS vendor.
- AIFMService has been installed.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 4 In the navigation pane, choose **REST NBI** > **Incident Task Settings**.

Step 5 On the **Incident Task Settings** page, click **Create**.

NOTE

AIFMService is an optional component. If AIFMService is not installed, you cannot create incident tasks.

Step 6 In the **Task Information** area, set **Task name** to the desired name.

NOTE

- After a task is created, you can click or in the **Operation** column to modify or delete the task.
- The **Incident Task Settings** page allows you to create a maximum of 10 tasks, with each task scheduled to start at least one hour earlier or later than another. (The interval is measured by hour, minute, and second, but not by year, month, or day. If the interval between any two tasks is less than an hour, even by one second, the system will trigger an error message.)

Step 7 Determine whether to use a third-party server to store the exported incident data. (By default, the system stores incident data on the local server.)

- If yes, set parameters in the **Export Model Settings** area by referring to **Table 3-15**.

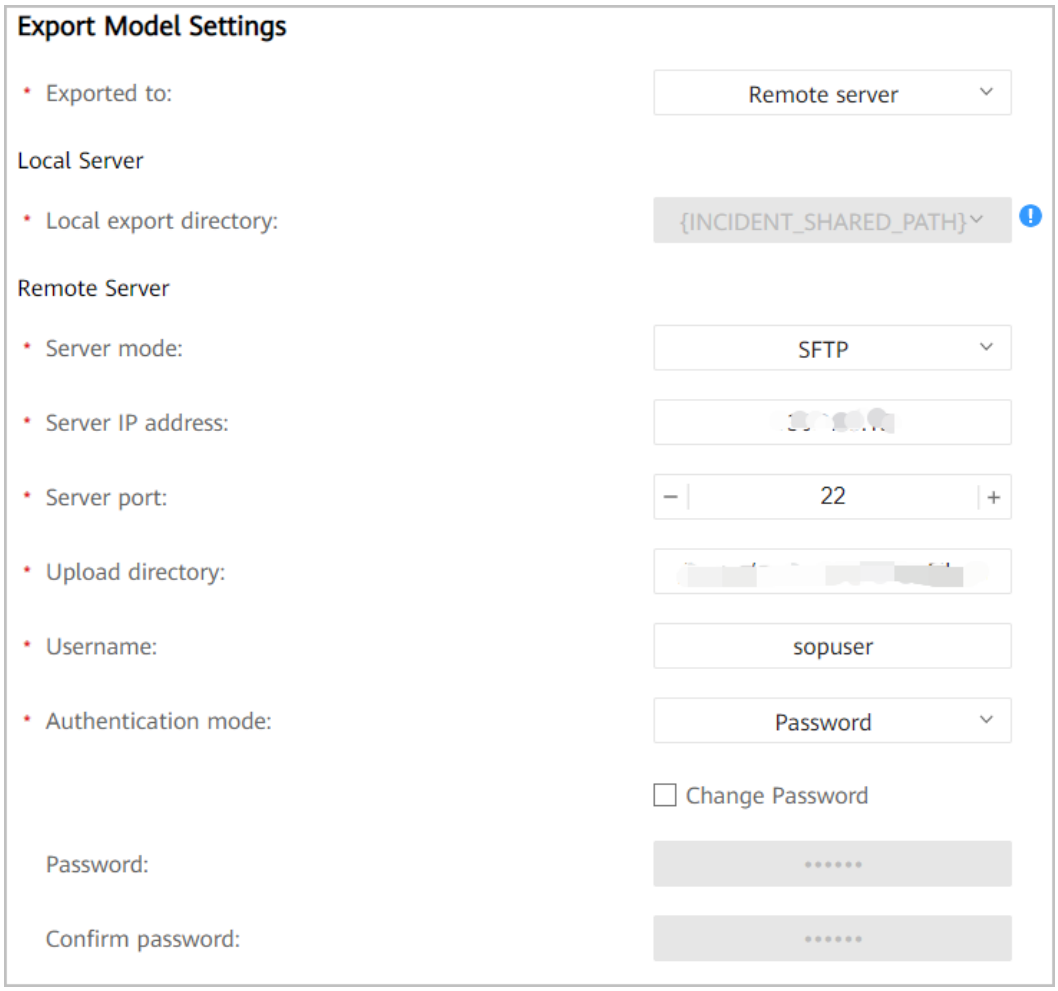


Table 3-15 Export server parameters

No.	Parameter	Mandatory	Description
1	Exported to	Yes	Type of server used to receive incident data. Set it to the actual plan. If **Local server** is selected, parameters 3 through 10 are not required.
2	Local export directory	Yes	Local directory used to store incident data.
3	Server mode	Yes	Transmission mode of incident data.
4	Server IP address	Yes	IPv4 or IPv6 address of the FTP/SFTP server that receives incident data.

No.	Parameter	Mandatory	Description
5	Server port	Yes	Port number of the FTP/SFTP server that receives incident data.
6	Upload directory	Yes	Directory where the FTP/SFTP server stores the received incident data.
7	Username	Yes	Name of the user who can transfer files through FTP/SFTP.
8	Authentication mode	Yes	Authentication mode. (Only **Password** is available.) **NOTE** The FTP/SFTP user password is required during first-time authentication. To change the password, select **Change Password**.
9	Password	Yes	Password for the user who can transfer files through FTP/SFTP. **NOTICE** • For security purposes, the password cannot be the username or the username spelled backwards, cannot be repetitive strings of any length, cannot be shorter than 8 characters, and must contain at least three of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (=~@#^*-_+[{}];:./?). • For security purposes, change the password in a timely manner, update it periodically, and keep it secure.
10	Confirm password	Yes	Confirm password.

If no, proceed to **Step 8**.

Step 8 Set parameters in the **Scheduled Export Settings** area.

- If you need scheduled inventory export, set **Scheduled export** to **Enable** and set other parameters based on **Table 3-16**.

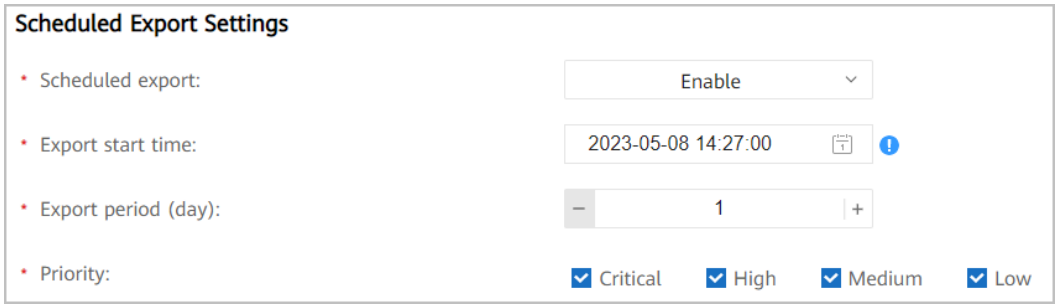


Table 3-16 Scheduled export parameters

Parameter	Description	Example
Export start time	Exporting network-wide incident data is a resource- and time-consuming process. To avoid slowing down the system, it is advisable to select an off-peak time. **NOTE** • If you want to set a specific start time, do so at least 30 seconds earlier before that time. • Counted from the execution time, the task exports only current incident data and historical incident data in the past three days.	12:00:00
Export period (day)	Value range: 1–31; Default: **1**	1
Priority	Severities of incidents to export. By default, all the severities are selected. You can select one (at least) or more severities among the following as needed: • Critical • High • Medium • Low **NOTE** If no severity is selected, an error will be reported upon the click of **Save**, and consequently, the task cannot be delivered.	-

- If you do not need scheduled export, set **Scheduled export** to **Disable** and directly go to **Step 9**.

Step 9 Click **Save**.

Step 10 In the dialog box that is displayed, click **OK**.

----End

3.9 Obtaining Text Files

The REST NBI supports full export and incremental export of inventory resources, and export tasks can be created for one or more types of inventory resources at a time. In addition, multiple tasks can be created for text export of incident data. After a user creates an export task, only that user can query the task status and download the files generated by the task.

NOTE

- Before obtaining inventory files, correctly configure inventory export tasks. For details, see **3.6 Configuring Inventory Export**.
- Before obtaining incident files, correctly configure incident export tasks. For details, see **3.8 Configuring Incident Export**.

3.9.1 File Export Directories

The REST NBI converts inventory resource data and incident data into files in a unified format and saves the files to specified directories.

After logging in to the Common_Service node, **ftpuser** can directly access these directories, namely:

- Full export of inventory resources: **/hfs_public/nbi/inv/export/***task ID/timestamp/file name*
- Incremental export of inventory resources: **/hfs_public/nbi/inv/incexport/***task ID/timestamp/file name*
- Incident export: **/hfs_public/nbi/incident/export/***timestamp/file name*

Table 3-17 Rules about the file export directories

Field	Description	Example
/hfs_public/nbi	Fixed prefix of the directory storing the exported files.	/hfs_public/nbi
/inv/export	Fixed prefix of the directory storing the fully exported inventory resource files.	/inv/export
/inv/incexport	Fixed prefix of the directory storing the incrementally exported inventory resource files.	/inv/incexport
/incident/export	Fixed prefix of the directory storing the exported incident files.	/incident/export
Task ID	A maximum of 10 inventory export tasks can be created at the same time, with each task scheduled to start at least one hour earlier or later than another task. **NOTE** The default task does not have this field in its export directory.	1
Timestamp	Timestamp Start time of an export task, in YYYYMMDD format.	20230307
File name	Name of the exported file, which is in .zip format. For details, see **3.9.2 File Naming Rule**.	-

3.9.2 File Naming Rule

To facilitate management, the REST NBI names inventory files and incident files based on the following rules:

Rule for naming inventory files: *{object-type}* - *{version}*-*{yyyymmddhhmmss}* *{serial}*.zip

Rule for naming incident files: *incident-{yyyymmddhhmmss}{serial}*.zip

Table 3-18 File naming rule

Field	Description	Example
{object-type}	Name of the resource model used for inventory export.	network-element
{version}	Version of the resource model used for inventory export. **NOTE** For ports and IGP links, the version is v3; for other resources, the version is v2.	v2
incident	Prefix in the names of files exported by incident tasks. The default value is **incident**.	incident
{yyyymmddhhmmss}	Timestamp End time of an export task, in YYYYMMDDhhmmss format.	20230307120325
{serial}	Package SN, which consists of three digits. Inventory files larger than 100 MB are split when being compressed into packages that are named in the sequence of 001, 002, 003, and so on. If a .zip package comes with 001 only, the original file is not split.	001

Additional Information

- File format and exported fields

  Incident tasks can only export JSON files through the REST NBI, whereas inventory files can be exported in CSV or JSON format. For details about the fields exported for each type of resource, see *NBI Inventory Attribute Support Summary* in the related **iMaster NCE REST NBI Documents** folder.

  NOTICE

  If Excel displays a security statement upon your attempt to open a CSV file exported from NCE, use a text editor to open the CSV file and check that no command injection risk is involved with the character strings starting with an equal sign (=), plus sign (+), minus sign (–), or at sign (@). Then, re-open the file with Excel.

  Null values come in different forms in different file formats:

  - JSON: does not return the attributes whose values are null. Doing so helps reduce unnecessary packet transmission; therefore, it is advisable to export data in JSON format.
  - CSV: returns the attributes whose values are null and leaves the corresponding places blank. Doing so helps retain complete resource information.
- File parsing

  Decompress the downloaded .zip packages to obtain original files.
  - In the exported incident files, each row records the data of an incident.
  - In the exported inventory files, each row records the data of a resource. In incremental files, each row records the changes made to a resource in the current period compared with the previous period.

3.10 Creating a REST NBI User for an OSS

In addition to normal work of the REST NBI and successful network communication, create a user on NCE for each OSS and assign the REST NBI permissions to it so that OSSs can access NCE through the REST NBI.

Context

NOTICE

- Before connecting different OSSs to the REST NBI, you need to create different access users on NCE. That is, one user cannot be used to access different OSSs.
- Users created on the NCE O&M plane can be used only for access authentication and operations on the NCE O&M plane. If a local user is created or its password is reset, change the password upon first login to the NCE O&M plane. Otherwise, the user cannot be used to interconnect with the NBI.
- For security purposes, when OSSs access NCE through the NBI, NCE authenticates the users they use. In addition, NCE controls the permissions of access users. Only users who have related permissions can call the REST NBI.
- More information about user management is available at the NCE information center.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the Security Management app and choose **User Management** from the main menu.

Step 4 On the **Roles** page, click **Create**.

1. Enter a role name, for example, **NBITestRole**.
2. Select managed objects.
   a. **All Objects**: includes all the resources that can be managed by the system. This is the default managed object provided by the system, and it cannot be modified or deleted.
   b. **Subnets**
   c. **Device Sets**
   d. **Devices**

   NOTE

   - Enable the domain-based function (**8.2 How Do I Enable the Domain-based Function for New Users?**) during role creation. Otherwise, operations on the resources of the selected managed objects will not take effect.
   - If the domain-based function is enabled, you need to select specific devices or device sets. Open the Security Management app and choose **User Management** from the main menu on the NCE O&M plane, you can create a device set with the desired devices on the **Device Sets** tab page (**User Management** > **Managed Objects**).
3. Select operation rights by referring to **Step 7**.

Step 5 On the **Users** page, click **Create**.

NOTICE

To be compatible with northbound users on U2000, NCE supports the user type **Local**. However, for security purposes, **Third-party** is recommended. Their differences are:

- Local users have permission to log in to the NCE O&M plane. Create a local user if you need to configure scheduled inventory data export on the GUI.
- Third-party users have no permission to log in to the NCE O&M plane. Create a third-party user if you need to export or query inventory data, query alarms, update alarms, and acknowledge or unacknowledge alarms through the REST NBI.

Set it as required.

Step 6 On the user creation page, add the new user to the **NBITestRole** role created in **Step 4** and set the attributes of the new user.

Table 3-19 User attributes

Attribute	Description
Basic information	The OSS uses the username and password set here to access NCE through the REST NBI. **NOTE** The username must consist of 6 to 32 characters and cannot contain spaces, escape characters, special characters "&'+/;<=>?\©®`~*()|:,[]{} or invisible characters.
Role	Select the **NBI User Group** role so that the user has all permissions of **NBI User Group**.
Access policy	IP addresses beyond the access control list (ACL) cannot access NCE. **NOTICE** By default, the ACL is blank. That is, the REST NBI does not verify OSS IP addresses. For security purposes, it is advisable to configure an ACL for the REST NBI.

NOTICE

For security purposes, change the initial password upon the first login and update it periodically according to complexity requirements, the password must meet the following requirements:

1. Consist of 8 to 32 characters.
2. Contain at least one uppercase letter (A–Z), one lowercase letter (a–z), one digit (0–9), and one special character such as !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~.
3. Cannot contain more than two consecutive occurrences of the same character or string repetitions (times: 4; length: 1).
4. Cannot contain the username, reverse of the username, mobile number, email address, or any word in the password dictionary.
5. For security purposes, after creating a local user, change its password upon first login.

Step 7 Set the managed objects and operation rights of the user.

Table 3-20 User's managed objects and operation rights

Attribute	Description
Managed objects	Users who access NCE through the REST NBI can only manage the specified objects (devices).

