Release Notes

1. Basic Information

Device Model	NTA NX3-2000E/1000E/HD2100/HD2200 vNTA
Software Version	V4.5R90F02
Upgrade File	update_nta_V4.5R90F02.200304build34994.bin MD5: 4B2FF7343819919823BDA32B44650113
Release Date	2020-03-27
How to Obtain	Obtain the upgrade file from the upgrade system or contact NSFOCUS technical support.

2. Version Mapping

Product Model	NTA NX3-2000E/1000E (NSF-2800) NTA NX3-HD2100/HD2200 (C236)
ADS	V4.5R90F01 V4.5R90F01SP01 V4.5R90F01SP02 V4.5R90F01SP03 V4.5R90F01SP04 V4.5R90F01SP05 V4.5R90F01SP06 V4.5R90F01SP07 V4.5R90F01SP08 V4.5R90F01SP09 V4.5R90F02
ADS M	V4.5R90F02
NTA-ATM	V4.5R89F03
Threat Analysis and Traceback System (TAT)	V2.0.0
Client Browser	Chrome Firefox
Documentation	NSFOCUS NTA Installation Guide/User Guide (V4.5R90F02)

3. New Requirements

No.	Requirement Description
1	Two DDoS alert plug-ins should be added for CLDAP and MS SQL amplification attacks.
2	The system uptime needs to be sent via SNMP traps every 5 minutes.
3	SNMP traps should be divided by the data source (global or region/IP group).
4	The auto-learning state should be correctly displayed when an auto-learning failure occurs during an HA switchover.
5	Status monitoring and running logging need to be added for the NTP service.
6	The function of alerting router flow data acquisition anomalies is required.
7	The function of alerting router SNMP data acquisition anomalies is required.
8	License verification should be optimized by displaying more specific messages to indicate the results.
9	The alert ID configuration needs to be added for custom alert plug-ins.
10	Collaboration with NSFOCUS Bigdata Security Analytics (BSA) needs to be expanded to cover bogus source IP addresses.
11	The GeoIP library needs to be updated.
12	The EBGP configuration needs to be added to allow the configuration of the remote AS for each neighbor during BGP session creation.
13	OpenSSL needs to be upgraded to V1.0.2u.
14	The SFTP service should be available via a third-party interface.
15	The **context** field is added in SNMPv3 configuration.
16	Report types sent via email need to be expanded to cover the bogus source IP report.
17	A port on ADS M can be specified for NTA management.
18	The custom-permission user group is added.

4. New Functions

4.1 Two New DDoS Alert Plug-ins

Description

1. Custom alert plug-ins for CLDAP and MS SQL amplification attacks are encapsulated as built-in attack alert plug-ins and enabled by default.

   Rule for CLDAP amplification: UDP, source port 389

   Rule for MS SQL amplification: UDP, source port 1434

2. Alerts for the two types of attack can also be sent to a system collaborating with NTA, like a cloud platform, third-party cloud platform, cloud cleaning platform, BSA, ADS M, NTA-ATM, and a SFTP server.
3. The UDP reflection alert plug-in also covers the two types of attack.

Configuration and Use

- Configuration > Global Alert Settings > Default DDoS Attack Detection Threshold

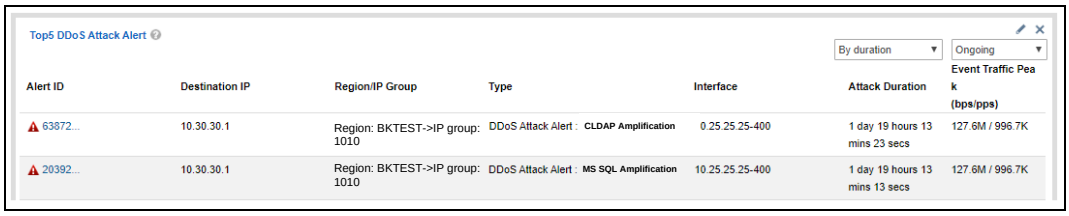
  Configure the detection mode and threshold for the two alert plug-ins.
- Configuration > Global Alert Settings > Alert-Plug-in Management

  Determine whether to enable the two alert plug-ins.
- Configuration > Alert Configuration Template > Region Alert Template > default template

  Edit settings of the two alert plug-ins under **Region DDoS Attack Alert**.
- Configuration > Alert Configuration Template > IP Group Alert Template > default template

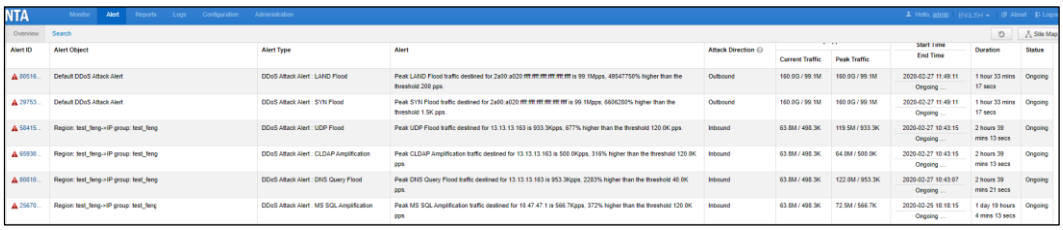
  Edit settings of the two alert plug-ins under **IP Group DDoS Attack Alert**.
- Monitor > Overview > Top5 DDoS Attack Alert

  View the two alert plug-ins.



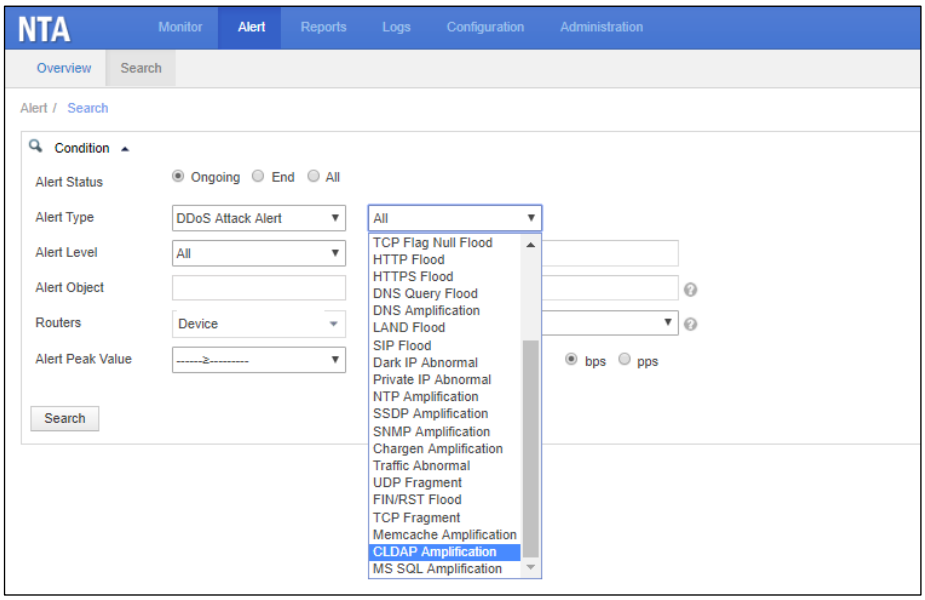
- Alert > Overview

  View the two alert plug-ins.



