NSFOCUS NTA Release Notes

1. Basic Information

Product Model	• NTA NX3-HD2100 • NTA NX3-HD2200 • NTA NX3-HD3000 • NTA VM • NTA NX5-HD3500 • NTA NX5-HFB6000 • NTA NX5-HFB8000 • NTA NX5-HFB3000 • NTA NX5-HFG10000
Software Version	• V4.5R90F07 • Build: 52467
Upgrade File	• update_nta_x86_V4.5R90F07.251125build52467.bin MD5: 51910029e63b11382c434ee4c004530c • update_nta_hygon_V4.5R90F07.251125build52467.bin MD5: ca407df3525881b6da960c7daf0e8afc • update_nta_arm_V4.5R90F07.251125build52467.bin MD5: c78db9e1dfcc605379ea4c2da0feea96
Release Date	2025-11-30
How to Obtain	Obtain the upgrade file from the upgrade system or contact NSFOCUS technical support.

2. Version Mapping

Source Software Version	• V4.5R90F06, V4.5R90F06SP01, or V4.5R90F06SP02 • V4.5R90F06SP02_M02B00 (for Phytium only)
Product Model	• x86: HD2100, HD2200, HD3000, HD3500, and VM • Hygon: HFB6000 and HFB8000 • Phytium: HFB3000
Management Platform	• ADS M: V4.5R90F07 • ADBOS: V4.5R90F07 • NPAI: 3.2.0
Software Client	None
Browser	• Firefox • Chrome
Documentation	NSFOCUS NTA V4.5R90F07 User Guide

3. Satisfied Requirements and Fixed Bugs

3.1 Satisfied Requirements

Requirement ID	Description	Remarks

3.2 Fixed Bugs

Bug ID	Severity	Type	Function/Component	Description
NTA-14584	Normal	Defect	Administration	[x86] Disabling the **tcp_tw_recycle** kernel parameter is recommended.
NTA-14601	Normal	Defect	Web	[Web] When the high-level alert setting is left blank, the page displays an error message "Sorry, the server cannot handle this request."
NTA-14599	Normal	Defect	Vulnerability scanning	[RSAS scan] RSA key security is enhanced.
NTA-14593	Normal	Defect	Web	[Alert configuration template] The **flowspec redirect_ip** configuration is not verified.
NTA-14588	Normal	Defect	Third-party interface	[Phytium] Forwarding SNMP trap audit logs fails.
NTA-14587	Normal	Defect	Third-party	[Collaboration with ADBOS] After NTA's system time is changed in the web-based

Bug ID	Severity	Type	Function/Component	Description
			interface	manager, the logs of newly triggered alerts fail to be forwarded.
NTA-14579	Trivial	Defect	Log management	[Web] The audit logs for enabling or disabling alert plug-ins are inaccurate.
NTA-14585	Normal	Defect	Web	[Web page] The layout of the **Top 5 DDoS Alerts** information under **Monitor > View** is abnormal.
NTA-14631	Normal	Defect	CBB	The dual-power supply detection occasionally reports alternating Down and Up logs.
NTA-15477	Normal	Defect	Administration	[Phytium] When the NTPD server address is unreachable, restarting the system causes the system time to jump forward by 8 hours.
NTA-15454	Normal	Defect	Third-party interface	[Third-party interface] snmpwalk cannot retrieve the ifSpeed or ifphysAddress information of NTA's 10G interface.
NTA-15790	Normal	Defect	Third-party interface	[Phytium - Third-party interface] Some OIDs cannot retrieve data.
NTA-15485	Normal	Defect	Administration	[NTP service] If either the primary or secondary server address becomes unreachable, a running log records that the NTP service is temporarily unavailable.
NTA-15458	Normal	Defect	Upgrade	[Phytium] Online upgrading of the threat intelligence database fails.
NTA-15765	Normal	Defect	Web	[Web] The maximum number is not applied when IP groups are configured in bulk.

4. Opened Ports

Peer Device	Connection	Protocol	Service	Port	Opened by Default	Configurable
Browser or client	Requesting client – nginx	TCP	nginx	443	☑	☑
Client	Requesting client – SSH	TCP	SSH	50022	☐	☑
Client	Requesting client – SNMP agent	TCP/UDP	SNMP agent	161	☐	☐
Netflow exporter	Netflow collector	UDP	DFI-flow collector engine	9999	☑	☑
sFlow	sFlow collector	UDP	DFI-flow collector	6343	☑	☑

Peer Device	Connection	Protocol	Service	Port	Opened by Default	Configurable
exporter			engine			

5. Function Changes

5.1 New Functions

New Function	Description
Attack detection	Added the traffic anomaly detection feature, including the **Src IP Access Frequency Abnormal**, **Geolocation Abnormal**, **Protocol Proportion Abnormal**, **Attack Signature Detected**, and **Threat Access Abnormal** alert plug-ins.
XC support	Support for the Kingbase database to handle China's homegrown device data.
Ease of use	Support for displaying the SSD/CF card status.
Updated touch point specifications	Support for displaying the common patch version.
Non-Functional Requirements (NFR) reliability	Optimized the device reliability.
License optimization	Removed the requirement that the start time of a new license must be later than that of the existing license.