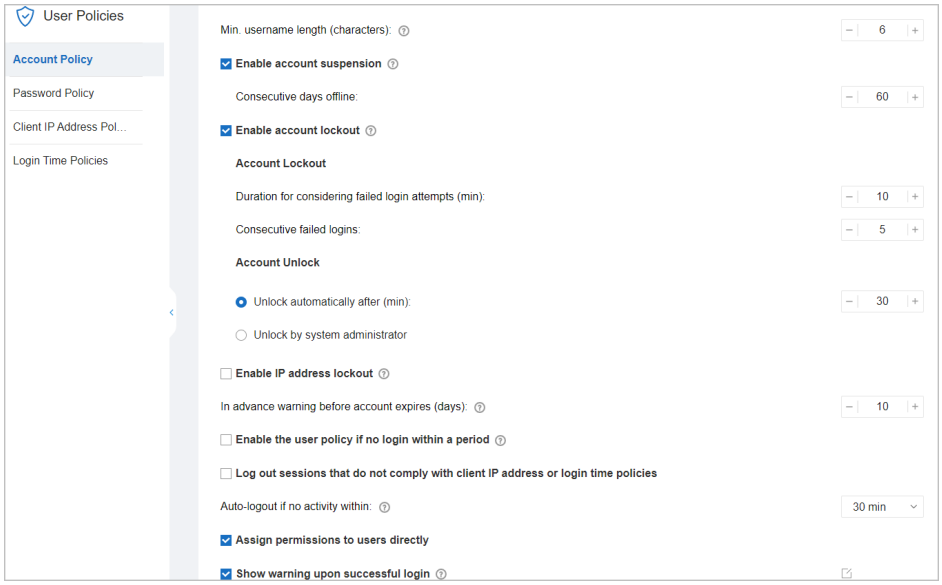
Attribute	Description
Operation rights	To use the REST NBI, the user must have related operation rights. The REST NBI involves the following operation rights: ● Local user: – Modifying REST NBI configuration items – Querying REST NBI configuration items ● Third-party user: – GET: calls GET APIs. – POST: calls POST APIs. – PUT: calls PUT APIs. – DELETE: calls DELETE APIs. – PATCH: calls PATCH APIs.

- Method 1 (recommended): Add a role by referring to **Step 4**, select managed objects and operation rights for this role, and add the northbound user to it.
- Method 2: Directly set the managed objects and operation rights of the user.

  By default, you cannot directly set managed objects or operation rights for individual users. If you need to, do as follows:

  a. Open the Security Management app and choose **User Policies** from the main menu.

  b. On the **Account Policy** page, select **Assign permissions to users directly**.



  c. On the **Users** page, click the username and set managed objects and operation rights.

----End

3.11 Configuring RESTful Callback

If the RESTful protocol is chosen to report service data, related RESTful protocol, alarm, alarm acknowledgment/unacknowledgement, event, and notification parameters need to be set.

Prerequisites

- You have the **Query Northbound RESTful Callback Configuration Items** and **Modify Northbound RESTful Callback Configuration Items** permissions.
- You have obtained the trust certificate, IP address, port number, username, password, authentication mode, required services and service information of the target RESTful server from the system administrator.

  NOTE

  If **Authentication mode** is **Token**, the following information is also required: **Token expiration time**, **Token request URL**, **Token request packet**, **Token value**, and **Token field in the request header**.

Context

- If a subscription with token preconfigured is created to interconnect with a third-party system using an interface, the interconnection information about the third-party system is automatically displayed on the **RESTful Callback** page. In this case, you can only view the interconnection information but cannot edit or delete it. In other words, if you attempt to edit the interconnection information, the parameters are dimmed.
- By default, NCE authenticates the third-party REST server. You need to import the identity certificate of the third-party REST server to the third-party REST server, and obtain the trust certificate of the third-party REST server and import it to NCE.
- If authentication on NCE is enabled on the third-party REST server, you need to obtain the trust certificate of NCE and import it to the third-party REST server. You also need to check whether an identity certificate is displayed on the **Identity Certificate** tab page of NCE. If no, you need to import one as prompted. If the identity certificate of NCE is updated, you need to obtain the corresponding trust certificate again and import it to the third-party REST server. Obtain the trust certificate of NCE as follows:
  a. On the O&M plane, choose **System** > **System Settings** > **Certificate Management** from the main menu.
  b. In the navigation pane, choose **Service Certificate Management**.
  c. Click the **NBIFrmNotifyService-RESTful** card.
  d. On the **Identity Certificate** tab page, click **Export** in the **Operation** column.

Procedure

Step 1 Import the trust certificate of the RESTful server to NCE.

1. Open the System Settings app and choose **System Settings** > **Certificate Management** from the main menu. Then click **Administrator Certificate Management** on the NCE O&M plane.
2. In the navigation pane, choose **Service Certificate Management**.
3. Click the **NBIFrmNotifyService-RESTful** card.

   NOTE

   If NCE authentication is enabled on the third-party RESTful server, import NCE's trust certificate to the third-party RESTful server. Also, if NCE's identity certificate is not present on the **Identity Certificates** tab page, you should import it there. Whenever NCE's identity certificate is updated, obtain the corresponding trust certificate (by clicking **Export** in the **Operation** column on the **Identity Certificates** tab page) and import the trust certificate to the third-party RESTful server.
4. Configure the trust certificate of NBIFrmNotifyService-RESTful. For details, see **Step 7**.

Step 2 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu on the O&M plane.

Step 3 In the navigation pane, choose **RESTful Callback**. In the **General Settings** area, set general parameters for the RESTful client.

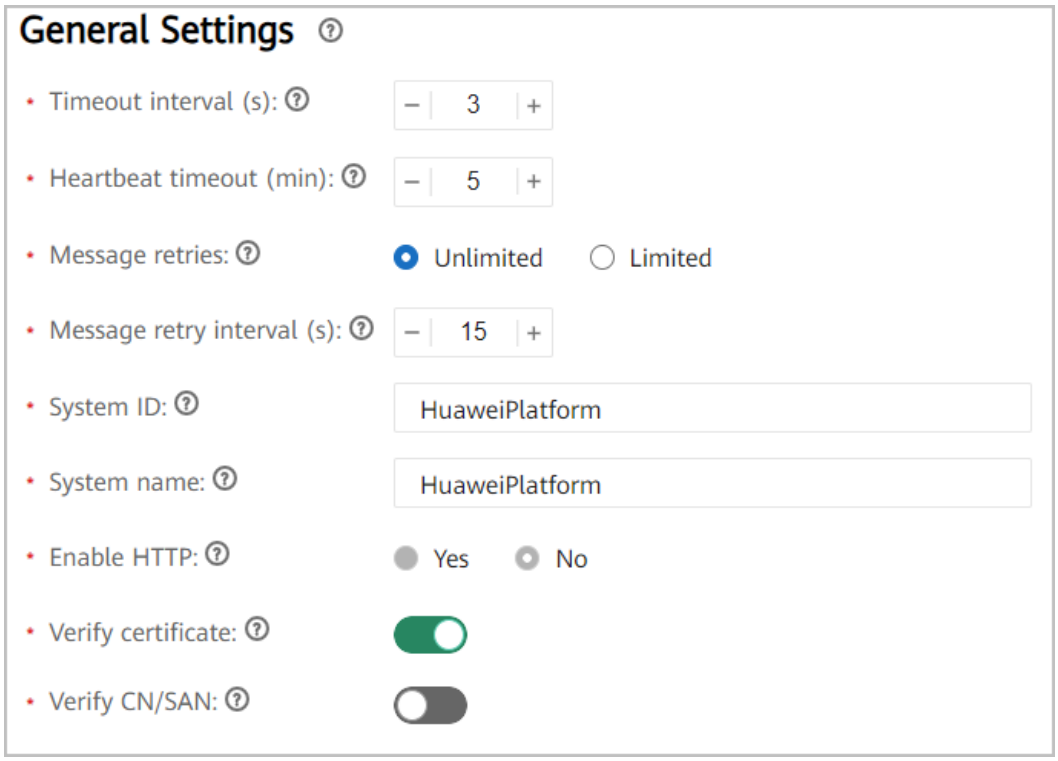


Table 3-21 General parameters

Parameter	Mandatory	Description	Example
Timeout interval (s)	Yes	The value range is from 1 to 60.	3

Parameter	Mandatory	Description	Example
Heartbeat timeout (min)	Yes	The value range is from 1 to 30.	5
Message retries	Yes	Number of times that a message can be resent after it failed to be sent to a third-party system. The options are as follows: • Unlimited • Limited (value range: 1–999)	Unlimited
Message retry interval (s)	Yes	Interval for resending a message after it failed to be sent to a third-party system. The value range is from 1 to 60.	15
System ID	Yes	ID of the source which sends heartbeat packets. It is used together with the system name to uniquely identify a source. The value should be a string of 1 to 64 characters, and only the following are allowed: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (_@() ,.^$~ '!-).	HuaweiPlatform
System name	Yes	Name of the source which sends heartbeat packets. It is used together with the system ID to uniquely identify a source. The value should be a string of 1 to 1024 characters, and only the following are allowed: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (_@() ,.^$~ '!-).	HuaweiPlatform

Parameter	Mandatory	Description	Example
Enable HTTP	Yes	The default value is **No**. **No** is recommended because HTTPS is more secure than HTTP. **NOTICE** • For security purposes, this parameter is non-editable by default. If you want to modify it, refer to **8.10 How Do I Enable or Disable Insecure Configurations of the RESTful Callback Interface?** • The HTTP(S) rate depends on the responsiveness of the server. Therefore, it is not recommended in large-scale networks.	-
Verify certificate	Yes	Whether to verify the server certificate. If enabled, NCE verifies the identity certificates of third-party systems. **NOTICE** For security purposes, you are advised to enable certificate verification.	-
Verify CN/SAN	Yes	If enabled, NCE verifies the common names (CNs) and subject alternative names (SANs) of third-party systems' identity certificates. To improve communication security, you are advised to enable CN/SAN verification. **NOTICE** For security purposes, disabling CN/SAN verification (when it is already enabled) will open a **Warning** dialog box for you to confirm whether to continue.	-

Step 4 Click **Apply**. In the **High Risk** dialog, select **I understand the risks and want to continue** and click **OK** for the general settings to take effect.

Step 5 In the **Third-Party Server Settings** area, click **Create**. The displayed page is organized into two areas: **Protocol Configuration** and **Service Configuration**.

Step 6 In the **Protocol Configuration** area, set RESTful server parameters.

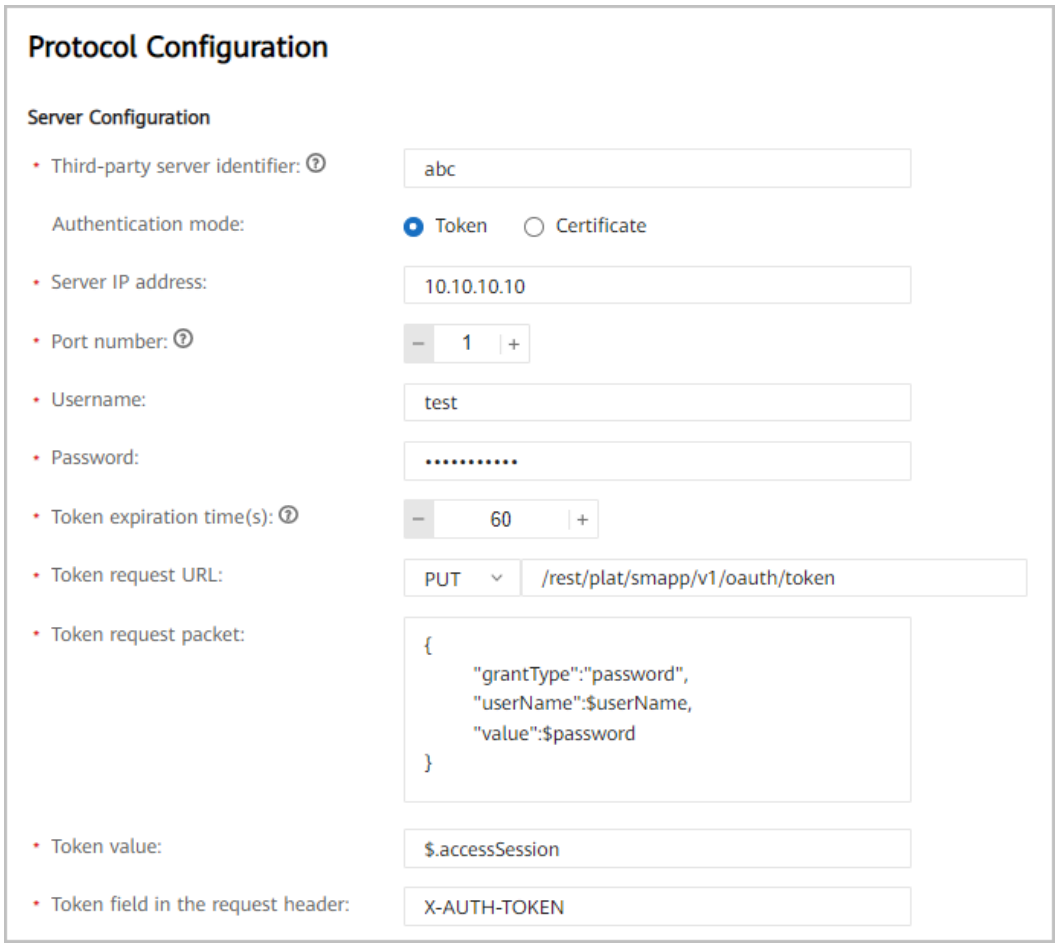


Table 3-22 RESTful server parameters

No.	Parameter	Description	Example
1	Third-party server identifier	Identifier of the reporting channel, which is used to identify a third-party NMS. The identifier should be a string of 1 to 128 characters, and only the following are allowed: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (_-).	-
2	Authentication mode	If **Authentication mode** is set to **Certificate**, only parameters 1–4 need to be set. The options are as follows: • Token • Certificate	-
3	Server IP address	IPv4 or IPv6 address of the RESTful server.	10.10.10.10

No.	Parameter	Description	Example
4	Port number	Port number of the RESTful server. Enter a number from 1 to 65535.	1
5	Username	Username for logging in to the third-party server. The name should be a string of 1 to 128 non-whitespace characters.	-
6	Password	Password for the user to log in to the third-party server. The password should be a string of 1 to 128 non-whitespace characters.	-
7	Token expiration time(s)	Enter a number from 60 to 31536000.	60
8	Token request URL	The request mode can be POST or PUT. The URL should be a string of 2 to 1024 characters, start with a slash (/), and contain one or more of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (_-). It cannot contain consecutive slashes (//) or end with a special character (_-).	/rest/plat/smapp/v1/oauth/token

9	Token request packet	Enter a request body in the .json format, including the username and password.	{
			"grantType":"password",
			"userName":$userName,
			"value":$password
			}

10	Token value	It should be a string of 1 to 128 non-whitespace characters.	$.accessSession
11	Token field in the request header	It should be a string of 1 to 32 non-whitespace characters.	X-AUTH-TOKEN

Step 7 In the **Service Configuration** area, set service parameters.