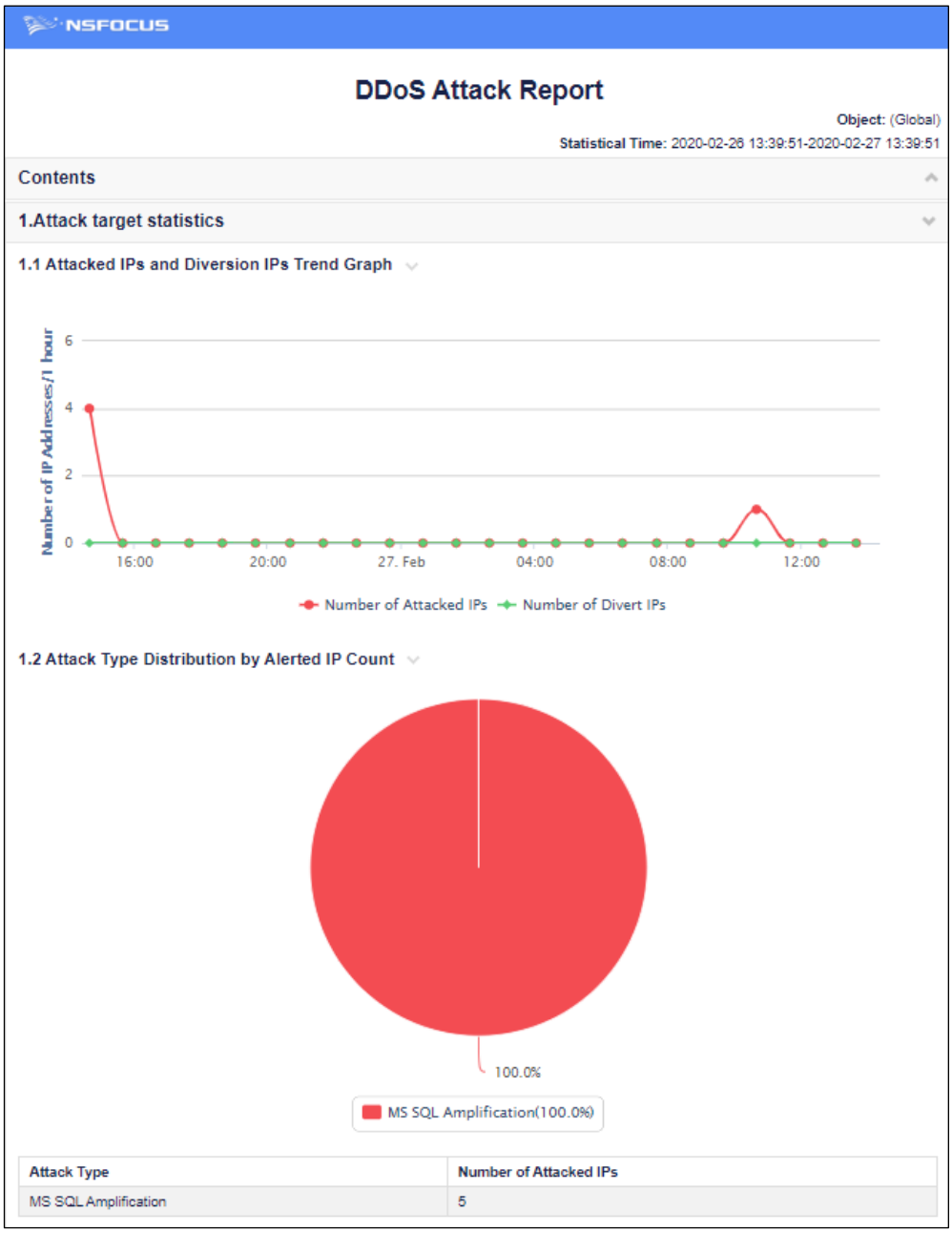
- Alert > Search

  Search for the two types of DDoS attack alert.



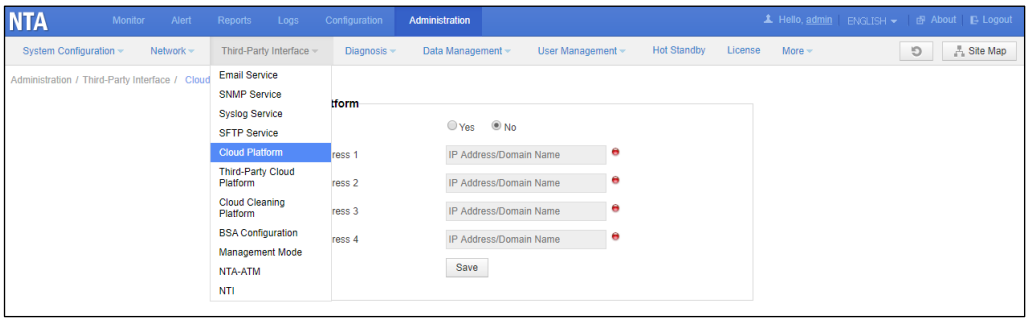
- Report > DDoS Attack Report

  Query reports of the two types of alert.



- Administration > Third-Party Interface

  Configure systems to which the two types of alert logs can be sent. Such systems include cloud platforms, third-party cloud platforms, cloud cleaning platforms, BSA, ADS M, NTA-ATM, and SFTP servers.



4.2 System Uptime Sent via SNMP Traps Every 5 Minutes

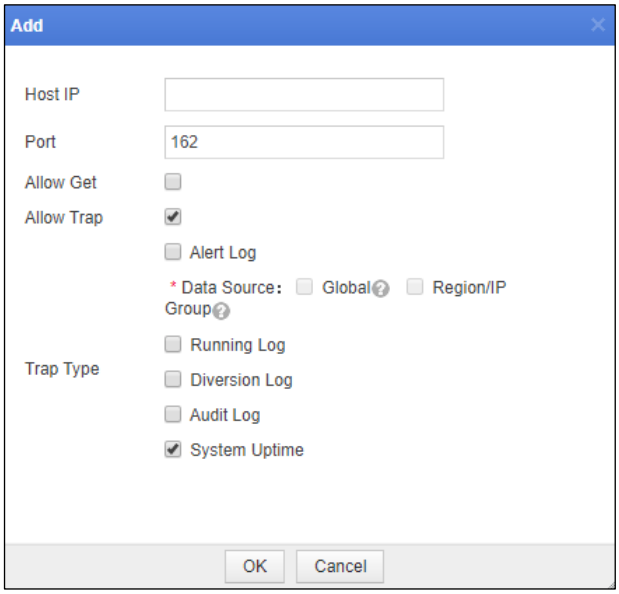
Description

1. The system uptime can be configured on the **SNMP Service** page.
2. The system runtime is sent every 5 minutes.
3. The SNMP description document is updated.

Configuration and Use

- Administration > Third-Party Interface > SNMP Service

  Enable the SNMP service. Add a new network management station with **System Uptime** selected for **Trap Type**.



System running logs are sent via SNMP traps every 5 minutes. The system uptime uses the common OID (1.3.6.1.2.1.1.3).

4.3 SNMP Traps Divided by Data Source

Description

1. SNMP traps are divided into two types: global alerts and alerts for regions and IP groups.

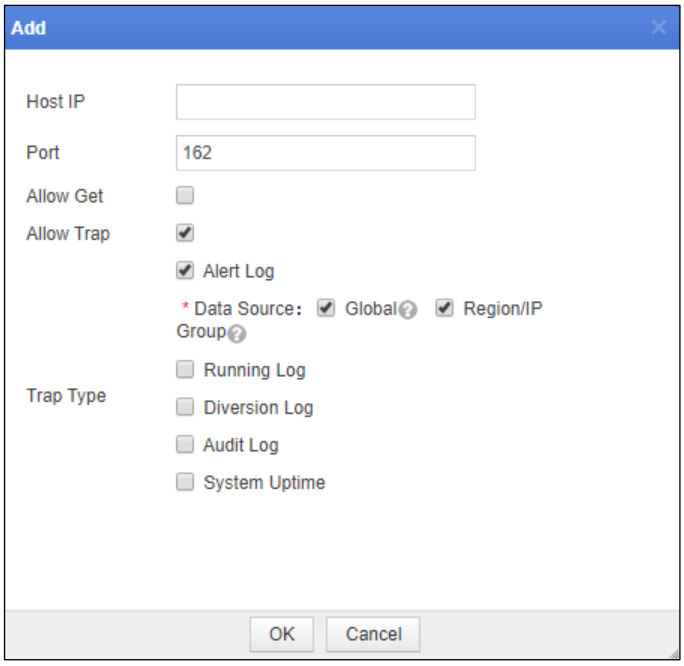
2. If **Region/IP Group** is selected, alert logs for regions and IP groups will be sent via SNMP traps. Specifically, such logs concern alerts that are generated for IP addresses included in regions or IP groups when an alert threshold set for the regions or IP groups is exceeded.

3. If **Global** is selected, logs for global alerts are sent. Specifically, these logs are generated for alerts that are reported for IP addresses excluded from regions or IP groups when a global alert threshold is exceeded.