5.2 Deleted Functions

Function	V4.5R90F06	V4.5R90F07	Impact	Reason for Deletion

5.3 Modified Functions

Function	V4.5R90F06	V4.5R90F07	Impact

6. Detailed Description of Function Changes

6.1 Traffic Anomaly Detection Feature (Including Source IP Access Frequency Abnormal, Geolocation Abnormal, Protocol Proportion Abnormal, Attack Signature Detected, and Threat Access Abnormal Alert Plug-ins)

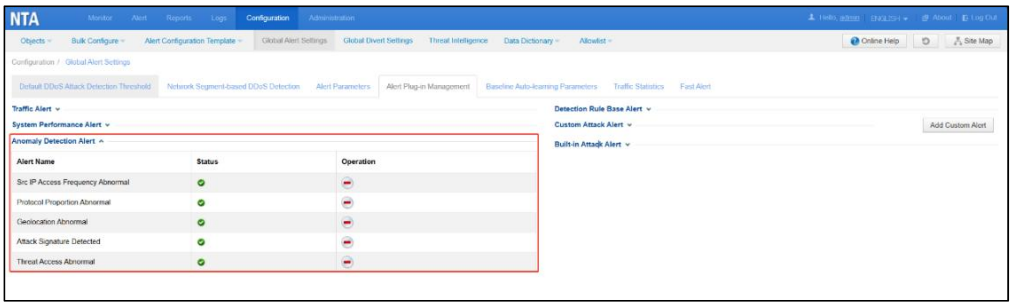
Function Description

The traffic anomaly detection feature is added to a variety of NTA V4.5R90F07 models (including Caswell C236, Caswell C621, HD-Hygon3, Workbeee-Hygon3, HD-Hygon5, Phytium, and Workbeee chassis) in DPI mode.

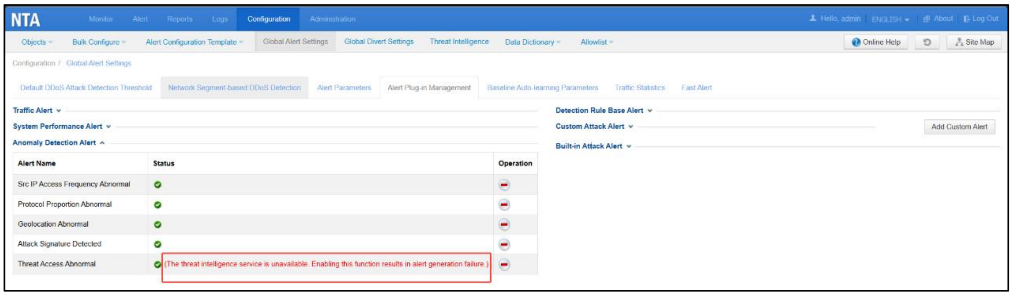
The traffic anomaly detection feature consists of the source IP access frequency anomaly detection, geolocation anomaly detection, protocol proportion anomaly detection, attack signature detection, and threat access anomaly detection.