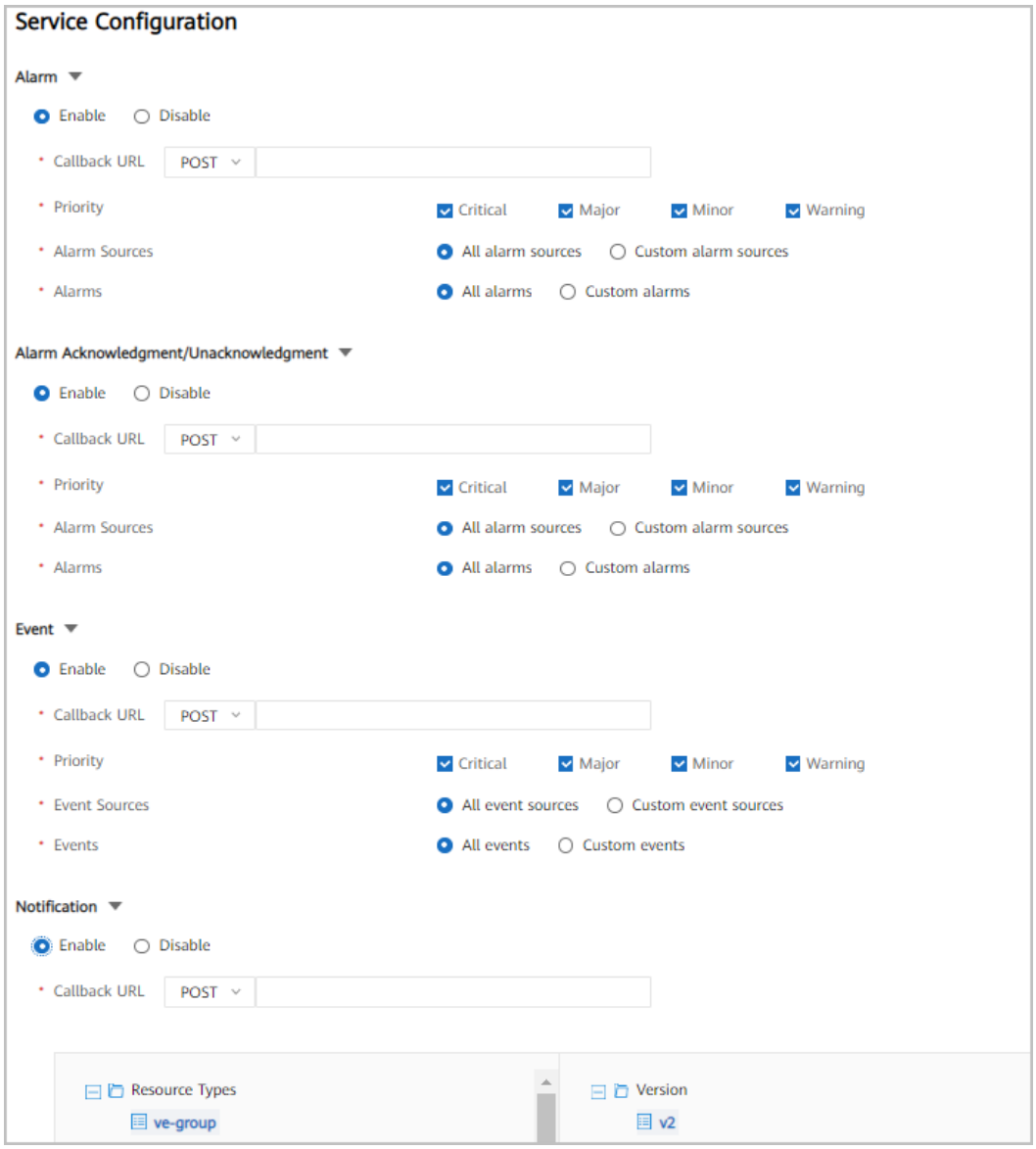


Table 3-23 Service parameters

Parameter	Value	Sub-item	Sub-item Description
Alarm	**Enable**: reports alarms.	Callback URL	The URL should be a string of 2 to 1024 characters, start with a slash (/), and contain one or more of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (_-). It cannot contain consecutive slashes (//) or end with a special character (_-).

Parameter	Value	Sub-item	Sub-item Description
		Priority	Severities of IETF alarms. You can select one (at least) or more severities among the following: • Critical • Major • Minor • Warning
		Alarm Sources	• **All alarm sources**: reports alarms from all sources. • **Custom alarm sources**: reports alarms from custom sources only. You can select a maximum of 20 sources.
		Alarms	• **All alarms**: reports all alarms. • **Custom alarms**: reports custom alarms only. You can select a maximum of 50 alarms.
	Disable (default value): does not report alarms.	-	-
Alarm Acknowledgment/ Unacknowledgment	**Enable**: reports acknowledged/ unacknowledged alarms.	Callback URL	The URL should be a string of 2 to 1024 characters, start with a slash (/), and contain one or more of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (_-). It cannot contain consecutive slashes (//) or end with a special character (_-).
		Priority	Severities of acknowledged/unacknowledged alarms. You can select one (at least) or more severities among the following: • Critical • Major • Minor • Warning
		Alarm Sources	• **All alarm sources**: reports acknowledged/ unacknowledged alarms from all sources. • **Custom alarm sources**: reports acknowledged/ unacknowledged alarms from custom sources only. You can select a maximum of 20 sources.

Parameter	Value	Sub-item	Sub-item Description
		Alarms	• **All alarms**: reports all acknowledged/ unacknowledged alarms. • **Custom alarms**: reports custom acknowledged/ unacknowledged alarms only. You can select a maximum of 50 alarms.
	Disable (default value): does not report acknowledged/ unacknowledged alarms.	-	-
Event	**Enable**: reports events.	Callback URL	The URL should be a string of 2 to 1024 characters, start with a slash (/), and contain one or more of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (_-). It cannot contain consecutive slashes (//) or end with a special character (_-).
		Priority	Severities of events. You can select one (at least) or more severities among the following: • Critical • Major • Minor • Warning
		Event Sources	• **All event sources**: reports events from all sources. • **Custom event sources**: reports events from custom sources only. You can select a maximum of 20 sources.
		Events	• **All events**: reports all events. • **Custom events**: reports custom events only. You can select a maximum of 50 events.
	Disable (default value): does not report events.	-	-

Parameter	Value	Sub-item	Sub-item Description
Notification	**Enable**: reports resource notifications.	Callback URL	The URL should be a string of 2 to 1024 characters, start with a slash (/), and contain one or more of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (_-). It cannot contain consecutive slashes (//) or end with a special character (_-).
		Resource Types	Custom types of resources for which notifications will be reported. Multiple types can be selected. **NOTE** In the same configuration task, only one version can be configured for the same resource type. If you want to configure another version, delete the configured version first.
		Operation	• create • modify • delete
	Disable (default value): does not report resource notifications.	-	-

Step 8 (Optional) To test connectivity between the NBI of NCE and the RESTful server, click **Check Connectivity**.

- If "Connectivity check successful" is displayed, click **OK**.
- If "Failed to check the connectivity" is displayed, click **OK**. Possible causes of failure include:
  a. Certificate configurations are incorrect.
  b. Failed to connect to the server.
  c. The username or password is incorrect.
  d. Failed to obtain the token.

Step 9 Click **Save**. When a success message is displayed, click **OK**.

----End

Related Tasks

- Modifying a third-party server

  In the **Third-Party Server Settings** area, click (**Edit**) in the **Operation** column.

NOTE

Modifying RESTful callback configurations may disrupt data reporting through the RESTful protocol. Exercise caution.

- Deleting a third-party server

  In the **Third-Party Server Settings** area, click (**Delete**) in the **Operation** column. Alternatively, select one or more RESTful servers and click **Delete** above the server list.

  NOTE

  Deleting third-party servers may disrupt data reporting through the RESTful protocol. Exercise caution.

- Checking connectivity

  In the **Third-Party Server Settings** area, click (**Check Connectivity**) in the **Operation** column to test connectivity between the NBI of NCE and the selected RESTful server.

4 Maintaining REST NBIs

This topic describes how to perform routine maintenance on the NBIs and how to start and stop the NBIs.

4.1 Routine Maintenance Operations

Table 4-1 Routine maintenance operations

Maintenance Interval	Maintenance Operation	Description
Daily maintenance	Check the security log.	Check the information related to security operations.
	Check the server resource usage.	Check the server resource usage, such as the CPU usage, memory usage, and disk usage.
Weekly maintenance	Check the server disk status.	Check the disk status periodically. If the disk is faulty, repair or replace it in a timely manner.

Maintenance Interval	Maintenance Operation	Description
	Check the server disk space.	Check the server disk space periodically and clean it in a timely manner.
	Check the OS log.	Check the OS running status.
	Check the running status of antivirus software.	Upgrade the antivirus software and remove virus to prevent servers and computers from being infected.
Monthly maintenance	Check the server time.	Check whether the server time is correct.
	Change the user password.	Change the password periodically to improve password security.
	Clean the server disk.	Clean the server disk periodically to free up space.

4.2 Checking the Running Status of an NBI Service

You can log in to the NCE management plane to check the running status of an NBI service and ensure that the NBI provides services properly.

Procedure

Step 1 Log in to the NCE management plane.

Open a browser, enter **https://***IP address of the management plane*:**31945** in the address bar, and press **Enter**.

NOTE

IP address of the management plane refers to the client login IP address configured on the OMP node.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.

Step 4 In the navigation pane, choose **Service Monitoring**.

Step 5 On the **Services** tab page, search for NBI services.

- If all NBI services are **Running**, no further action is required.

- If any NBI service status is not **Running**, check whether the service is required. If it is required, contact Huawei technical support.

----End

4.3 Starting and Stopping NBI Services

During routine maintenance, you can start and stop NBI services on the NCE management plane.

4.3.1 Starting an NBI Service

NBIInventoryService, NBIPerformanceService, and NBINotifyService can be deployed in Manager, Manager+Controller, or Manager+Controller+Analyzer. By default, they are not started in Manager but started in Manager+Controller and Manager+Controller+Analyzer.

To make them automatically start up in Manager, refer to **8.9 How Do I Change the Startup Modes of NBI Processes?**

Procedure

The following uses the NCE/InventoryNBI/InventoryNBI_NBIInventoryService instance as an example to describe how to start an NBI service.

Step 1 Log in to the NCE management plane.

Open a browser, enter **https://***IP address of the management plane***:31945** in the address bar, and press **Enter**.

NOTE

IP address of the management plane refers to the client login IP address configured on the OMP node.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.

Step 4 In the navigation pane, choose **Service Monitoring**.

Step 5 In the right pane, click the **Services** tab, enter "InventoryNBI" in the search box, select **NCE/InventoryNBI/InventoryNBI_NBIInventoryService**, and click **Start**.

Step 6 On the **Services** tab page, check the status of the service. If **Status** is **Running**, the operation is successful.

----End

4.3.2 Stopping an NBI Service

If an NBI is no longer required, you can stop the corresponding NBI service on the **Panoramic Monitoring** page. By default, NBI services automatically start after system installation. Exercise caution when performing this operation, as this operation may affect system operations.

Procedure

The following uses NCE/InventoryNBI/InventoryNBI_NBIInventoryService as an example to describe how to stop an NBI service.

Step 1 Log in to the NCE management plane.

Open a browser, enter **https://***IP address of the management plane*:**31945** in the address bar, and press **Enter**.

NOTE

IP address of the management plane refers to the client login IP address configured on the OMP node.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.

Step 4 In the navigation pane, choose **Service Monitoring**.

Step 5 On the **Services** tab page,search for NBI services, select NCE/InventoryNBI/InventoryNBI_NBIInventoryService and click **Stop**.

Step 6 On the **Services** tab page, check the status of the service. If **Status** is **Not running**, the operation is successful.

----End

5 Commissioning

5.1 Invoking the REST APIs of NCE with Insomnia

Insomnia is a free open-source desktop API client for invoking REST APIs. For details about this tool, visit **https://insomnia.rest/**.

After installing Insomnia, perform the following steps to invoke simple REST APIs:

1. An NCE user for NBI system login authentication has been created. For details, see **5.1.1 Creating a User**.
2. Invoke the "Get Token" API to obtain a token for the session.
3. Invoke service APIs with this token to implement service functions.

5.1.1 Creating a User

This section describes how to create an NCE user and bind the user to an NCE role.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the management plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter the username and password, and click **Log In**.

Step 3 Open the Security Management app and choose **User Management** from the main menu.

Step 4 Choose **Users** from the navigation pane. On the page that is displayed, click **Create**.

Step 5 Set user information as prompted and click **Next**.

NOTE

Set **Type** to **Third-party system access** and clear the **Change the password at the first login** check box in advanced settings.

Step 6 Configure the default role **NBI User Group** for NBI users and click **Next**.

Table 5-1 Roles and their operation permissions

Role	Subclass	Operation Permission	Description
NBI User Group	API Management	Perform GET operation	Provides permission to invoke GET APIs.
		Perform POST operation	Provides permission to invoke POST APIs.
		Perform PUT operation	Provides permission to invoke PUT APIs.
		Perform DELETE operation	Provides permission to invoke DELETE APIs.
		Perform PATCH operation	Provides permission to invoke PATCH APIs.

Step 7 Click **OK**.

----End

5.1.2 Installing and Configuring Insomnia

Insomnia is a powerful desktop API client that supports basic invocations of REST APIs. This section uses Insomnia 6.0.1 as an example.

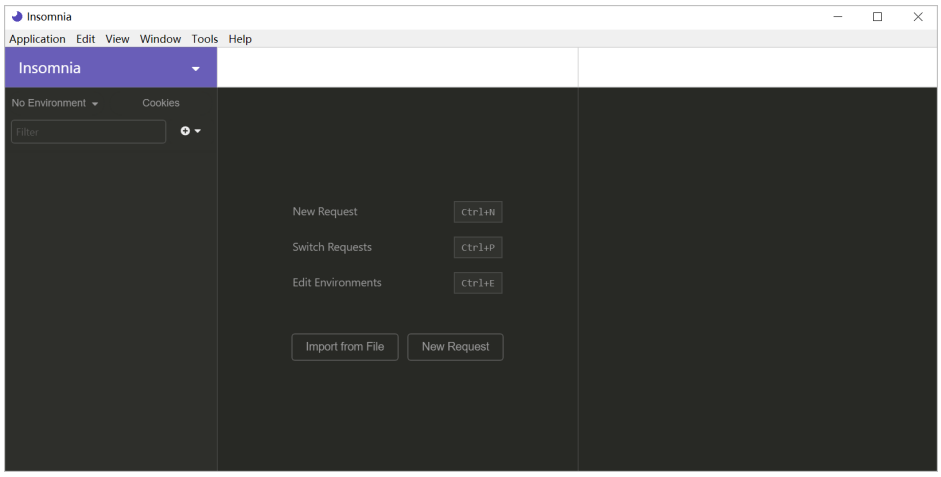
Procedure

Step 1 Obtain the latest Insomnia from **https://insomnia.rest/download/core/?** and install it on the local PC.