Configuration and Use

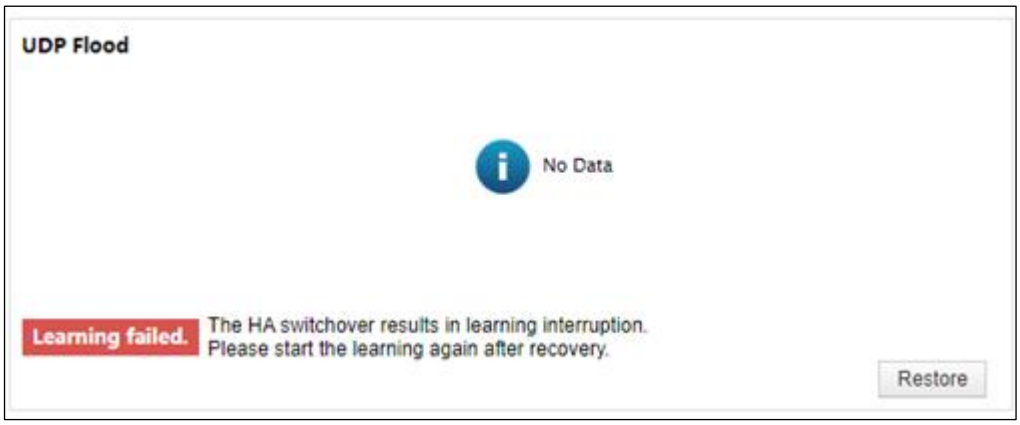
- Administration > Third-Party Interface > SNMP Service

  Enable the SNMP service. Add a new network management station and configure the data source of alert logs sent via SNMP traps.



4.4 Optimization of the State Indicating the Auto-Learning Failure Occurring During an HA Switchover

Assume that there are two NTAs (NTA1 is active and NTA2 is standby) that work in HA mode. If an HA switchover occurs during traffic auto-learning, the auto-learning state changes to "failed" and the cause of the failure is displayed on the **Traffic auto-learning** page under **Monitor**.



4.5 Status Monitoring and Running Logging Added for NTP Service

Description

1. Monitor > Machine Status

   The NTP service is added in the last row of the table in the **System Engine** area. When the green indicator is on, the NTP process is running properly.

   When the green indicator is on, the NTP process is running properly.
   When the yellow indicator is on, the NTP process has stopped running.

   When "No service" is displayed, no NTP process is running, which may be because no NTP server is configured or the system time is in synchronization with ADS M.

2. Administration > System Configuration > Basic Information

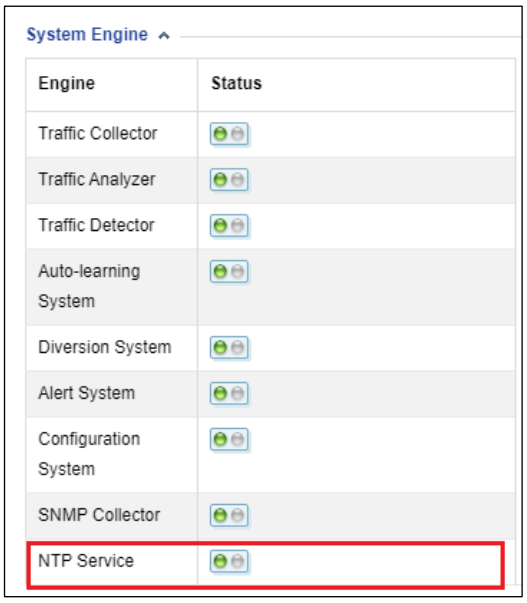
   The NTP service is added in the last row of the table in the **System Engine** area. The status of this service is displayed in the same way as other engines.

3. Administration > Third-Party Interface > SNMP Service

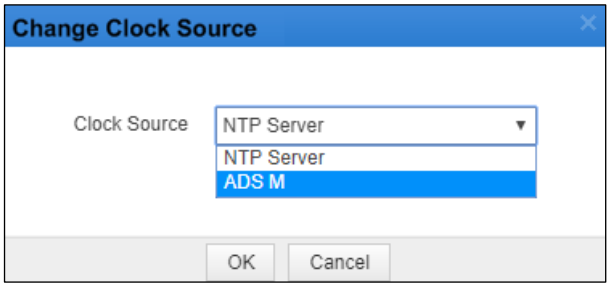
   When a website management station is added or edited, after you select the check box for **Allow Trap**, you can determine which types of logs can be sent via SNMP traps. In this case, if the NTP process is enabled, after the **Running Log** is selected for **Trap Type**, running logs sent via SNMP traps will contain NTP logs.

Configuration and Use

- The NTP service runs properly.



- The clock source is changed to ADS M.



- The NTP service has stopped.

System Engine

Engine	Status
Traffic Collector	
Traffic Analyzer	
Traffic Detector	
Alert System	
Configuration System	
SNMP Collector	
Auto-learning System	
Diversion System	
NTP Service	No service.

4.6 Addition of Alerting on Router Flow/SNMP Data Acquisition Anomaly

Description

1. New alerts: alerts on flow data acquisition anomalies and SNMP data acquisition anomalies in the **Router Alert Configuration** area for a router on the **Routers** page under **Configuration > Objects**.
2. New alert plug-ins: Alert plug-ins for flow data acquisition anomalies and SNMP data acquisition anomalies in the **Router Alert** area on the **Alert Plug-in Management** page under **Configuration > Global Alert Settings**.
3. The two types of alert can also be included in alert logs sent to collaborative systems, including an email server, SNMP server, syslog server, SFTP server, and cloud platform.
4. Alerts on router data acquisition anomalies can be retrieved under **Alert > Search**.

Configuration and Use

- Configuration > Global Alert Settings > Alert-Plug-in Management

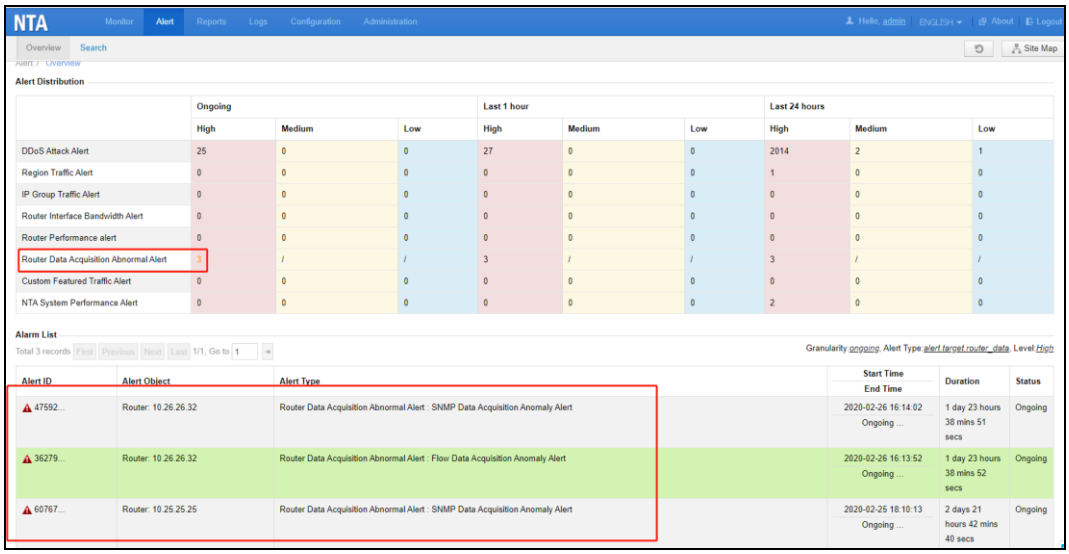
  Determine whether to enable the two alert plug-ins.
- Configuration > Objects > Routers

  Click a device name, click **Edit**, and enable the alert plug-ins for SNMP data acquisition anomalies and flow data acquisition anomalies and set the alert latency period threshold for the two plug-ins on the **Router Alert Configuration** page.
- Configuration > Objects > Routers

  Click the interface number for a router and enable the monitoring function for the interfaces.

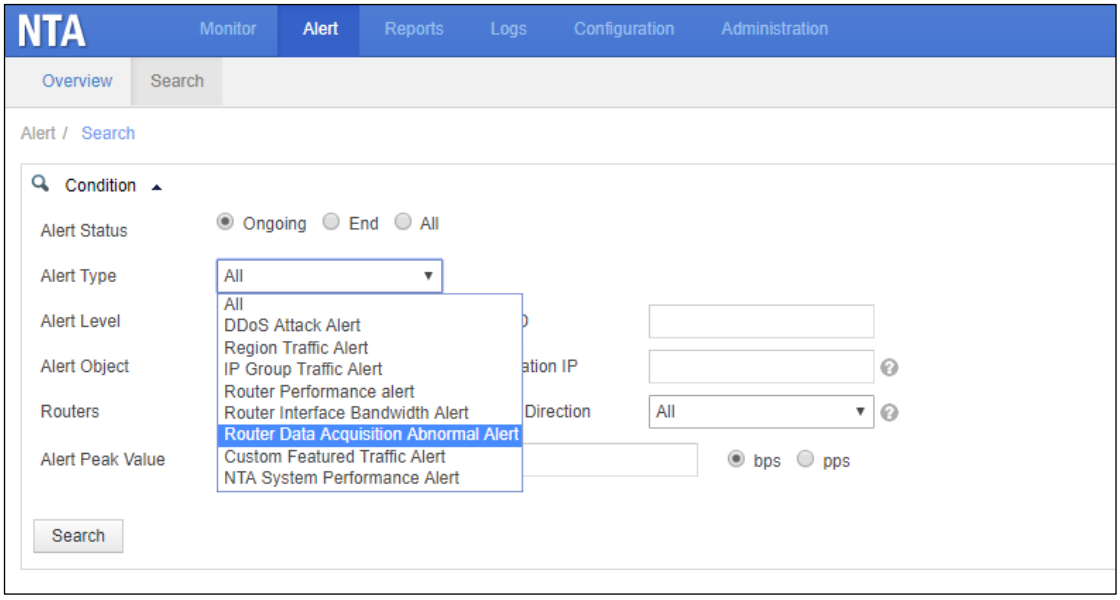
- Alert > Overview

  View the new alerts.



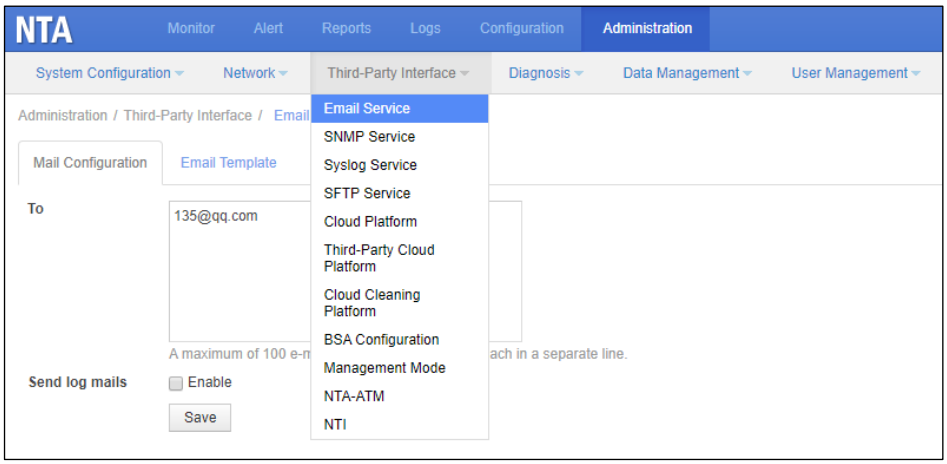
- Alert > Search

  Select **Router Data Acquisition Abnormal Alert** for **Alert Type**.



- Administration > Third-Party Interface

  Logs for the new alerts can be sent to a collaborative system such as an email server, SNMP server, syslog server, SFTP server, or cloud platform.



4.7 License Verification Optimized by Providing More Specific Error Information

When an error occurs during import of an NTA license, the cause of the error displayed on the web-based manager is not accurate. Therefore, technical support personnel cannot rapidly locate the fault and have to report this issue to R&D engineers. To resolve this issue, the license verification process is optimized by providing more specific information about errors.

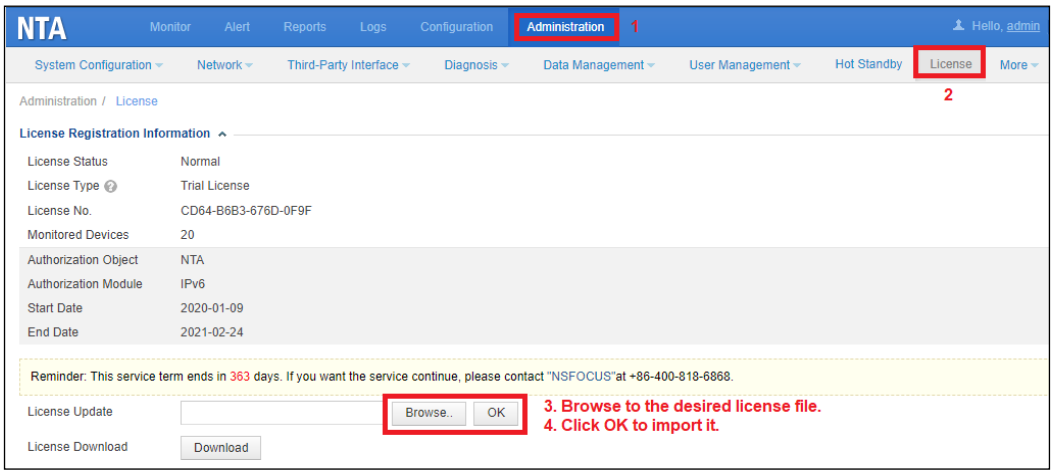
Description

Check Item		Message Displayed on the Web Page
Whether the user has the license change permission (only users with this permission can perform this operation)		You do not have the permission for this operation.
Whether a license file has been uploaded		No file uploaded.
Whether the license file is executable		File upload error. Cannot execute the file.
Whether the license file name contains characters other than the valid ones (digits, letters, spaces, and hyphens)		File upload error. The file name contains invalid characters.
Whether the license file size is larger than 10 MB		File upload error. The file size cannot be larger than 10 MB.
License content	The interim license is not deleted from the web-based manager and the license to be imported is the same as the existing one.	License update failure. You cannot import the same license.
	The expiry date of the license is earlier than the current date.	License uploaded, but the new license may already expire.
	The license file fails to be opened.	License update failure. Cannot open the license file.
	The license file fails to be decrypted (in case an XML file needs to be exported).	License update failure (in case an XML file needs to be exported). Cannot decrypt the license file.
	The license file fails to be decrypted (in case an XML file does not need to	License update failure. Cannot decrypt the license file.

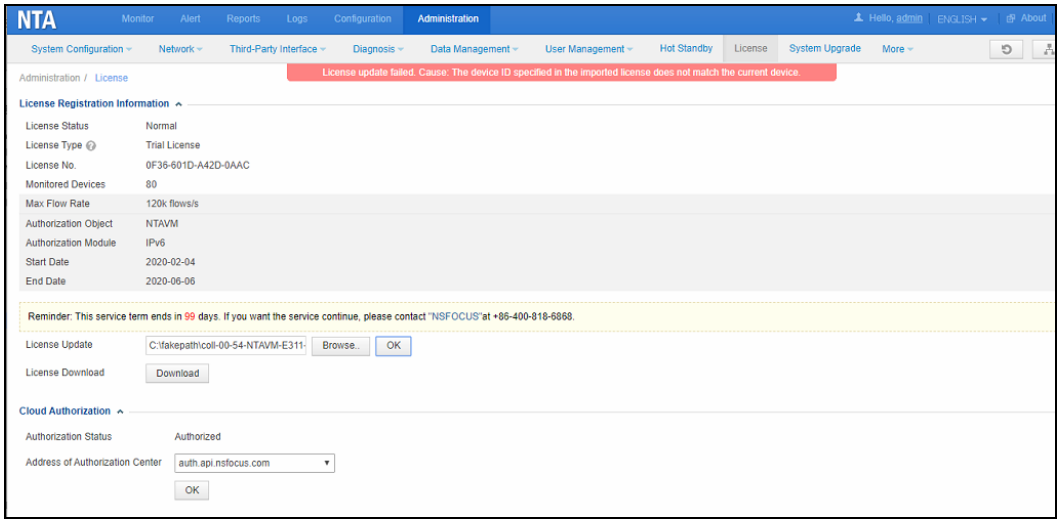
Check Item		Message Displayed on the Web Page
	be exported).	
	The product type covered by the license is neither COLLAPSAR nor MAGICFLOW.	License update failure. The product type is incorrect.
	An interim license exists and its validity start date is later than that of the new license.	License update failure. The validity start date of the existing license is later than that of the new license.
	The device ID fails to be obtained.	License update failure. Cannot obtain the device ID.
	The device ID obtained from the license is different from the actual device ID.	License update failure. The device ID covered by the new license does not match the ID of the local device.
	The license's validity start date is later than the current date.	License update failure. The license's validity start date is yet to come.
	An interim license exists and the result of its actual days of use plus its validity start date falls on a date later than the validity end date of the new license, which is still valid according to the system time. This happens maybe because the system time has been changed.	License update failure. The license has expired.
	The device model covered by the license fails to be obtained.	License update failure. Cannot obtain the device model covered by the license.
	The device model (hostname) covered by the license fails to be obtained.	License update failure. Cannot obtain the device model covered by the license.
	The device model, though obtained, is empty.	License update failure. Invalid device model.
	The license type is "Subscription", but the device is not a virtual device.	License update failure. Subscription license imported, which is applicable only to virtual devices.
	The device model obtained from the license is different from the actual device model.	License update failure. The device ID covered by the new license does not match the actual device model.
	No file is created during license verification.	License update failure. Cannot create any file.
	The new license is correctly parsed.	License uploaded.