NOTE

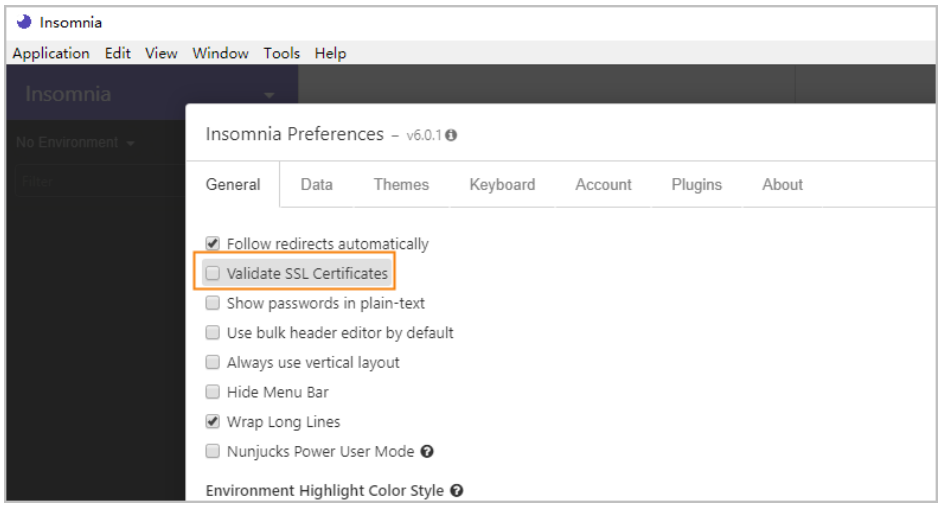
Insomnia has three editions: Free, Plus, and Team. Download the Free edition.

Step 2 Open Insomnia.



Step 3 Configure one-way authentication.

1. Choose **Application** > **Preferences** from the main menu of Insomnia.
2. Clear the check box before **Validate certificates**.



----End

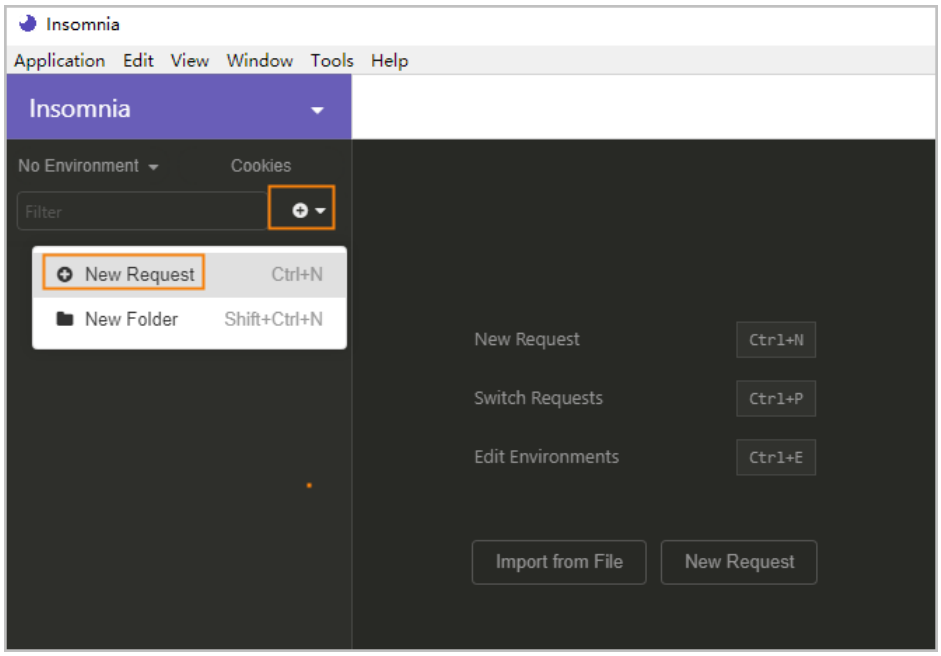
5.1.3 Obtaining a Token

Huawei NCE accepts REST requests from authenticated users only. You need to obtain a token from NCE for authentication upon subsequent invocations of open APIs.

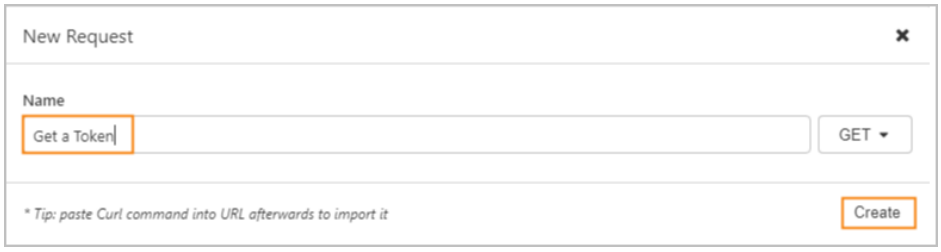
Procedure

Step 1 Open Insomnia.

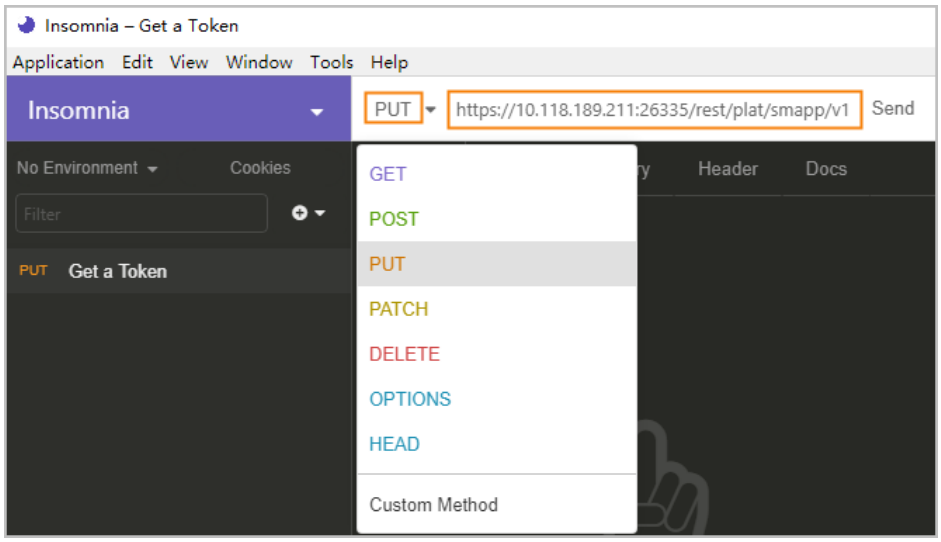
Step 2 Click  and choose **New Request**.



Step 3 In the **New Request** dialog box, set **Name** to **Get a Token** and click **Create**.



Step 4 Set the method to **PUT** and enter this URL next to it: **https://***floating IP address of Common_Service nodes***:26335/rest/plat/smapp/v1/sessions**.

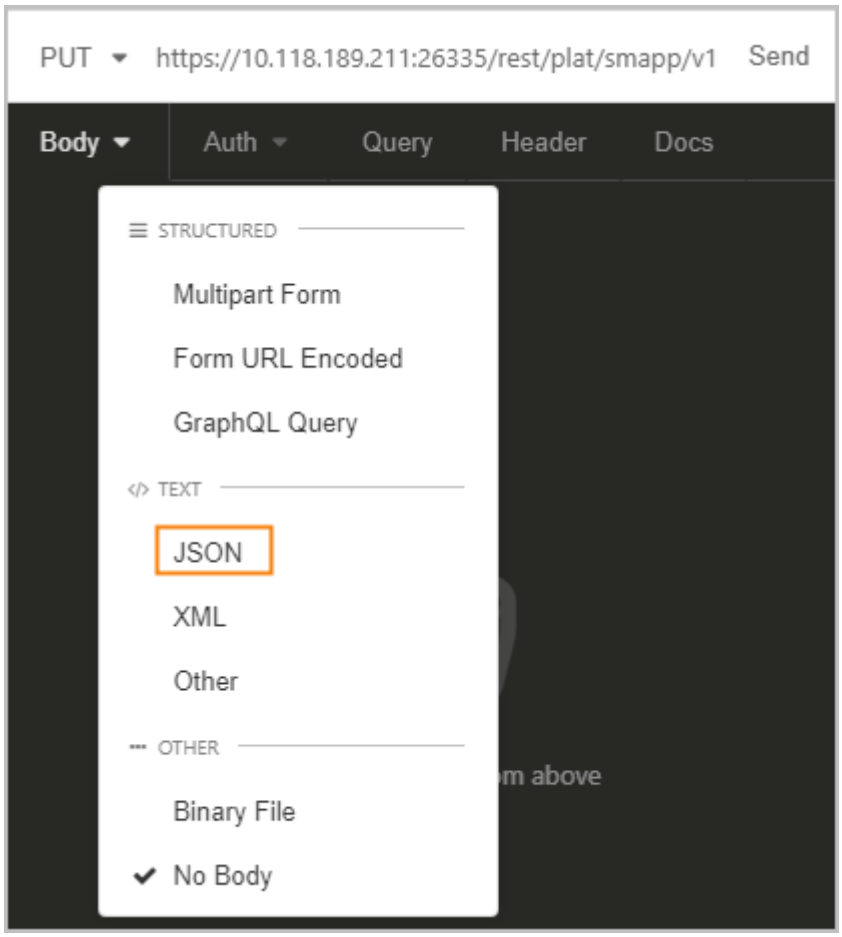


NOTE

Replace *floating IP address of Common_Service nodes* and **26335** with the actual address and port that NCE uses for northbound communication.

Step 5 Set body parameters.

On the **Body** tab page, select the **JSON** format.



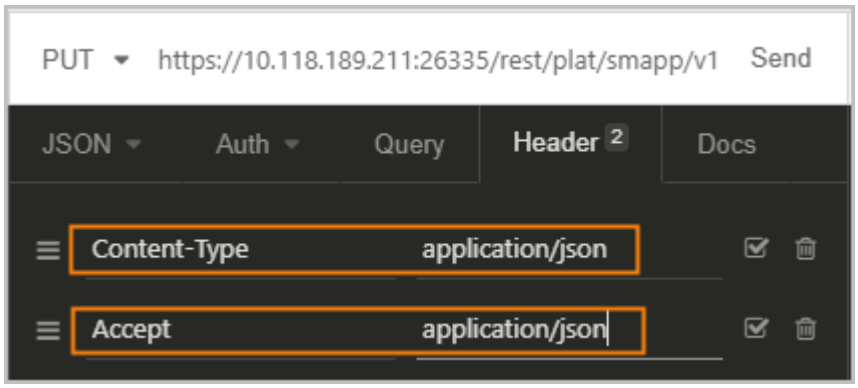
In the lower pane, set request body parameters. (Set **userName** to the northbound user created in **5.1.1 Creating a User**. Set **value** to the password for the northbound user.)

```
{
"grantType": "password",
"userName": "***",
"value": "********"
}
```

Step 6 Set header parameters.

On the **Header** tab page, set the following parameters:

```
Content-Type: application/json
Accept: application/json
```

Step 7 Click **Send**.

Insomnia sends a "Get a Token" request to NCE. Then NCE returns status code 200 and a token in **accessSession**. This token will be used as a credential for invoking other APIs.

Figure 5-1 Success response

----End

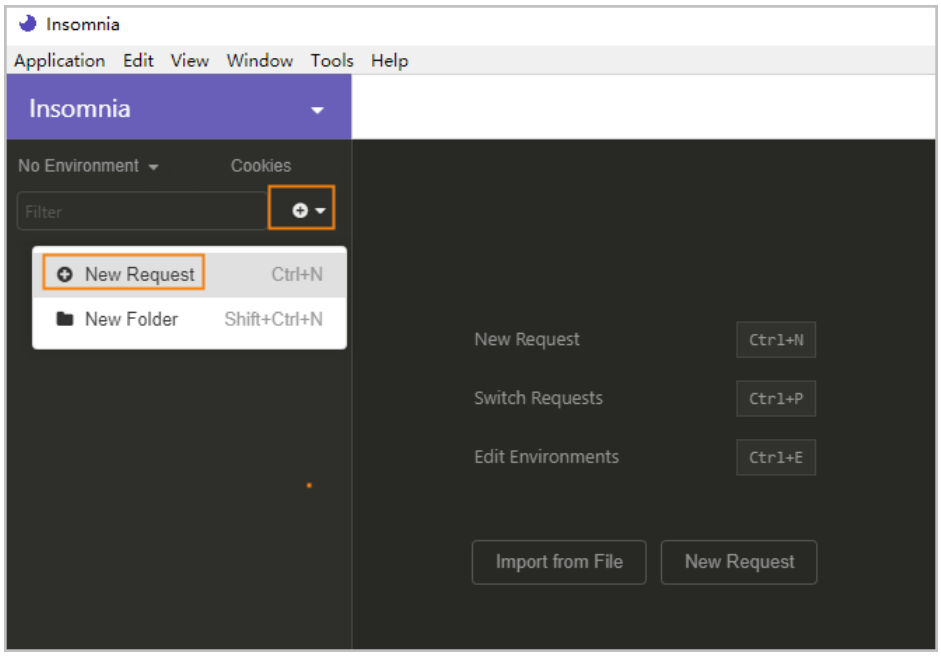
5.1.4 Querying NE Information

This section describes how to call interfaces through Insomnia to query all NE information, including NE IP addresses, names, and types.

Procedure

Step 1 Open Insomnia.

Step 2 Click  and choose **New Request**.



Step 3 In the **New Request** dialog box, set **Name** to **Query NE Information** and click **Create**.

Step 4 Set the method to **GET** and enter this URL next to it: **https://***floating IP address of Common_Service nodes***:26335/restconf/v2/data/huawei-nce-resource-inventory:network-elements**.

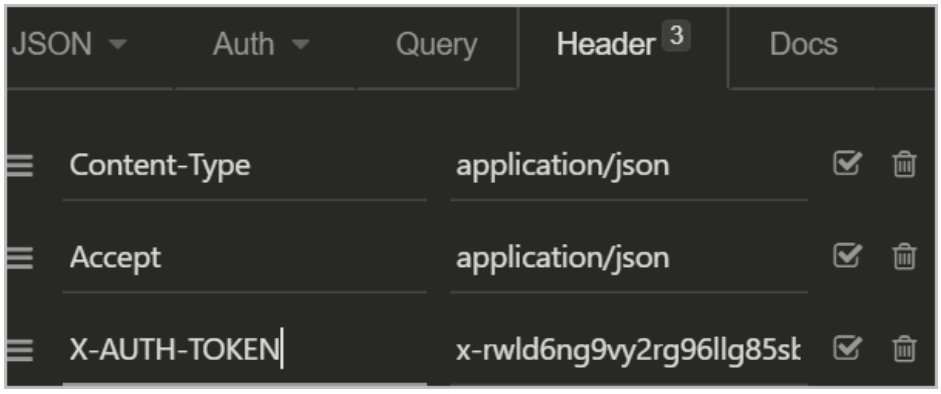
NOTE

Replace *floating IP address of Common_Service nodes* and **26335** with the actual address and port that NCE uses for northbound communication.

Step 5 Set header parameters.

On the **Header** tab page, set the following parameters:

```
Content-Type: application/json
Accept: application/json
X-AUTH-TOKEN: x-rwld6ng9vy2rg96llg85sbdisbmrfw1gdfamaoepoahcaq2nliams8s8epapiofx2r5druhi5g7wmmjzc5btftlduo7w88bybuqp7xmlup9htd5gpg4bmmrufvnt4aan
```



Step 6 Click **Send**.