Configuration and Use

Choose **Administration > License**, browse to the desired license file, and upload it to replace the current license.



If the license fails to be imported, the system displays an error message, as shown in the following figure.



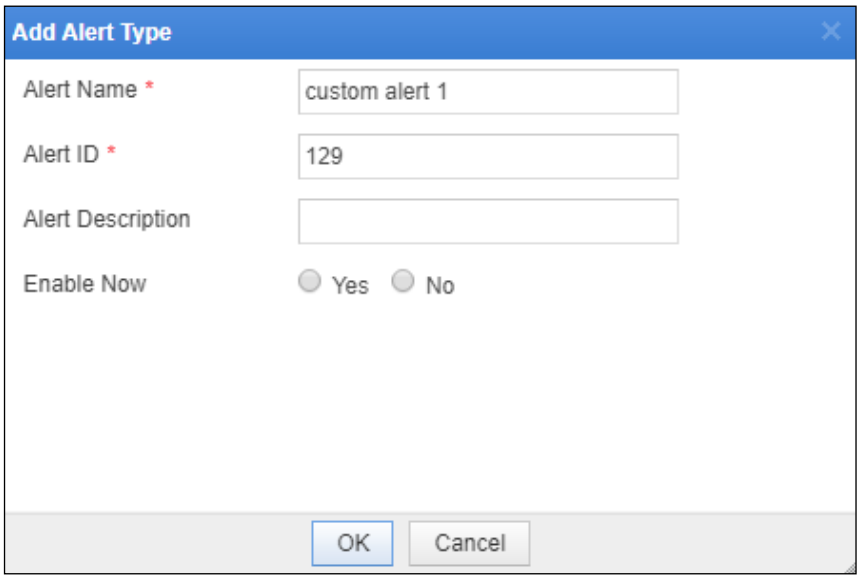
4.8 Alert ID Added for Custom Alerts

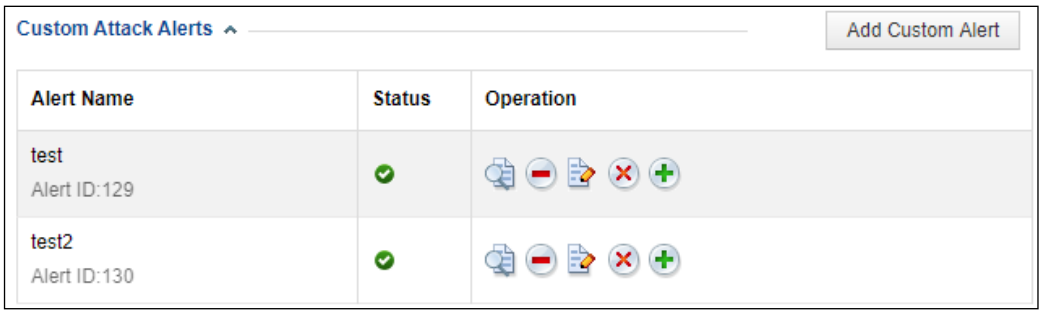
Description

Alert ID is added for custom alerts.

Configuration and Use

Choose **Configuration > Global Alert Settings > Alert Plug-in Management** and click **Add Custom Alert**. The alert ID must be unique and ranges from 129 to 200.





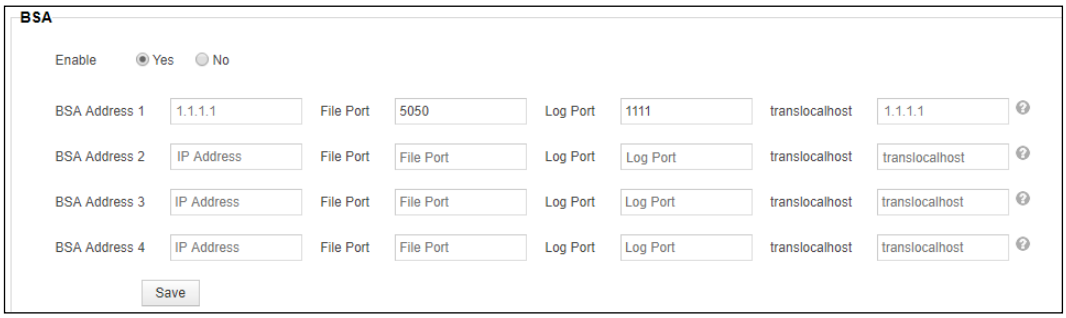
4.9 Collaboration with BSA Expanded to Cover Bogus Source IP Addresses

Description

NTA's collaboration with BSA is expanded to cover bogus source IP addresses. After detecting such IP addresses, NTA will send the information to BSA, thereby improving traceability of attack events.

Configuration and Use

This function works in the background. Choose **Administration > Third-Party Interface > BSA Configuration**, correctly configure file ports, and enable collaboration with BSA. Then NTA will send data of bogus source IP addresses to BSA every 15 minutes.



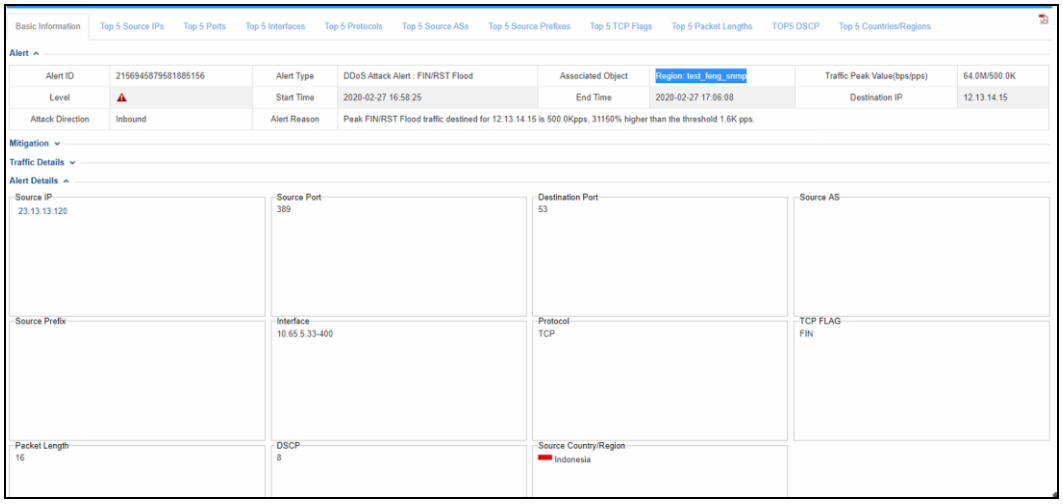
4.10GeoIP Library Updated

Description

According to corporate requirements, the GeoIP library is updated and a unified format is used to display related information. The related API is adapted to this change, but users do not need to modify any configuration for this purpose on the web-based manager.

Configuration and Use

The update of the GeoIP library does not require any configuration by users. After the update, for source IP addresses of collected traffic and those included in alert details, their country/region information is also provided, as shown in the following figure.



4.11EBGP Configuration Added to Allow Configuration of Remote AS for Each Neighbor During BGP Session Creation

Description

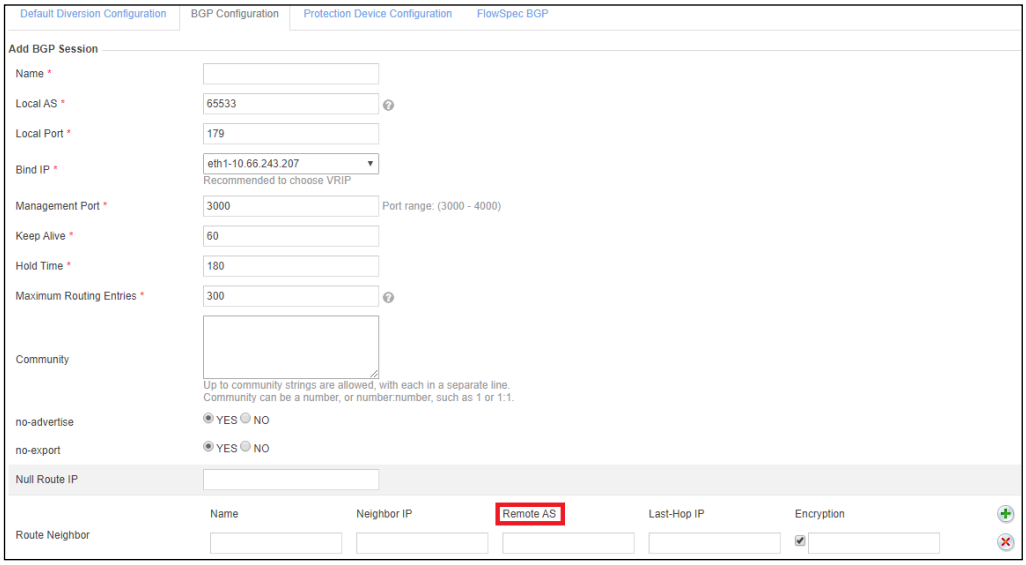
For BGP sessions, **Remote AS** is added for each route neighbor and dispatched to the BGP configuration file.

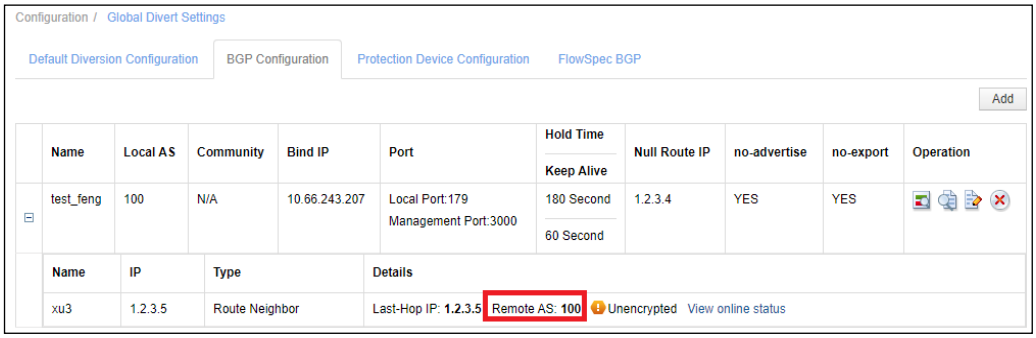
Configuration and Use

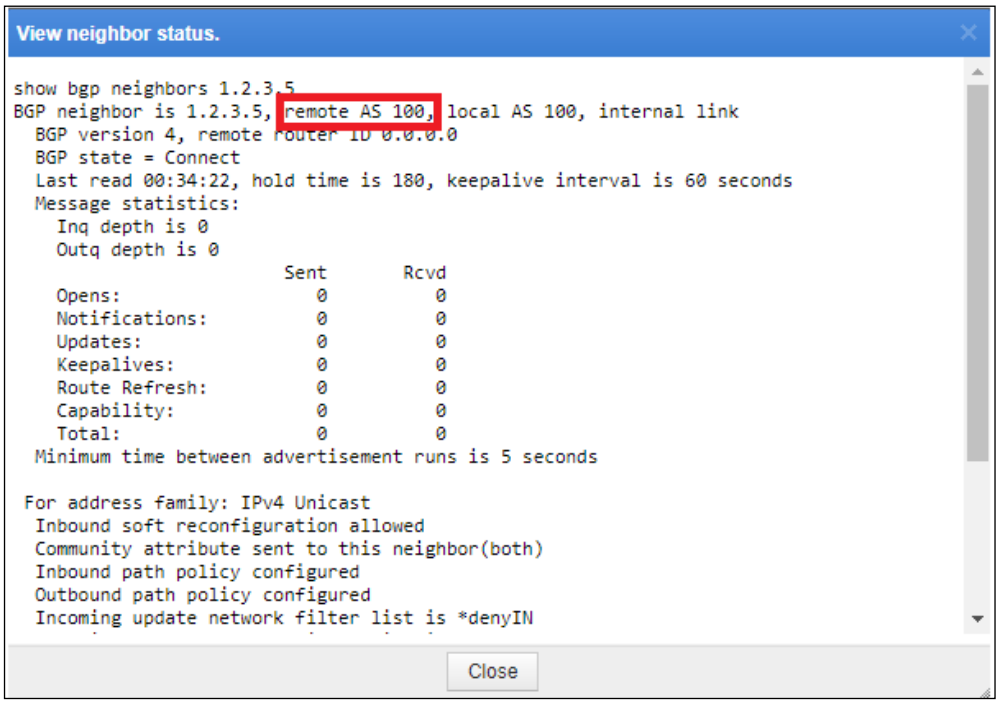
Choose **Configuration > Global Divert Settings > BGP Configuration**, and click **Add**.

The value range of **Remote AS** is the same as that of **Local AS**.

The value of **Remote AS** can be different from that of **Local AS**.







An EBGP neighbor is successfully created.

4.12 OpenSSL Upgraded to V1.0.2u

Currently, NTA uses OpenSSL 1.0.2j, which was released in 2016 and contained a number of security bugs. Recently, a vulnerability was reported in OpenSSL, affecting 1.0.2t and before. For this reason, OpenSSL used by NTA is upgraded to V1.0.2u.

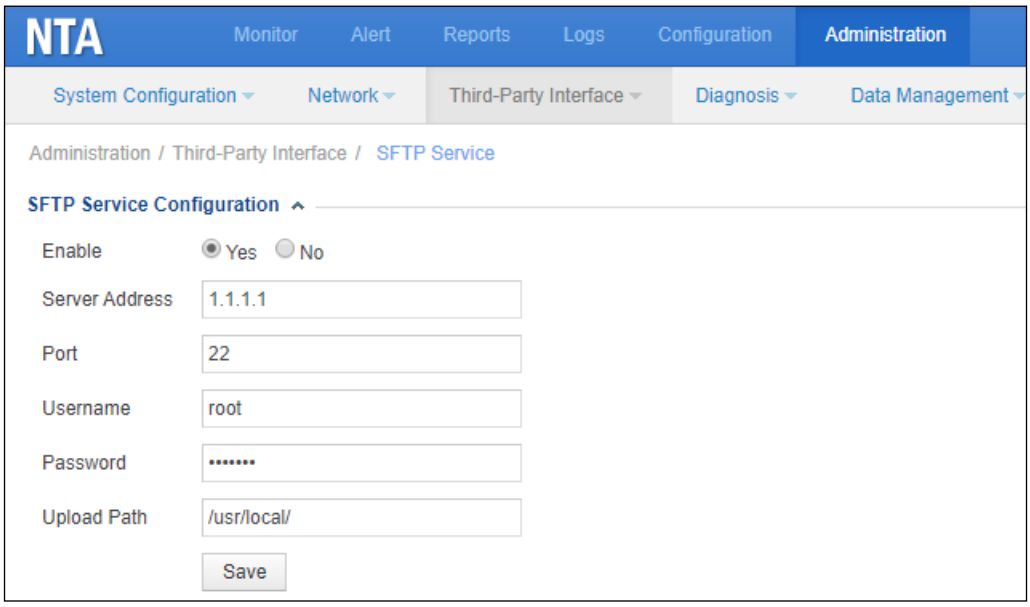
4.13 SFTP Available via a Third-Party Interface

Description

NTA's basic information, status information, and log messages are stored in a log file named in the format of "NTA-[device name]-[device IP]-timestamp.txt". This log file is uploaded to the specified location of the configured SFTP server via SFTP. (For details, see *PVD-NTA-V4.5R90F02-SFTP Specifications* enclosed here.)