Insomnia sends a "Query NE Information" request to NCE. Then NCE returns status code 200 and the following NE information:


```
{
 "network-elements": {
  "network-element": [
   {
    "res-id": "5977807f-a6d5-11ea-bc31-286ed4890a8c",
    "ip-address": "10.118.135.4",
    "is-gateway": -1,
    "dev-sys-name": "10.118.135.4",
    "physical-id": 1,
    "container": true,
    "patch-version": "SPH207",
    "location": "shenzhen? ? ?",
    "product-name": "MA5600T",
    "ref-parent-subnet": "b3131aeb-a6d5-11ea-bc31-286ed4890a8c",
    "software-version": "MA5600V800R018C10,SPH207",
    "manufacturer": "HuaWei",
    "remark": "",
    "name": "10.118.135.4",
    "roles": [
     "OLT"
    ],
    "detail-dev-type-name": "MA5600T",
    "communication-state": "0",
    "alias": "",
    "sn": "029937T0E7044610",
    "admin-status": "active",
    "mac": "04-f9-38-ca-fe-d5",
    "create-time": 1591324584000,
    "last-modified": 1591432458751
   },
   {
    "res-id": "b3b85bad-a6d5-11ea-bc31-286ed4890a8c",
    "ip-address": "10.12.12.12",
    "is-gateway": -1,
    "physical-id": 1,
    "container": false,
    "patch-version": "",
    "location": "",
    "product-name": "MDU",
    "ref-parent-subnet": "b386eb6c-a6d5-11ea-bc31-286ed4890a8c",
    "software-version": "MDU",
    "manufacturer": "HuaWei",
    "remark": "",
    "name": "10.12.12.12",
    "roles": [
     "MXU"
    ],
    "detail-dev-type-name": "MDU",
    "communication-state": "1",
    "alias": "",
    "admin-status": "inactive",
    "create-time": 1591324736000,
    "last-modified": 1591432458718
   },
   ...
  ]
 }
}
```


----End

5.2 Commissioning APIs in cURL Command Mode (Euler)

cURL is a file transfer tool that uses URL rules to work on the CLI in Euler. By using the cURL command, you can simulate the process of a client calling the API of a server.

Prerequisites

- You have completed REST interface interconnection.
- You have obtained the user name and password for logging in to Euler.

Procedure

Step 1 Log in to Euler.

Step 2 (Optional) Run the following command to view cURL parameters and their meanings:

```
curl --help
```

Step 3 Run the following commands to simulate API calling:

```
curl -v -k -H "Content-type:application/json" -X PUT -d '{ "grantType": "password", "userName": "xxx", "value": "********"}' https://10.118.187.40:26335/rest/plat/smapp/v1/sessions
```

NOTE

The API URL, token, IP address, and port number in the cURL command are only examples. Replace them with actual data to complete API calling. The IP address must be the floating IP address of the northbound API gateway, and the port number must be fixed at 26335.

If the response message contains the following information, the API is successfully called. If another status code, such as 404, is displayed, locate and rectify the fault based on the description of the status code.

```
HTTP/1.1 200 OK
{"accessSession":"x-496lnyiooaimepmmpi6roaobbw88vvvu8a6lmoc7fu2ofusale6r1c09heal44fvukc7epbyteqr2q09liermntg3s1cml04sb2lkbenpimofuvubxanil88uokaryvu","roaRand":"a92f67ff25a1073919d70f68b1bbca4247b635914ba4aa23","expires":1800,"additionalInfo":null}
```

----End

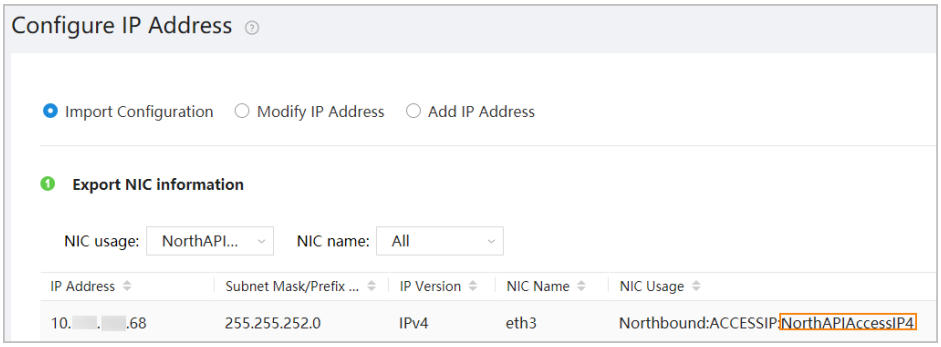
6 General Operations

6.1 Checking the Northbound IP Address

This section describes how to check the northbound IP address used for interconnecting with the OSS.

Procedure

- In the Manager scenario, it is the NorthAPIAccessIP address of the NMS_Server node.
  a. Log in to the NCE management plane.
     Open a browser, enter **https://*IP address of the management plane*:31945** (such as **https://10.10.10.12:31945**) in the address bar, and press **Enter**. On the page that is displayed, enter a username and password and click **Log In**.
  b. Choose **Maintenance** > **Network Configuration** > **Configure IP Address** from the main menu.
  c. Click **Import Configuration**. In the **Export NIC information** area, set **NIC Usage** to **NorthAPIAccessIP4**.
  d. The displayed IP address is the NorthAPIAccessIP address.



If no NorthAPIAccessIP address is displayed or the IP address is not the planned one, correct the IP address by referring to "Management and Maintenance > Administrator Guide > Systerm Configuration > Network Configuration" in *iMaster NCE Product Documentation (Project Deployment & System Maintenance, Arm)* or *iMaster NCE Product Documentation (Project Deployment & System Maintenance, x86)*.

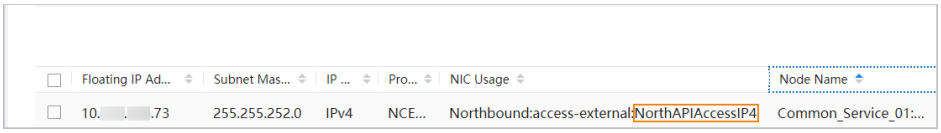
- In the Manager+Controller+Analyzer scenario without IP address convergence, it is the NorthAPIAccessIP4 address of the Common_Service node.

  a. Log in to the NCE management plane.

  Open a browser, enter **https:***//IP address of the management plane*:**31945** (such as **https://10.10.10.12:31945**) in the address bar, and press **Enter**. On the page that is displayed, enter a username and password and click **Log In**.

  b. Choose **Maintenance** > **Network Configuration** > **Configure Floating IP Address** from the main menu.

  c. In the floating IP address list, find the floating IP address whose **NIC Usage** contains **NorthAPIAccessIP4**.



If no floating NorthAPIAccessIP address is displayed or the IP address is not the planned one, correct the IP address by referring to "Management and Maintenance > Administrator Guide > Systerm Configuration > Network Configuration" in *iMaster NCE Product Documentation (Project Deployment & System Maintenance, Arm)* or *iMaster NCE Product Documentation (Project Deployment & System Maintenance, x86)*.

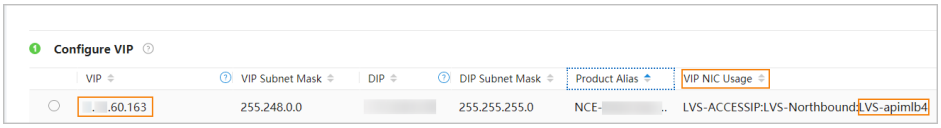
- In the Manager+Controller+Analyzer scenario with IP address convergence, it is the LVS-apimlb IP address of the GW node.

  a. Log in to the NCE management plane.

  Open a browser, enter **https:***//IP address of the management plane*:**31945** (such as **https://10.10.10.12:31945**) in the address bar, and press **Enter**. On the page that is displayed, enter a username and password and click **Log In**.

  b. Choose **Maintenance** > **Global Load Balancing** > **Configure Global Load Balancing** from the main menu.

  c. In the **Configure VIP** area, find the IP address whose **VIP NIC Usage** contains **LVS-apimlb**.



If no LVS-apimlb IP address is displayed or the IP address is not the planned one, correct the IP address by referring to "Management and Maintenance > Administrator Guide > Systerm Configuration > Network Configuration" in *iMaster NCE Product Documentation (Project Deployment & System Maintenance, Arm)* or *iMaster NCE Product Documentation (Project Deployment & System Maintenance, x86)*.

6.2 Security Configurations of the REST NBI

Properly configuring the REST NBI will facilitate data exchange with third-party systems. Using the HTTP protocol to communicate with third-party systems may pose security risks. To mitigate these risks, it is advisable to use the HTTPS protocol instead. The detailed configuration method is available in **3.5 Configuring the HTTP or HTTPS Protocol**.

Refer to **6.3.2 Checking Service Configurations** if you need to check for risks in the security configurations of the REST NBI.

6.3 Security Configurations of the Northbound SFTP Protocol

The security configuration function of NCE supports risk check and baseline management for service configuration items.

The northbound SFTP protocol involves these service configuration items: **Northbound Inventory Service - Security Configuration of SFTP** and **Northbound Notification Service - Security Configuration of SFTP**

Refer to **6.3.1 Managing Baselines** if you need to view or modify the risk levels and baselines of these items.

Refer to **6.3.2 Checking Service Configurations** if you need to check for risks in or modify these items.

6.3.1 Managing Baselines

If the existing baselines do not meet service requirements, security administrators can modify the risk levels and baselines (such as protocols, keys, or algorithms) of service configuration items on the page for managing baselines. In addition, the values in baselines of service configuration items can be restored to the default settings.

Procedure

Step 1 Open the Security Management app and choose **Security Configuration Check** > **Application Security** from the main menu.

Step 2 In the navigation pane, choose **Baseline Management**.

Step 3 On the **Baseline Management** page, click the name of the desired service configuration item to view the baseline of the service configuration item.

Step 4 Click **Modify** in the **Operation** column of the row that contains the desired service configuration item to modify the baseline and change the risk level.

NOTE

- For service function security, you are advised to configure baselines of secure protocols, keys, and algorithms for the service configuration items.
- Click **Restore Defaults** to restore the baseline of service configuration items to the default settings.

Step 5 Click **OK**.

The application security function will check for risks of protocols, keys, and algorithms used by service configuration items based on the configured baselines, and provide risk warnings and rectification suggestions.

----End

6.3.2 Checking Service Configurations

Security administrators can configure check policies based on service security requirements to periodically check whether protocols, keys, and algorithms used by services meet the baselines, and rectify the risks based on the check results. To meet special requirements such as compatibility requirements, you can configure insecure protocols, keys, and algorithms on the panel for risk details. Exercise caution when performing this operation. For service function security, you are advised to use secure protocols, keys, and algorithms.

Prerequisites

You have logged in to the O&M plane as a security administrator.

Procedure

Step 1 Open the Security Management app and choose **Security Configuration Check** > **Application Security** from the main menu.

Step 2 On the **Configuration Check** page, check a single item or check items in batches as required.

- Single item check

  Click **Check** in the **Operation** column of the row that contains the required item.
- Batch check

  Click **Check Now** to check items (except those added to the whitelist).
- Daily check

  Click **Set Check Time** and set the daily check time. The application security function automatically checks service configuration items every day based on the set time.

Step 3 View the check results.

- After the check is complete, view the results in the **Check Result** column.
- In the upper part of the **Configuration Check** page, view the result distribution charts of all check items so that you can learn about the overall risk information.

Step 4 Click the name of a desired configuration item. On the panel that is displayed, view the details about the risk. You can rectify the risk based on the suggestions.

Step 5 **Optional:** If **Configuration Item** can be set on the panel of risk details, set **Configuration Item** based on site requirements and click **Save**.

NOTE

If the modified value contains insecure protocols, keys, or algorithms, security risks may occur. Exercise caution when performing this operation. For service function security, you are advised to use secure protocols, keys, and algorithms.

----End

Related Tasks

- Adding an item to the whitelist: If a service configuration item does not have security risks or is not used, click **Add to Whitelist** in the **Operation** column of the row that contains the item to add it to the whitelist. The application security function will exclude whitelisted items when performing the security check to improve the check efficiency.
- Removing an item from the whitelist: If the security check needs to include a whitelist item, click **Remove from Whitelist** in the **Operation** column of the row that contains the item.

7 Privacy Data Protection

NCE is responsible for protecting users' personal data and privacy.

The REST NBI may involve the following sensitive and personal data, which requires proper protection. The protection measures are also listed in **Table 7-1**.

Table 7-1 Privacy data list

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
tel-number	Telephone number.	• Port inventory files exported through NBIs • Port resource inventory queried through NBIs	REST	• This field is returned upon the export of port inventory files. • This field is returned upon the query of port resource inventory.	• Loganonymization • Interface authentication • Encrypted SSL/HTTPS channel	The data exists in the process of exporting port inventory files or querying port resource inventory through NBIs.

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
sn	Serial number of NE.	• NE inventory files exported through NBIs • NE resource inventory queried through NBIs	REST	• This field is returned upon the export of NE inventory files. • This field is returned upon the query of NE resource inventory.	• Log anonymization • Interface authentication • Encrypted SSL/HTTPS channel	The data exists in the process of exporting NE inventory files or querying NE resource inventory through NBIs.

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
mac	MAC address of NE.	• NE inventory files exported through NBIs • NE resource inventory queried through NBIs	REST	• This field is returned upon the export of NE inventory files. • This field is returned upon the query of NE resource inventory.	• Log anonymization • Interface authentication • Encrypted SSL/HTTPS channel	The data exists in the process of exporting NE inventory files or querying NE resource inventory through NBIs.

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
sn	Serial number of ONU.	• ONU inventory files exported through NBIs • ONU resource inventory queried through NBIs	REST	• This field is returned upon the export of ONU inventory files. • This field is returned upon the query of ONU resource inventory.	• Log anonymization • Interface authentication • Encrypted SSL/HTTPS channel	The data exists in the process of exporting ONU inventory files or querying ONU resource inventory through NBIs.

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
mac	MAC address of ONU.	• ONU inventory files exported through NBIs • ONU resource inventory queried through NBIs	REST	• This field is returned upon the export of ONU inventory files. • This field is returned upon the query of ONU resource inventory.	• Log anonymization • Interface authentication • Encrypted SSL/HTTPS channel	The data exists in the process of exporting ONU inventory files or querying ONU resource inventory through NBIs.

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
loid	ONU authentication information	• ONU inventory files exported through NBIs • ONU resource inventory queried through NBIs	REST	• This field is returned upon the export of ONU inventory files. • This field is returned upon the query of ONU resource inventory.	• Log anonymization • Interface authentication • Encrypted SSL/HTTPS channel	The data exists in the process of exporting ONU inventory files or querying ONU resource inventory through NBIs.

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
name	Customer name.	• Customer inventory files exported through NBIs • Customer resource inventory queried through NBIs	REST	• This field is returned upon the export of customer inventory files. • This field is returned upon the query of customer resource inventory.	• Log anonymization • Interface authentication • Encrypted SSL/HTTPS channel	The data exists in the process of exporting customer inventory files or querying customer resource inventory through NBIs.

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
remark	Remark of customer.	• Customer inventory files exported through NBIs • Customer resource inventory queried through NBIs	REST	• This field is returned upon the export of customer inventory files. • This field is returned upon the query of customer resource inventory.	• Log anonymization • Interface authentication • Encrypted SSL/HTTPS channel	The data exists in the process of exporting customer inventory files or querying customer resource inventory through NBIs.

The REST NBI compliant with the TMF model may involve the following sensitive and personal data, which requires proper protection. The protection measures are also listed in **Table 7-2**.

Table 7-2 Privacy data list

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
customer	Customer name.	• Trail created on the NCE O&M plane • Trail created through the NBI	REST	• Upon a trail query, data is returned in the interface response. • During path creation, data is filled in the interface request.	• SSL encrypted transmission • Log anonymization	The data exists in the process of creating and querying trails through the interface.
telNumber	Telephone number.	• Create a POTS user through the NBI. • Query a specified POTS user through the NBI. • Query a specified POTS user through the NBI.	REST	• Delivered parameter for creating a POTS user. • Return parameter for obtaining a specified POTS user. • Delivered parameter for modifying the attributes of a POTS user.	• SSL encrypted transmission • Log anonymization	The data exists in the process of creating, querying, and modifying POTS user information.

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
registrationId	Registration ID.	• Query a specified POTS user through the NBI. • Modify a subnet interface through the NBI. • Query RU objects managed by NEs through the NBI. • Query ONT details by OLT, PON, and ONT through the NBI.	REST	• Delivered parameter for creating a subnet. • Delivered parameter for modifying a subnet. • Delivered parameter for querying RU objects managed by NEs. • Delivered parameter for querying ONT details.	• SSL encrypted transmission • Log anonymization	This data exists in the process of creating and modifying subnets, querying RU objects managed by NEs, and querying OTN details.

Data Field	Description	Data Source	Data Application Scope	Handling Method	Protection Measure	Data Life Cycle
password	Register password.	• Query a specified POTS user through the NBI. • Modify a subnet interface through the NBI. • Query RU objects managed by NEs through the NBI. • Query ONT details by OLT, PON, and ONT through the NBI.	REST	• Delivered parameter for creating a subnet. • Delivered parameter for modifying a subnet. • Delivered parameter for querying RU objects managed by NEs. • Delivered parameter for querying ONT details.	• SSL encrypted transmission • Log anonymization	This data exists in the process of creating and modifying subnets, querying RU objects managed by NEs, and querying OTN details.

8 FAQs

8.1 How Do I Customize the REST NBI?

Refer to the following procedure if you need to customize the scenario, alarm settings, or inventory settings of the REST NBI.

Procedure

Step 1 Log in to the NCE O&M plane.

Open a browser, enter **https://***IP address of the O&M plane*:**31943** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 4 Perform operations based on customization needs.

- Customizing the scenario

  In the navigation pane, choose **REST NBI** > **Common Settings**. In the right pane, set **Scenario name**.

- Customizing alarm settings

  In the navigation pane, choose **REST NBI** > **Alarm Settings**. In the right pane, expand **Advanced Settings**.

- Customizing inventory settings

  In the navigation pane, choose **REST NBI** > **Custom Settings**. In the right pane, expand **Advanced Settings**.

Step 5 Set the following parameters based on customization needs.

Table 8-1 Northbound parameters

Customization Needs	Parameter Name	Description	Value Range	Default Value
Scenario	Scenario name	Name of the scenario. If there is no custom scenario, retain the default value **COMMON**. **NOTE** If this parameter is set to **COMMON_WITH_DN**, the **distinguished-name** field will be added to the responses of the NE, board, port, and link inventory export and query interfaces.	--	COMMON

Customization Needs	Parameter Name	Description	Value Range	Default Value
Alarm settings	Iterator destroy time (hour)	Time when the lifecycle of an iterator in the system expires. The default value is 10 hours.	Integer from 1 to 10	10
	Number of cached alarms	Total number of cached alarms allowed by the system.	Integer from 10000 to 50000	10000
	Number of iterators	Total number of iterators supported by the system. The default value is 10.	Integer from 1 to 1000	200
	The length of Object Info in Log	Limits the length of logs to be printed.	Integer from 100 to 99999999	10000
	Is verify the time format	Whether to check the time format delivered (UTC time or local time).	• **1** (Yes) • **0** (No)	0
Inventory settings	Export third-party controller data	If NCE-Super is deployed together with NCE-T or NCE-IP, NCE-Super can obtain third-party controller data, eliminating the need to export third-party controller data through NBIs. Therefore, set this parameter to **No**.	• Yes • No	Yes

----End

8.2 How Do I Enable the Domain-based Function for New Users?

Question

If different users configure inventory or alarm tasks, how do I enable the domain-based function to limit each user to resources within their respective management domains?

Answer

After the domain-based function is enabled, different users can only perform operations on resources within their respective management domains.

Procedure

Step 1 Create a user who has permission on a specific management domain.

1. Create a role with specific managed objects and operation rights.
2. Create a user.
3. Bind the user to the role created in **Step 1.1**.

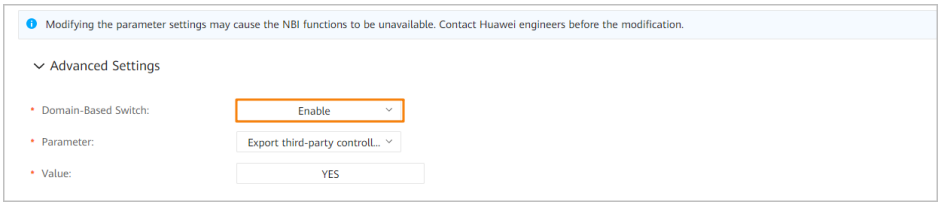
For details, see **3.10 Creating a REST NBI User for an OSS**.

Step 2 Enable the domain-based function.

NOTE

- Only local users can enable the domain-based function on the NCE O&M plane.
- However, once enabled, the domain-based function is also available to third-party users.
- The domain-based function can be used only when **Scenario name** is **COMMON** (default value).

1. Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.
2. In the navigation pane, choose **REST NBI** > **Custom Settings**.
3. On the **Custom Settings** page, expand **Advanced Settings**.
4. In the **Advanced Settings** area, set **Domain-Based Switch** to **Enable** and click **Save**.



NOTE

- Before the domain-based function is enabled, inventory and alarm tasks are performed for network-wide resources. That is, all users can perform operations on network-wide resources.
- After the domain-based function is enabled, inventory and alarm tasks are limited to resources within users' management domains. That is, users can only perform operations on resources within their respective management domains.
  - Domain-based function for inventory tasks: Only subnets, NEs, boards, ports, slots, optical NEs, links, and chassis are supported.
  - Domain-based function for alarm tasks: Only optical NEs, NMSs, subracks, NEs, boards, ports, ONUs, and OTN trails are supported.
  - Users can view resources within their management domains on the NCE O&M plane: Open the Security Management app and choose **User Management** from the main menu. In the navigation pane, choose **Users**. On the page that is displayed, click a username to go to the user details page, and click the **Managed Objects** tab.
- Non-admin users will be prompted for secondary authorization authentication when they disable the domain-based function. They need to enter the name and password of the **admin** user or another user who has the application-level **Secondary Authorization Authentication** permission.

Step 3 Create an inventory or alarm task as the new user created in **Step 1**.

----End

8.3 How Do I Query the IP Address of a Node?

Symptom

During fault diagnosis, the management IP address needs to be queried based on the name of the node where a service resides.

Procedure

The following describes how to query the management IP address of a node:

Step 1 Log in to the NCE management plane.

Open a browser, enter **https://***client login IP address of the management plane*:**31945** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu. In the navigation pane, choose **Node Monitoring**.

Step 4 In the node list, find the node that you want to query.

Step 5 Click the node name. On the top of the page for node details, the IP address is the management IP address of the node.

----End

8.4 How Do I Query the Floating IP Address of a Node?

Symptom

During fault diagnosis, the floating IP address needs to be queried based on the name of the node where a service resides.

Procedure

The following describes how to query the floating IP address of the node:

Step 1 Log in to the NCE management plane.

Open a browser, enter **https://***client login IP address of the management plane*:**31945** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

Step 3 Choose **Maintenance** > **Network Configuration** > **Configure Floating IP Address** from the main menu.

Step 4 In the floating IP address list on the **Configure Floating IP Address** page, view the floating IP address in the row that contains the corresponding node.

----End

8.5 How Do I Obtain and Configure a Security Certificate for the REST Interfaces based on the TMF Model?

When you use the REST interfaces based on the TMF model, you need to configure the REST interfaces by referring to section "Configuring NBI Security Connections" in *iMaster NCE XML NBI User Guide* of NCE of the corresponding version.

8.6 How Do I Generate a Private Key File?

Question

How do I generate an SFTP private key file when I use the SFTP protocol and select the public key authentication mode?

Answer

NOTICE

- For security purposes, use 3072-bit or longer RSA keys when the public key algorithm is ssh-rsa.
- For security purposes, you are recommended to set a password for the private key, and the password is expected to meet the following rules: 1) Differ from the username and the reverse of the username. 2) Consist of at least eight characters. 3) Contain at least three types of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters (=~@#^*-_+ [{}];:./?).4) Not be composed of repeated strings of any length, for example, aaaaaaaa, abababab, or abcdabcd.

Step 1 Generate a key pair.

1. Use PuTTY to log in to the Common_Service node of the client as the **sopuser** user, and run the following command to switch to **ossuser**:

   su - ossuser

2. On the client, run the following command to go to **/home/ossuser**:

   cd /home/ossuser

3. (Optional) Check whether the **.ssh** folder exists in **/home/ossuser** on the client. If no, run the following command to create the **.ssh** folder. If yes, directly go to step 4.

   mkdir -p .ssh

4. Run the following command on the client to access the **.ssh** folder:

   cd .ssh

5. Run the following commands on the client to generate a key pair. (You do not need to enter the private key because it is stored in the default file **/home/ossuser/.ssh/id_rsa**, but need to enter the password for the private key at the "passphrase" prompt.)

   ssh-keygen -t rsa -b 3072

   ```
   Generating public/private rsa key pair.
   Enter file in which to save the key (/home/ossuser/.ssh/id_rsa):
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   ```

   If the following information is displayed, the operation is successful:

   ```
   Your identification has been saved in /home/ossuser/.ssh/id_rsa.
   Your public key has been saved in /home/ossuser/.ssh/id_rsa.pub.
   The key fingerprint is:
   SHA256:MsqgZE4l8+I9XzPV1LY+HVdK1ZFiLiBVBuYtUxFxUH8 ossuser@NMS-Server-01
   The key's randomart image is:
   +---[RSA 3072]----+
   |         .+oO*o .=|
   |       .o.+ oo.o.|
   | o .    .+.oooo.E|
   |  =       =..o..o|
   | =..  o S. .....|
   |*.oo . o.   . . o|
   |.o oo  +     o . |
   |    o . o     .  |
   |     .           |
   +----[SHA256]-----+
   ```

Step 2 Run the following command to exit from the **ossuser** user:

exit

----End

8.7 How Do I Configure Public Key Authentication for the SFTP Server?

To further enhance the security of the SFTP protocol, the REST NBI allows users to configure public key authentication for the remote SFTP server. The functions involved by the REST NBI for uploading files through SFTP include current alarm query, historical alarm query, and scheduled inventory export. The following describes how to configure public key authentication for uploading files to the SFTP server through the REST NBI.

NOTICE

For security purposes, the SFTP upload function of the northbound notification and inventory service supports only the following algorithms by default during SSH connection:

- Algorithms supported in fresh installation scenarios(notification):
  - Data encryption algorithms: aes128-ctr, aes192-ctr, and aes256-ctr
  - Key exchange algorithms: diffie-hellman-group-exchange-sha256, diffie-hellman-group15-sha512, diffie-hellman-group16-sha512, diffie-hellman-group17-sha512, diffie-hellman-group18-sha512, curve25519-sha256, and curve25519-sha256@libssh.org
  - Host public key algorithms: ssh-ed25519, ssh-ed25519-cert-v01@openssh.com, rsa-sha2-256, and rsa-sha2-512
  - Message authentication algorithms: hmac-sha2-256, hmac-sha2-512, hmac-sha2-256-etm@openssh.com, and hmac-sha2-512-etm@openssh.com
- Algorithms supported in fresh installation scenarios(inventory):
  - Data encryption algorithms: AES128-CTR,AES192-CTR,AES256-CTR
  - Key exchange algorithms: diffie-hellman-group-exchange-sha256, diffie-hellman-group15-sha512, diffie-hellman-group16-sha512, diffie-hellman-group17-sha512, diffie-hellman-group18-sha512, curve25519-sha256
  - Host public key algorithms: ssh-ed25519, rsa-sha2-256, and rsa-sha2-512
  - Message authentication algorithms: hmac-sha2-256, hmac-sha2-512
- In upgrade scenarios, the algorithms in the source version are supported by default.
- You can view, check, and modify the security configurations of the SFTP server on the NCE O&M plane. Navigation Path: Open the Security Management app and choose **Security Configuration Check** > **Application Security** from the main menu. For example, to configure the SFTP algorithms of the northbound notification service, click **SFTP Security Configuration for the Northbound Notify Service**; to configure the SFTP algorithms of the northbound inventory service, click **SFTP Security Configuration for the Northbound Inventory Service.** For details, see **6.3 Security Configurations of the Northbound SFTP Protocol**.

Procedure

Step 1 (Optional) Log in to the SFTP server. If the **.ssh** folder does not exist in the home directory of the SFTP server, run the following commands to create it:

cd *FTPUSER_HOME*

mkdir -p .ssh

Step 2 (Optional) Log in to the SFTP server. If the **authorized_keys** file does not exist in *FTPUSER_HOME/***.ssh**, run the following commands to create it:

cd *FTPUSER_HOME/.ssh*

touch authorized_keys

NOTE

Step 1 and Step 2 are performed on the SFTP server. Set **FTPUSER_HOME** to the home directory of the SFTP server. For example, if the username of the SFTP server is **ossadm**, the home directory of the user is **/home/ossadm**.

Step 3 Copy the client's public key file **id_rsa.pub** to the SFTP server.

This file is located in **/home/ossuser/.ssh** on the Common_Service node of the client.

1. Use PuTTY to log in to the Common_Service node of the client as the **sopuser** user, and run the following command to switch to the **ossuser** user:

   su - ossuser

2. Run the following commands to copy **id_rsa.pub** to the SFTP server:

   cd /home/ossuser/.ssh

   scp id_rsa.pub *ftpuser*@*remote_host_ip*:*FTPUSER_HOME*/.ssh

   NOTE

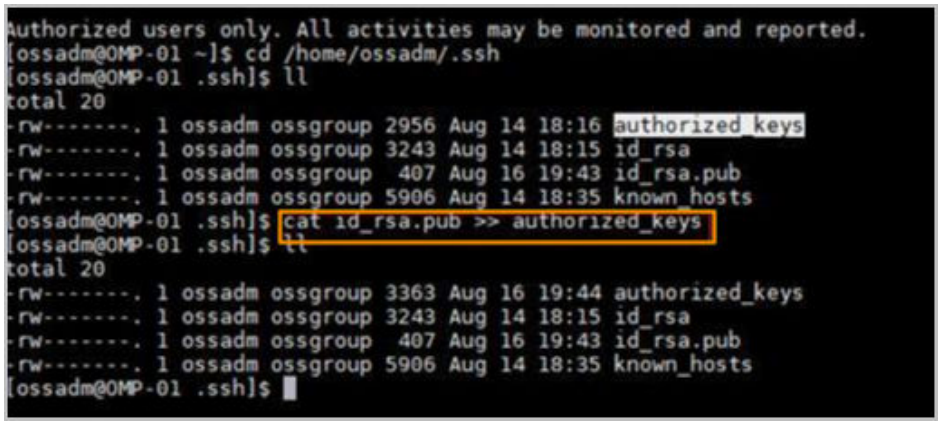
   - **ftpuser**: username for logging in to the SFTP server
   - **remote_host_ip**: IP address of the SFTP server

Step 4 Add the public key in the **id_rsa.pub** file on the SFTP server to the **authorized_keys** file.

Log in to the SFTP server and run the following commands to add the public key in the **id_rsa.pub** file to the **authorized_keys** file:

cd *FTPUSER_HOME*/.ssh

cat id_rsa.pub >> authorized_keys



NOTE

Step 4 needs to be performed on the SFTP server.

Step 5 Check whether key-based client login has been configured successfully.

Use PuTTY to log in to the Common_Service node of the client as the **sopuser** user, and run the following commands to check whether you can log in to the SFTP server with a key. If yes, the preceding configuration is successful and you can proceed to **Step 6**. Otherwise, reconfiguration is required.

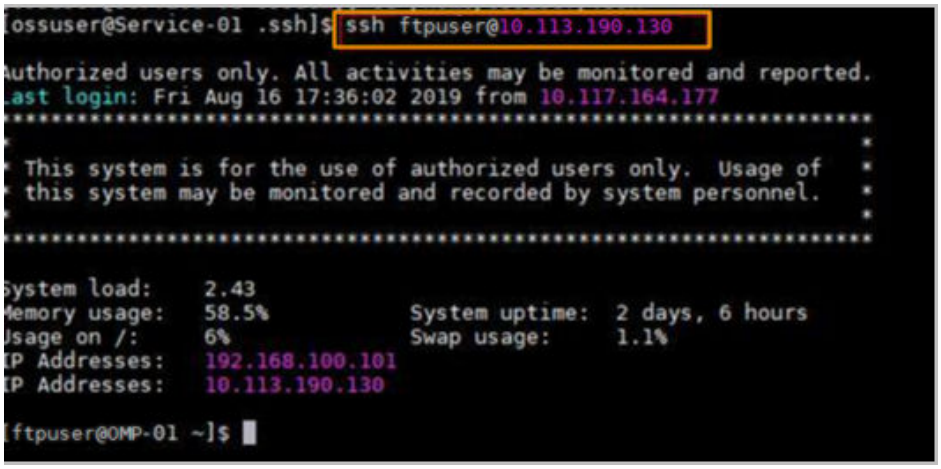
su - ossuser