Configuration and Use

Administration > Third-Party Interface > SFTP Service



The SFTP server obtains device information every minute and stores it in the "NTA-[device name]-[device IP]-timestamp.txt" file before sending the file to the specified location of the SFTP server. Such a file looks like this:

```
cls<NTA> obj<10_66_243_195> par<dev_status> val<0> msg<Device status: normal>
cls<NTA> obj<10_66_243_195> par<state_fan> val<0> msg<Fan status: N/A for vNTA>
cls<NTA> obj<10_66_243_195> par<state_engine> val<0> msg<Engine status: normal>
cls<NTA> obj<10_66_243_195> par<state_bgp> val<1> msg<neighbor BGP neighbor status: abnormal>
cls<NTA> obj<10_66_243_195> par<state_ads> val<1> msg<test Collaboration failed,testads Collaboration failed>
cls<NTA> obj<10_66_243_195> par<state_port_H> val<0> msg<H Port status: Up>
cls<NTA> obj<10_66_243_195> par<state_port_M> val<0> msg<M Port status: Up>
cls<NTA> obj<10_66_243_195> par<state_traffic> val<0> msg<Traffic on ports: normal>
cls<NTA> obj<10_66_243_195> par<lic_state> val<53> msg<License valid from 20191128,License valid to 20200418>
cls<NTA> obj<10_66_243_195> par<lic_start_time> val<20191128> msg<License valid from 20191128>
cls<NTA> obj<10_66_243_195> par<lic_end_time> val<20200418> msg<License valid to 20200418>
cls<NTA> obj<10_66_243_195> par<state_cpu> val<10> msg<CPU usage 10%>
cls<NTA> obj<10_66_243_195> par<state_memory> val<14> msg<Memory usage 14%>
cls<NTA> obj<10_66_243_195> par<state_temp_cpu> val<0> msg<CPU temperature: N/A for vNTA>
cls<NTA> obj<10_66_243_195> par<state_temp_board> val<0> msg<Mainboard temperature: N/A for vNTA>
cls<NTA> obj<10_66_243_195> par<state_uptime> val<255364> msg<System uptime: 255364 seconds>
cls<NTA> obj<10_66_243_195> par<state_router> val<1> msg<1.1.1.1 Flows on routers: abnormal>
cls<NTA> obj<10_66_243_195> par<log_alert> val<0> msg<No attack>
```

4.14 Addition of the context Field in SNMPv3 Configuration

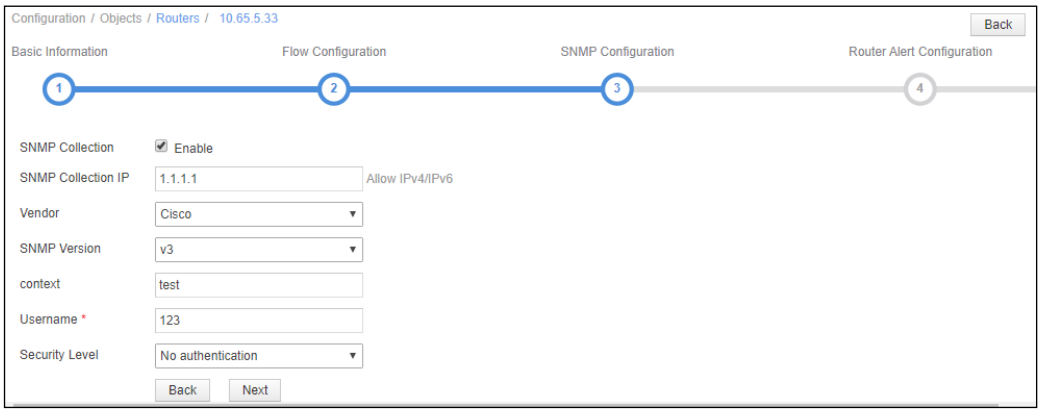
Description

Considering that some routers, such as those from ZTE, use the **context** field, the **context** field is added for SNMPv3 specified during router configuration.

Configuration and Use

Configuration > Objects > Routers

When adding a router, set the **context** parameter if **v3** is selected as the SNMP version during SNMP configuration. If the router does not use this field, leave this parameter empty.



4.15 Report Types Sent via Email Expanded to Cover the Bogus Source IP Report

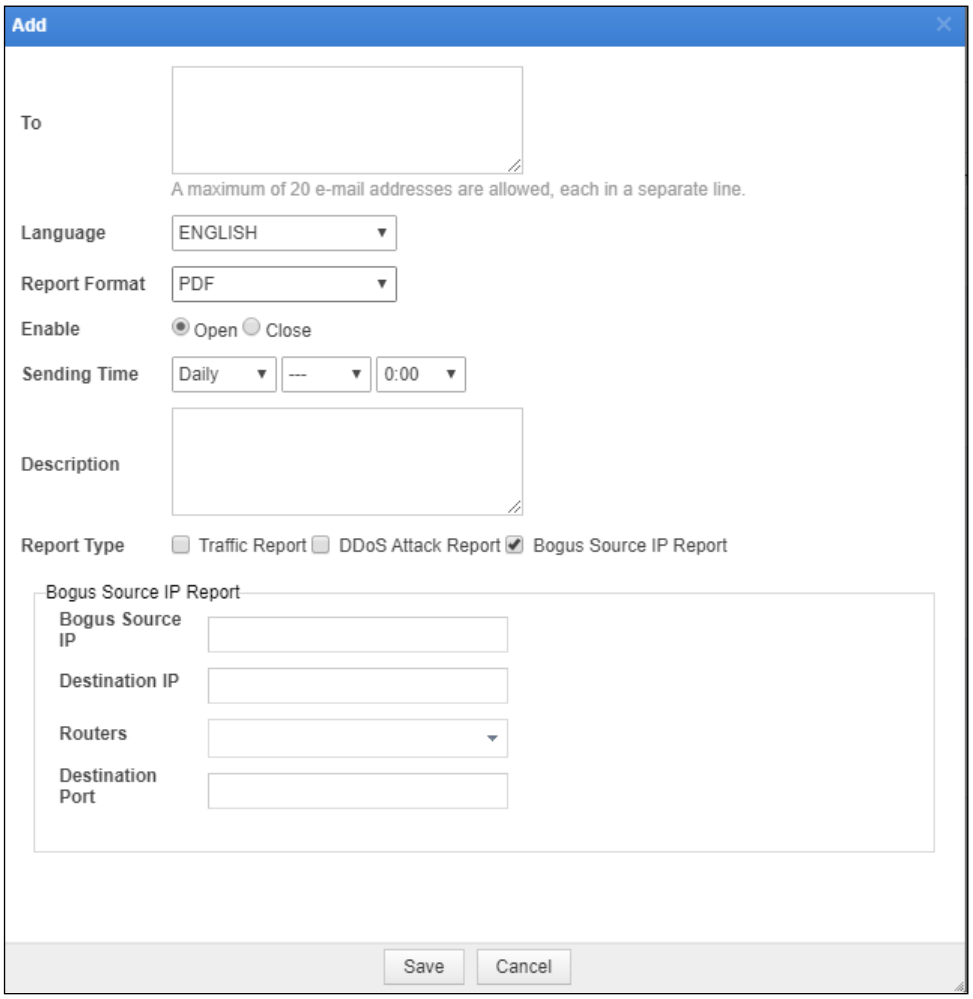
Description

The bogus source IP report is added as a new type of reports that can be sent via email. After this report type is selected, NTA will filter data of detected bogus source IP addresses pursuant to the specified conditions and then send such data as a PDF or CSV file as scheduled.

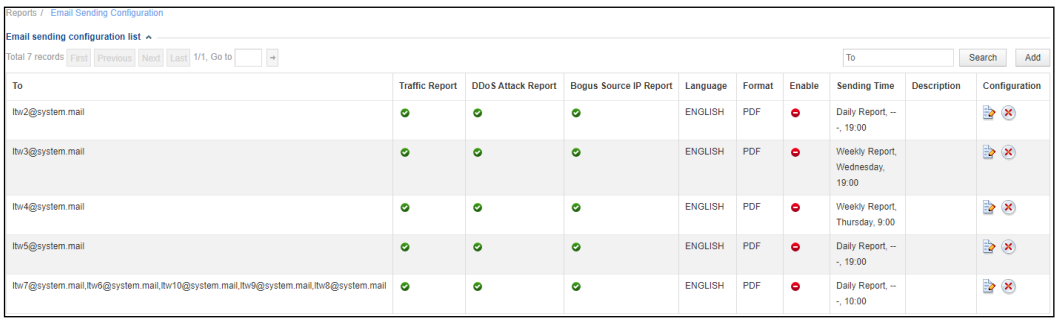
Configuration and Use

Choose **Reports > Email Sending Configuration** and click **Add**.

In the **Add** dialog box, set parameters and click **Save**.



After the configuration is complete, the new entry appears in the email sending configuration list. At the specified time, NTA will automatically send this type of reports.