```
Password:
```

ssh *ftpuser@remote_host_ip*

NOTE

- **ftpuser**: username for logging in to the SFTP server
- **remote_host_ip**: IP address of the SFTP server



Step 6 Modify file permissions.

Check whether the permissions of the client's **id_rsa** and **id_rsa.pub** files in **/home/ossuser/.ssh** and the server's **authorized_keys** file in *FTPUSER_HOME*/**.ssh** are 600. If not, change them to 600.

chmod 600 *file name*

NOTE

The northbound inventory service is deployed in cluster mode. To ensure that all inventory files can be uploaded to the SFTP server, perform the operations described in **8.6 How Do I Generate a Private Key File?** and **8.7 How Do I Configure Public Key Authentication for the SFTP Server?** on all Common_Service nodes of the client.

Step 7 (Optional) Run the following commands to import the key file for the notification service:

cd /opt/oss/NCE/apps/NBINotifyService/script

sh manageNotifyConfig.sh

If the following information is displayed, enter **SFTP_PRIVATE_KEY**:

```
[INFO] [2021-06-16 15:45:28,091] Please enter the item name which you want to modify: (s: save, q: quit)
SFTP_PRIVATE_KEY
```

Enter **1** and the key password.

```
[INFO] [2021-06-16 15:46:05,128] Please select the operation to be performed:
1. Configure SFTP private key
2. Delete SFTP private key
0. Exit
Enter a number (0-2):
1
[INFO] [2021-06-16 16:27:23,850] Enter the absolute path of the SFTP private key(0: Exit):
```



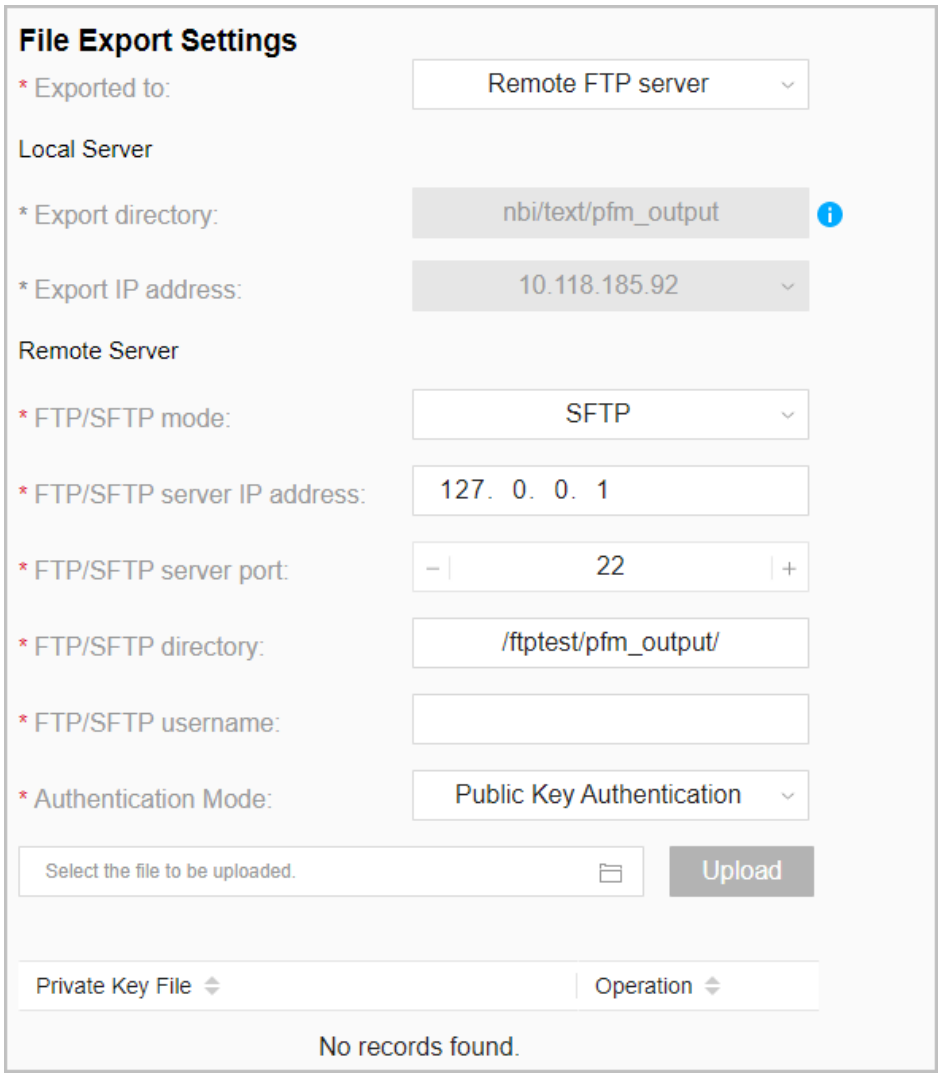
```
/home/ossuser/.ssh/id_rsa
[INFO] [2021-06-16 16:27:35,890] Enter the key password (0: Exit):

[INFO] [2021-06-16 15:46:42,442] Please enter the item name which you want to modify: (s: save, q: quit)
s
[INFO] [2021-06-16 15:46:45,058] Begin to update the xml configuration item value.
[INFO] [2021-06-16 15:46:45,327] The following configuration item values have been modified successfully!
SFTP_PRIVATE_KEY: is changed.
SFTP_PRIVATE_KEY_SECRET: is changed. ->********
[INFO] [2021-06-16 15:46:45,336] The SFTP private key file content has been saved. If the SFTP private key file is not deleted, the SFTP private key may be leaked. Are you sure you want to delete.(y: delete; n: not delete):
y
[INFO] [2021-06-16 15:53:25,340] The following configuration item values have been modified successfully!
```

NOTICE

Upgrade scenario: If you connect to the SFTP server in public key authentication mode, you are advised to generate a new private key file and use it to replace the original one to prevent security risks.

Step 8 (Optional) To upload inventory files to the SFTP server, you need to modify the following configuration items on NCE.

- Export mode settings



NOTE

- **Exported to**: **Remote FTP server**
- **FTP/SFTP mode**: **SFTP**
- **FTP/SFTP server IP address**: IP address of the SFTP server
- **FTP/SFTP server port**: **22**
- **Inventory FTP/SFTP upload directory**: directory on the SFTP server to which full export files are uploaded
- **Increment FTP/SFTP upload directory**: directory on the SFTP server to which incremental export files are uploaded
- **FTP/SFTP username**: username of the SFTP server
- **Authentication Mode**: **Public Key Authentication** (An SFTP private key file needs to be uploaded for authentication. For details about how to generate a private key file, see **8.6 How Do I Generate a Private Key File?**)

  After uploading an SFTP private key file:

  - If the private key file is encrypted, set **Encrypt private key** to **Yes** and enter the correct file password in the **Enter the private key password** dialog box.
  - If the private key file is not encrypted, set **Encrypt private key** to **No** and click **OK** in the **Enter the private key password** dialog box.

----End

8.8 How Do I Configure Fingerprint Authentication for the SFTP Server?

Question

How do I configure fingerprint authentication for the SFTP server through the NBI?

Answer

To further enhance the security of the SFTP protocol, the NBI allows users to configure fingerprint authentication for the remote SFTP server.

Step 1 Use PuTTY to log in to the client node as the **sopuser** user.

Step 2 Run the following command to switch to **ossuser**:

su - ossuser

Step 3 Run the following command to configure fingerprint authentication for the SFTP server:

cd /opt/oss/share/NCE/*{serviceName}*/conf

NOTE

Replace *{serviceName}* with the target feature name, for example, NBINotifyService for the alarm feature and NBIInventoryService for the inventory feature.

Check for the fingerprint file **known_hosts**. If it is present, fingerprint authentication has been enabled for the server and therefore you can directly go to **Step 4**. If it is not present, run the following command:

touch known_hosts

Step 4 Modify the file permission.

Within the client directory **/opt/oss/share/NCE/*{serviceName}*/conf**, change the permission of the **known_hosts** file to 640 if it is not 640 currently.

chmod 640 *filename*

Step 5 (Optional) If the host public key algorithm or the public key of the SFTP server has changed, delete the fingerprint record of the SFTP server to prevent connection issues.

1. Enter **vi known_hosts** to edit the fingerprint file.
2. Select the line corresponding to the SFTP server and enter **dd**.
3. Enter **:wq** to save the changes.

Step 6 (Optional) Disable fingerprint authentication for the SFTP server.

If you need to disable fingerprint authentication for the SFTP server, delete the fingerprint file by running the following command:

rm known_hosts

----End

8.9 How Do I Change the Startup Modes of NBI Processes?

Procedure

Step 1 Log in to the NCE management plane.

Open a browser, enter **https://***client login IP address of the management plane*:**31945** in the address bar, and press **Enter**.

Step 2 Enter the username and password, and click **Log In**.

Step 3 Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.

Step 4 In the navigation pane, choose **Service Monitoring**.

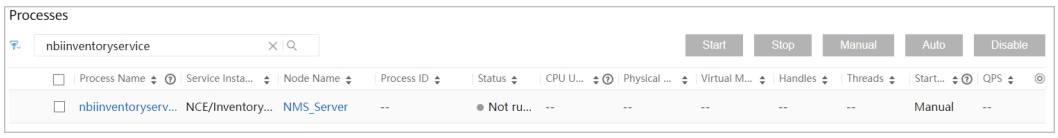
Step 5 Click the **Process** tab. The process list is displayed.

Step 6 Search for the nbiinventoryservice, nbinotifyservice, and nbiperformanceservice processes, and perform **Step 7** to **Step 9** for each of them.

Step 7 Select the process, click **Start** above the process list, and confirm the operation as prompted.

Step 8 Select the process, click **Auto** above the process list, and confirm the operation as prompted.

Step 9 Check that **Status** and **Startup Type** are **Running** and **Auto**, respectively.



----End

8.10 How Do I Enable or Disable Insecure Configurations of the RESTful Callback Interface?

When the NBI interconnects with a third-party system, protocols such as HTTPS required. For system security purposes, NCE supports secure configurations by default. To meet the requirements that some peer systems use insecure configurations, NCE provides the functions of enabling and disabling insecure parameter options. For security purposes, you are advised to use the secure parameter options provided by default.

Prerequisites

To enable HTTP, you have obtained the IP address of a node where the nbifrmconfigservice process instance of NBIFrm resides. For details, see **8.3 How Do I Query the IP Address of a Node?**.

Procedure

Step 1 Use PuTTY to log in to a node where the nbifrmconfigservice process instance of NBIFrm resides, as the **sopuser** user in SSH mode.

Step 2 Run the following command to switch to the **ossuser** user:

su - ossuser

```
Password: password for the ossuser user
```

Step 3 Run the following command to go to the target directory:

cd *installation directory*/**NCE/apps/NBIFrmConfigService/bin**

Step 4 Run the following commands to enable or disable insecure parameter options:

- Enabling insecure parameter options
  - To make the **Enable HTTP** parameter configurable in the **RESTful Callback** > **General Settings** area, perform the following operations:

    sh configTool.sh -u httpSwitch on

    Information similar to the following is displayed. Read the information carefully and confirm whether to continue.

    ```
    Http protocol is insecure. Are you sure to continue? [y/n]
    ```

    Enter **y** and press **Enter**.

    If information similar to the following is displayed, the command execution is successful. Otherwise, contact Huawei technical support.

    ```
    Update...
    success
    ```

  - To make the **Protocol type** parameter configurable on the **Server** tab page on the **FTP NBI** > **Local Server** page, perform the following operations:

    sh configTool.sh -u ftpServerEnable on

    Information similar to the following is displayed. Read the information carefully and confirm whether to continue.

    ```
    FTP protocol is insecure. Are you sure to continue? [y/n]
    ```

    Enter **y** and press **Enter**.

    If information similar to the following is displayed, the command execution is successful. Otherwise, contact Huawei technical support.

    ```
    Update...
    success
    ```

  - To make the **Protocol type** parameter configurable in the **Protocol Configuration** area on the **FTP NBI** > **Third-Party Server** page, perform the following operations:

    sh configTool.sh -u ftpOssEnable on

    Information similar to the following is displayed. Read the information carefully and confirm whether to continue.


```
FTP protocol is insecure. Are you sure to continue? [y/n]
```

Enter **y** and press **Enter**.

If information similar to the following is displayed, the command execution is successful. Otherwise, contact Huawei technical support.

```
Update...
success
```

- Disabling insecure parameter options
  - To make the **Enable HTTP** parameter unconfigurable in the **RESTful Callback** > **General Settings** area, run the following command:

    sh configTool.sh -u httpSwitch off

    If information similar to the following is displayed, the command execution is successful. Otherwise, contact Huawei technical support.

    ```
    Update...
    success
    ```

  - To make the **Protocol type** parameter unconfigurable on the **Server** tab page of the **FTP NBI** > **Local Server** page, run the following command:

    sh configTool.sh -u ftpServerEnable off

    If information similar to the following is displayed, the command execution is successful. Otherwise, contact Huawei technical support.

    ```
    Update...
    success
    ```

  - To make the **Protocol type** parameter unconfigurable in the **Protocol Configuration** area on the **FTP NBI** > **Third-Party Server** page, run the following command:

    sh configTool.sh -u ftpOssEnable off

    If information similar to the following is displayed, the command execution is successful. Otherwise, contact Huawei technical support.

    ```
    Update...
    success
    ```

----End

Related Commands

Command Function	Command	Description
Viewing RESTful protocol configurations	• **configTool.sh -l** • **configTool.sh --list**	None

Command Function	Command	Description
Modifying RESTful protocol configurations	• **configTool.sh -u** *config_name config_value* • **configTool.sh --update** *config_name config_value*	• *config_name*: Name of the configuration item. The option is as follows: **httpSwitch**: Specifies whether the **Enable HTTP** parameter is configurable on the **RESTful Callback** page. • *config_value*: Value of the configuration item. The options are as follows: – **on**: The **Enable HTTP** parameter is configurable on the **RESTful Callback** page. You can select **Yes** or **No**. – **off**: The **Enable HTTP** parameter is not configurable on the **RESTful Callback** page. You can select only the default option **No**.
Viewing FTP protocol configurations	• **configTool.sh -l** • **configTool.sh --list**	None

Command Function	Command	Description
Modifying FTP protocol configurations	• **configTool.sh -u** *config_name config_value* • **configTool.sh --update** *config_name config_value*	• *config_name*: Name of the configuration item. The options are as follows: – **ftpServerEnable**: Specifies whether the **Protocol type** parameter is configurable on the **FTP NBI > Local Server > Server** page. – **ftpOssEnable**: Specifies whether the **Protocol type** parameter is configurable on the **FTP NBI > Third-Party Server > Create** page. • *config_value*: Value of the configuration item. The options are as follows: – **ftpServerEnable**: The options can be **on** and **off**. The default value is **off**. – **on**: The **Protocol type** parameter is configurable on the **FTP NBI** > **Local Server** > **Server** tab page. You can select **FTP** or **SFTP**. – **off**: The **Protocol type** parameter is not configurable on the **FTP NBI** > **Local Server** > **Server** tab page. You can select only the default option **SFTP**. – **ftpOssEnable**: The options can be **on** and **off**. The default value is **off**. – **on**: The **Protocol type** parameter is configurable on the **FTP NBI** > **Third-Party Server** > **Create** page. You can select **FTP** or **SFTP**. – **off**: The **Protocol type** parameter is not configurable on the **FTP NBI** > **Third-Party Server** > **Create** page. You can select only the default option **SFTP**.

8.11 How Do I Transmit Data Without Using the IP Address Specified by the FTP Server?

Question

In passive FTP mode, the NBI uses the IP address specified by the FTP server by default during data transmission. How do I transmit data without using that address?

Answer

Disable the function of trusting the IP address returned by the server. Specifically, do as follows.

NOTICE

Running the **vi** command to modify system configuration files is a risky operation. Any misoperation may cause SSH login failure on nodes. Before that, contact Huawei engineers to confirm whether you can use the **vi** command.

The REST NBI involves NBIInventoryService and NBINotifyService. When taking the following procedure (which uses NBIInventoryService as an example), you need to update the service name in related commands and directories.

Procedure

Step 1 Use PuTTY to log in to all Common_Service nodes as the **sopuser** user.

Step 2 Run the following command to switch to the **ossuser** user:

su - ossuser

Step 3 Run the following command to go to **/opt/oss/NCE/apps/NBIInventoryService/bin**:

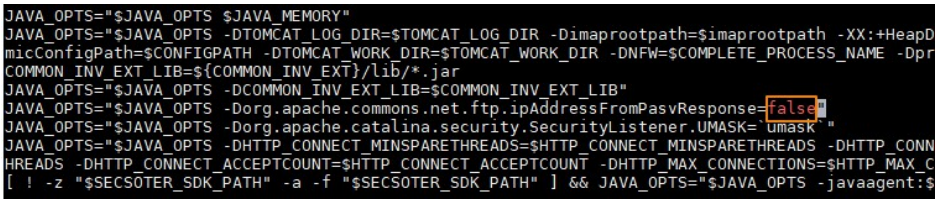
cd /opt/oss/NCE/apps/NBIInventoryService/bin

Step 4 Run the following command to open the **start.sh** file in the vi editor:

vi start.sh

Step 5 Press **/** in the vi editor to enter the last line mode. When the cursor jumps to the last line in the vi editor, enter **Dorg.apache.commons.net.ftp.ipAddressFromPasvResponse** and press **Enter**. The vi editor highlights the search result.

Step 6 Press **i** in the vi editor to enter the insert mode and change the value of **Dorg.apache.commons.net.ftp.ipAddressFromPasvResponse** from **true** to **false**. Then press **Esc** to exit the insert mode, enter **:wq!**, and press **Enter** to save the settings and close the vi editor.



Step 7 Run the following command to convert the **start.sh** file into the Unix format:

dos2unix start.sh

```
dos2unix:converting file start.sh to Unix format...
```

Step 8 Run the following command to exit from the **ossuser** user:

exit

Step 9 Log in to the management plane and restart NBIInventoryService.

----End

A Glossary

E

edge termination point	A termination point (TP) that is at the entrance or exit of a multi-layer subnetwork (such as add-drop or TPs that terminate topological links between two subnetworks).
element management system	A system used to manage a portion of a network which contains one or more multi-layer subnetworks. The EMS is used as the root of the naming tree in the NML-EML interface.
equipment	A manageable physical component of a network element, such as a circuit pack, fan, or any other type of replaceable unit within a network element.
equipment holder	A holder that represents resources of the network elements that are capable of holding other physical components. Specific resources that can be represented by an equipment holder include racks (bays), shelves, slots, and sub-slots.

L

Location	An area, position, or portion of space that somebody or something can occupy. It is further divided into a geographic place that relates to world-centric places and a local location that relates to locally defined coordinate systems.

M

managed element	EMS (management) view of a network element (NE).
multi-layer subnetwork	A MultiLayer Subnetwork represents the topology provided by the EMS system. The main services provided within a MultiLayer Subnetwork are the set-up and tear-down of subnetwork connection (SNC).

N

network element	Telecommunications hardware equipment that is addressable and manageable. NEs provide support or services to the user and can be managed through an Element management system (EMS). An NE is a combination of hardware and software that primarily performs a telecommunications service function. A group of interconnected network elements form a network.
P	
party	An individual, organization or organization unit. Party is an abstract concept that should be used in places where the business says something.
party role	The part played by a party in a given context with any characteristics, such as expected pattern of behavior, attributes, and/or associations that it entails. PartyRole is an abstract concept that should be used in places where the business refers to a Party playing a Role.
physical termination point	A physical termination point (PTP) represents the actual or potential endpoint of a topological link. Essentially, this is a representation of a physical port.
ProductBundle	A type of product that is composed of other products. The other products may be ProductBundles or ProductComponents.
ProductSpecification	A detailed description of a tangible or intangible object made available externally in the form of a ProductOffering to customers or other parties playing a PartyRole. A ProductSpecification may consist of other ProductSpecifications supplied together as a collection. Members of the collection may be offered in their own right. ProductSpecifications may also exist within groupings, such as ProductCategories, ProductLines, and ProductTypes.
R	
Route	A partially ordered series of cross connects through which the SNC traverses.
S	
Service	A realization of a product facing the customer (CustomerFacingService) or how a service is provisioned within a provider's infrastructure (ResourceFacingService). Services are defined by a ServiceSpecification. The purpose of the specification is two-fold. First, it is used to define attributes, methods, and relationships that are common to all services. Second, it provides a convenient point to define how services interact with other parts business entities.

service access point	A point of entry where the service can be accessed. This point of entry is always associated (directly or indirectly) with a physical resource (such as a PTP, a CTP). However, sometimes the SAP is an object or a logical resource that contains or identifies the support of the physical resource.
ServiceCatalog	A group of service specifications that share common characteristics. For example one catalog could group all internet related service specifications.
ServiceCharacteristicValue	A value passed over the activation interface to convey an individually set service characteristic (that is, not reference in a ServiceTemplate) or to override a globally set characteristic value (present in a ServiceTemplate). A ServiceCharacteristic-Value will apply only to the specific service instance created.
ServiceDefinition	A type of service specification (from the SID) introduced for the purpose of service fulfillment. It defines all the ServiceSpecCharacteristics that must be used to create corresponding service instances: The ones which are set globally (the corresponding values are defined only in ServiceTemplates and are sometimes designated as "invariant"). The ones which are set individually (the corresponding values can be defined only over the Activation Interface and are sometimes designated as "variant"). A ServiceSpecCharacteristic specified in a ServiceDefinition may be associated with ServiceSpecCharacteristicValues to restrict the typing information or to specify a default value.
service order	A type of request (as defined in the SID model). In particular, a service order is used to query and control the progress of a request for some actions (for example, provision or activation) on the services that comprise a given product instance. It should be mentioned that the OSS/J Order Management API (JSR 264) defines a service order as follows: "a type of request that represents a customer order's products decomposed into the services through which the products are realized. Service orders are generated within the confines of the SM&O layer."
service order item	Item used to represent the order aspects of the services associated with a given service order. There is one service order item for each service associated with a service order.
service request	A request made by the CRM layer to the SM&O layer as defined in the TMForum eTOM to take an action on one or more CFS instances given a product identifier, a product specification name and a related set of characteristics. This request can be realized by template and by value.

ServiceSpecCharacteristic

A characteristic quality or distinctive feature of a service as represented in a ServiceSpecification (specialized as ServiceDefinition or ServiceTemplate). In particular it contains typing information which can be arbitrarily complex.

A ServiceSpecCharacteristic can be atomic or composite (also called "packages"). The components of a composite ServiceSpecCharacteristic can in turn be atomic or composite.

ServiceSpecCharacteristicValue

A value that can be associated with a ServiceSpecCharacteristic in compliance with the specified type information.

- When associated with a ServiceSpecCharacteristic in a ServiceDefinition, it is used to restrict the typing information (in this case several ServiceSpecCharacteristicValues may be used) or to specify additional information (for example, default value).
- When associated with a ServiceSpecCharacteristic in a ServiceTemplate, it will apply globally to all the service instances conforming to this ServiceTemplate.

In this case, the ServiceSpecCharacteristicValue is set at the design stage when the ServiceTemplate is created, and it cannot be modified afterwards.

A ServiceSpecCharacteristic present in a ServiceTemplate is sometimes qualified as being "invariant", since it cannot be modified after the creation of the ServiceTemplate (the term "globally set" can also be used).

A ServiceSpecCharacteristic which value is passed over the Activation Interface is sometimes qualified as being "variant", since the value must be given for each service instance created (the term "individually set" can also be used).

ServiceSpecification

Changeable as well as invariant attributes, methods, relationships and constraints which define a service. It can be conceptually thought of as a template that different service instances can be instantiated from. Each of these service instances will have the same invariant characteristics. However, the other characteristics of the instantiated service will be specific to each instance.

ServiceSpecificationType

A generic category of ServiceSpecifications.

Each ServiceSpecificationType serves to group a set of particular ServiceSpecifications that share the same behavior and other semantics. One result of this is to be able to more efficiently define a set of related services that can be grouped together to form a higher-level service.

For example, a given higher-level service might include VPN and QoS services. If these services are always used together, then they can be categorized using a common type.

ServiceTemplate

A type of service specification (from the SID) introduced for the purpose of service fulfillment.

It defines specific ServiceSpecCharacteristicsValues for the globally set ServiceSpecCharacteristics that can be dynamically referenced by multiple service instances during their lifecycle span. A ServiceTemplate is checked against its associated service definition by verifying the presence of the ServiceSpecCharacteristics and the validity of the corresponding assigned ServiceSpecCharacteristicsValues. Each of the associated service instances will have the same invariant characteristics whose values are taken from the service template.

However, when activating a service, it may be possible to specify over the Activation Interface a ServiceCharacteristicsValue which overrides the corresponding ServiceSpecCharacteristicValue available in the associated ServiceTemplate.

In this case the new proposed value applies only to the service instance created, and the ServiceSpecCharacteristicValue in the ServiceTemplate is not modified.

In order not to descend into sub-classing, the ServiceTemplate is considered to be generic such that it serves as a framework for defining technology or service specific templates. Other TMForum groups, or service providers, may use the ServiceTemplate as a foundation for building or populating ServiceTemplates.

subnetwork connection

A relationship between two of the following types of endpoints:

- Physical termination point (PTP)
- Connection termination point (CTP)
- Group termination point (GTP)
- Floating termination point (FTP)

An SNC represents a transparent end-to-end connection or a trail (closed or half-open) through or within a multi-layer subnetwork according to the roles associated to its endpoints. If the SNC represents a connection, its endpoints are CTPs or FTPs with the SNC's layer rate as the connectable layer rate. In the case of GTPs (that is, a bundled connection), the SNC does not have an explicit layer rate. If the SNC represents a trail, its endpoints are CTPs, FTPs, or PTPs. An SNC must be on a multi-layer subnetwork.

subscriber

An entity (associated with one or more users) that is engaged in a service subscription with a service provider. The subscriber is allowed to subscribe and unsubscribe services, to register a user or a list of users authorized to use these services, and also to set the limits relative to the use that associated users make of these services.

T

termination point	A logical abstraction of a TP(actual or potential) on any of the following: 1. A topological link 2. A subnetwork connection (SNC) 3. A flow domain fragment (FDFr) 4. A cross connection (CC)
topology link	A physical connection between two physical termination points (PTPs) or a trail between two termination points (TPs), such as an ATM connection between two ATM NI CTPs. The two TPs are called the source and sink TPs of the TL.
transmission descriptor	A collection of attributes used to define multi-layered transmission parameters and additional information parameters on a termination point (TP).

B Acronyms and Abbreviations

A	
ABR	asynchronous batch response
AFB	asynchronous file bulk
AID	alarm identifier
ARR	asynchronous request/reply
ASN.1	Abstract Syntax Notation One
AVC	attribute value change
C	
CDE	common desktop environment
CPU	central processing unit
E	
EdgeTP	edge termination point
EH	equipment holder
EQT	equipment
EMS	element management system
EOW	Ethernet over WDM
F	
FIFO	first in first out
FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
GNE	gateway network element
GUI	graphical user interface

H	
HA	high availability
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I	
ID	identity
IP	Internet Protocol
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
J	
JMS	Java message service
L	
LAN	local area network
M	
MAC	media access control
MD	management domain
MDP	message dispatch process
ME	managed element
MEP	message exchange pattern
MLSN	multi-layer subnetwork
MO	managed object
MTOSI	Multi-Technology Operations System Interface
MTNM	multi-technology network management
N	
NE	network element
NEL	network element level
NML	network management level
NMS	network management system
O	
OS	operating system
ONE	optical network element
OTN	optical transport network
OSGI	open services gateway initiative

OSS	operations support system
OSN	optical switching network
OSI	open systems interconnection
P	
PC	personal computer
PDH	plesiochronous digital hierarchy
PTP	physical termination point
S	
SAP	service access point
SC	state change
SDH	synchronous digital hierarchy
SFB	synchronous file bulk
SIT	synchronous iterator pattern
SNC	subnetwork connection
SOAP	Simple Object Access Protocol
SONET	synchronous optical network
SRR	synchronous request response
SSL	Security Socket Layer
SSM	synchronization status message
SFTP	Secure File Transfer Protocol
SML	service management layer
SOA	service-oriented architecture
T	
TCP	Transport Control Protocol
TL	topological link
TMD	transfer descriptor
TMF	Tele Management Forum
TMN	telecommunication management network
TP	termination point
TCA	threshold-crossing alarm
U	
UPC	usage parameter control

UTC	coordinated universal time
W	
WAN	wide area network
WSN	Web services notification