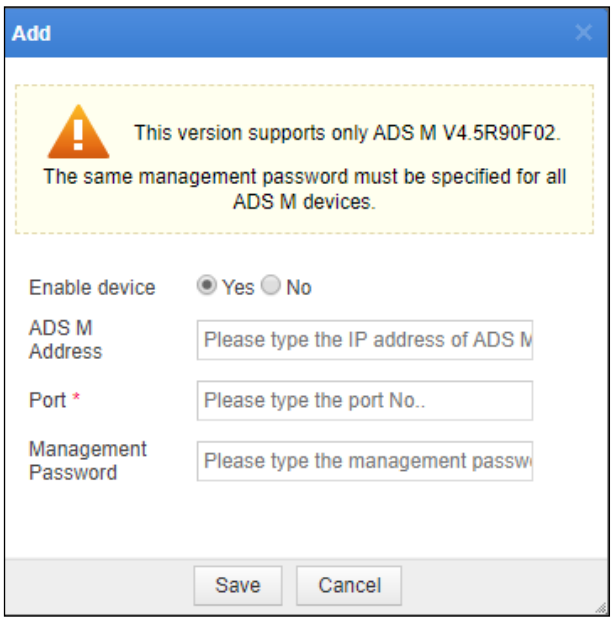


4.16 Port Configurable for Management by ADS M

Configuration and Use

Choose **Administration > Third-Party Interface > Management Mode**, click **Add**, and set parameters, including **Port**, which is a mandatory parameter.

The value range of the port is 1–65535. If an invalid port number is typed, the system prompts that "Please type a valid port number, which must be in the range of 1–65535."



4.17 Custom-Permission User Group Added

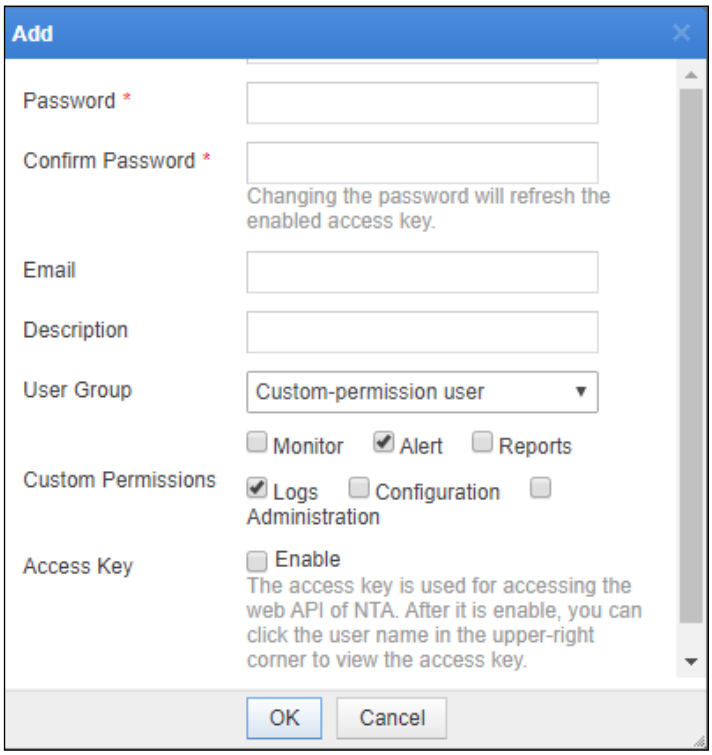
Configuration and Use

Choose **Administration > User Management > Account Configuration** and click **Add**. In the **User Group** drop-down list, a new group, **Custom-permission user**, is added.

If this group is selected, **Custom Permissions** is displayed, including the following information:

□ Monitor □ Alert □ Reports □ Logs □ Configuration □ Administration

One or more such permissions can be selected.



5. Fixed Bugs

- Bug 166073 – NTA completes auto-learning, but "No data" is displayed for some results.
- Bug 162349 – A message prompting a cloud-side authentication error is displayed on a hardware device.
- Bug 168247 – Logs of events that lasted a short time fail to be sent to the cloud cleaning platform.

6. Upgrade Procedure

Note: You must upgrade in strict accordance with the upgrade path.

The upgrade procedure is as follows:

Step 1 Log in to the web-based manager of NTA and choose **Administration** > **System Upgrade**.

Step 2 Browse to **update_nta_V4.5R90F02.200304build34994.bin** and click **Upload**.

Step 3 Read upgrade notes and click **Confirm Upgrade** to start the upgrade.

Step 4 Wait about 5 minutes and then refresh the current page.

Step 5 Click **About** in the upper-right corner of the web-based manager to check the current system version.

a. If **Product Version** is **V4.5R90F02.200304build34994**, the upgrade succeeded.

b. If not, the upgrade failed and you need to contact NSFOCUS technical support.

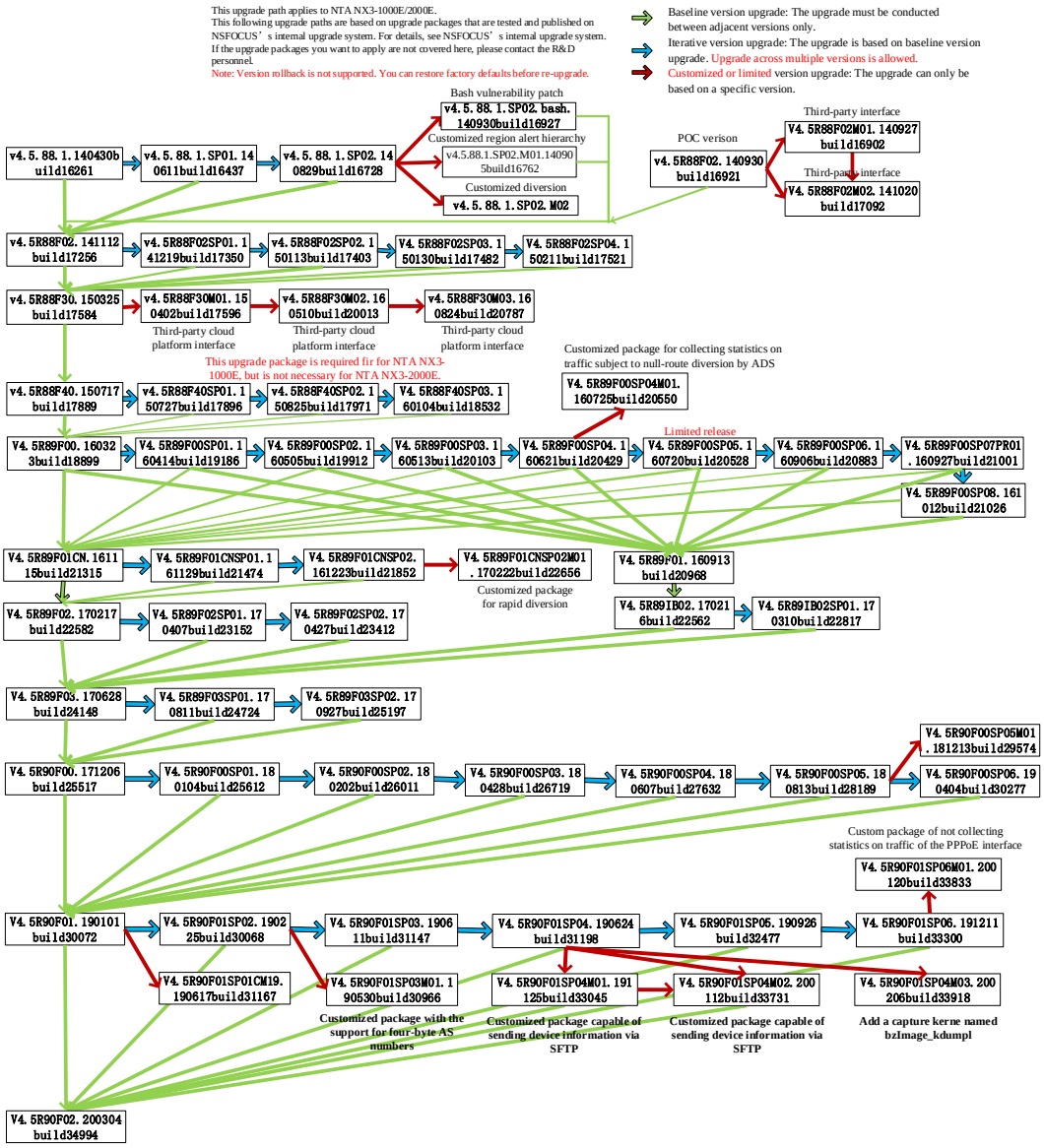
----End

It is normal that the following situations arise during upgrade:

- The web-based manager displays an error message "502 Bad Gateway" for or directly denies your access request.
- All services will stop running.
- The upgrade takes about 5 minutes. If the page remains unresponsive after 5 minutes, you need to manually refresh the page.

Note that the system will automatically restart after the installation is complete.

7. Upgrade Path



8. Appendix

PVD-NTA-V4.5R9
0F02-SFTP Requir