Configuration

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

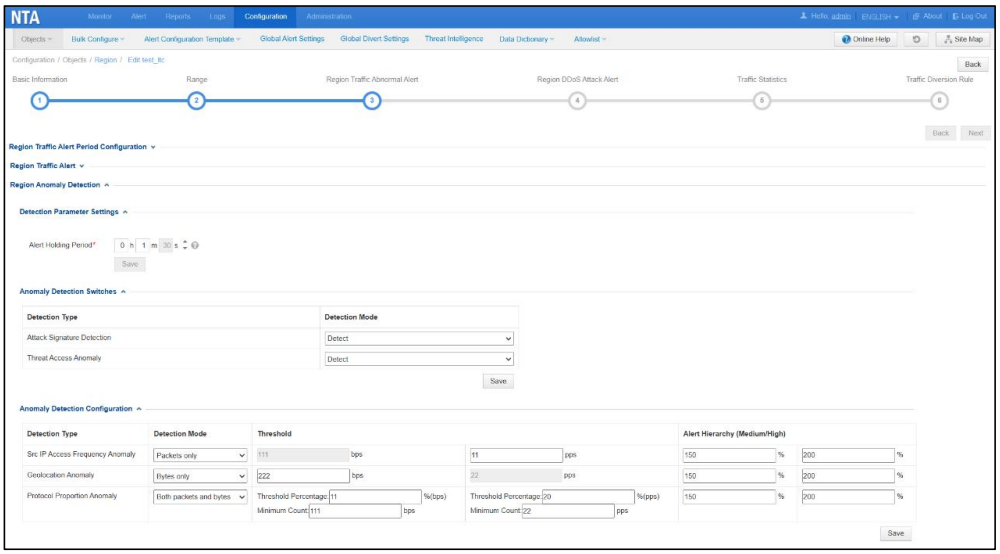


Note that when the licensed threat intelligence service is inactive or expires, the threat access anomaly alert cannot be triggered even if the threat access anomaly feature is enabled.



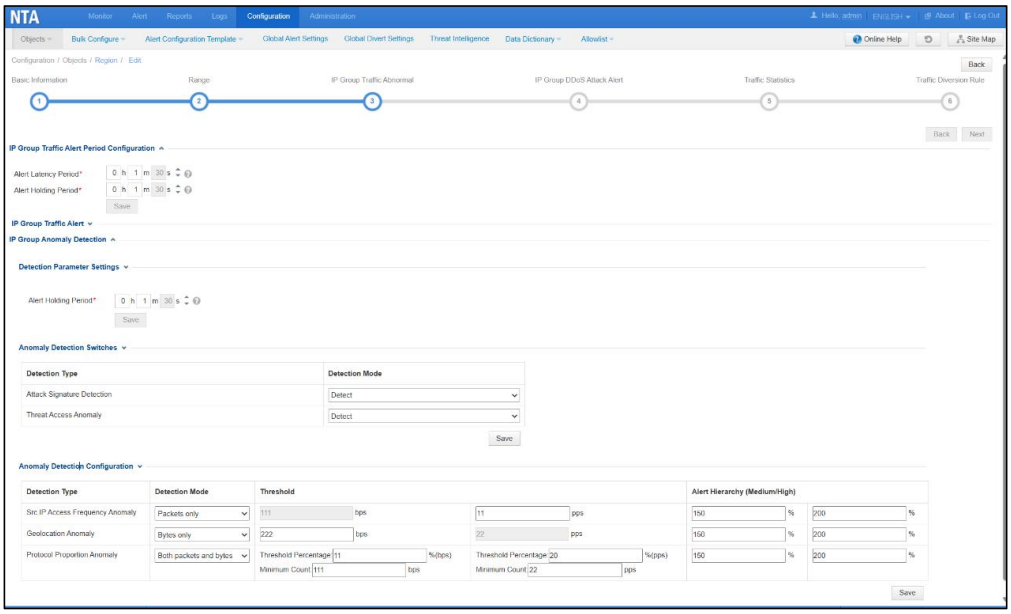
- Region configuration:

  Choose **Configuration > Objects > Region**. Then edit the region configuration under **Region Traffic Abnormal Alert > Region Anomaly Detection**.

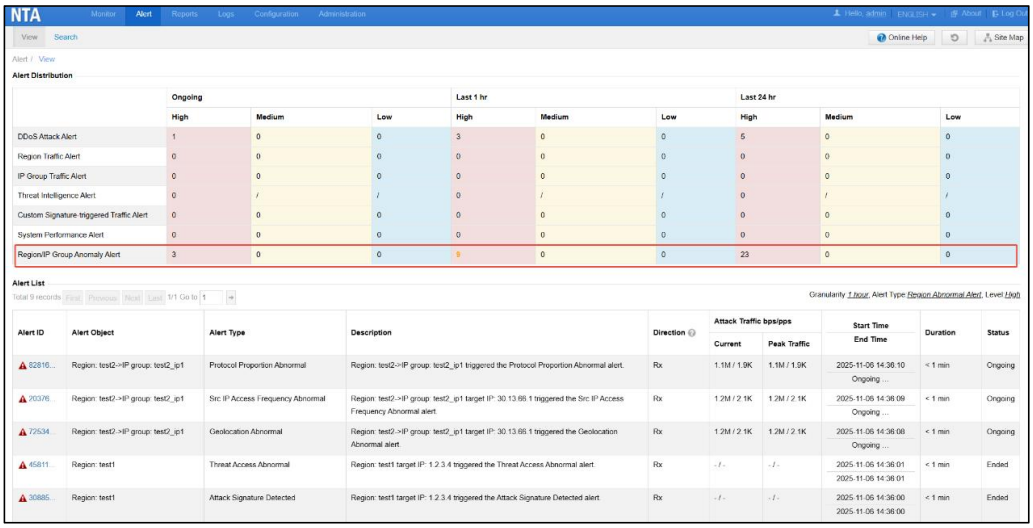


- IP group configuration:

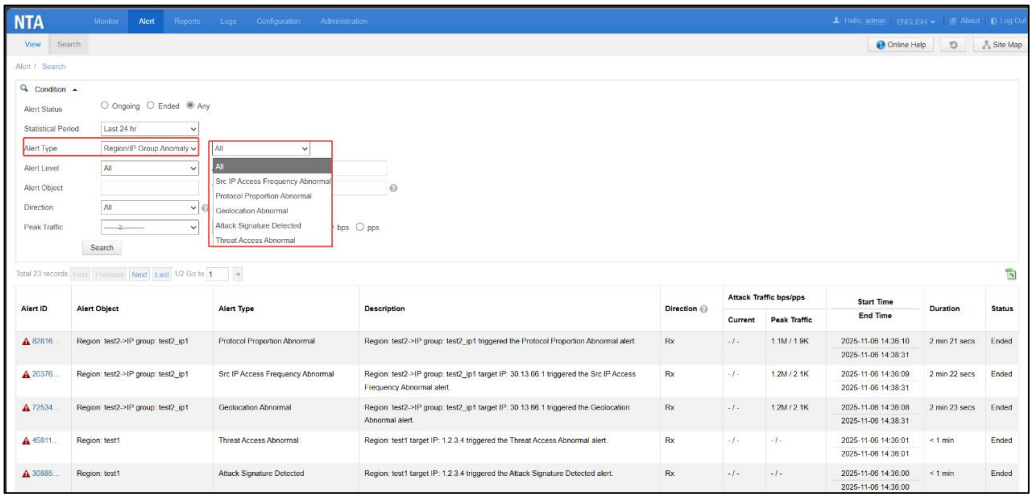
  Choose **Configuration > Objects > Region**. Then click ⊞ in front of a region to edit the IP group configuration under **IP Group Traffic Abnormal > IP Group Anomaly Detection**.



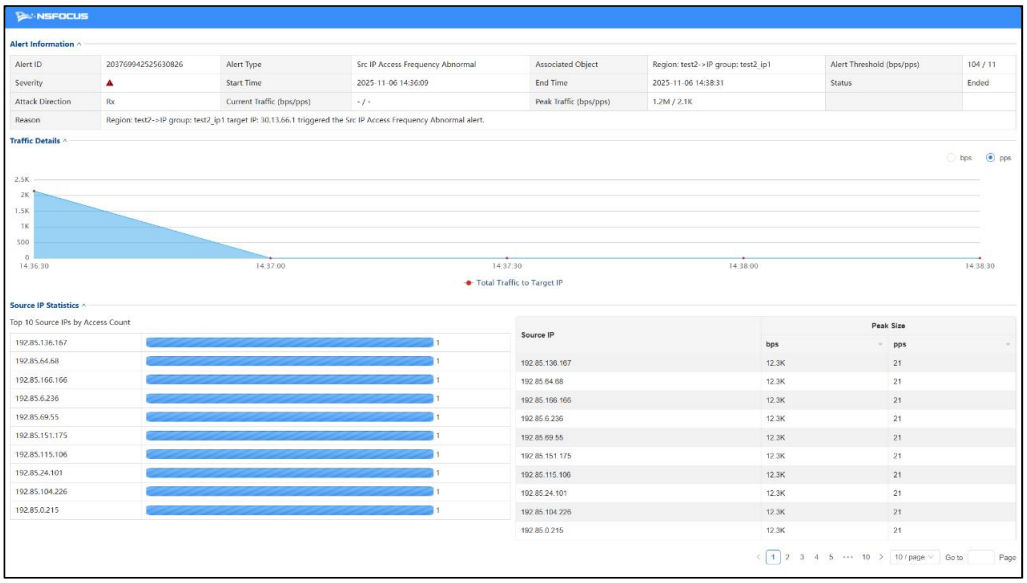
Region/IP Group Anomaly Alert is added under **Alert > View** to display five types of traffic anomaly detection alerts. Among them, source IP access frequency abnormal alerts, geolocation abnormal alerts, and protocol proportion abnormal alerts are displayed by **Ongoing**, **Last 1 hr**, and **Last 24 hr**, while attack signature detected alerts and threat access abnormal alerts are displayed by **Last 1 hr** and **Last 24 hr**.

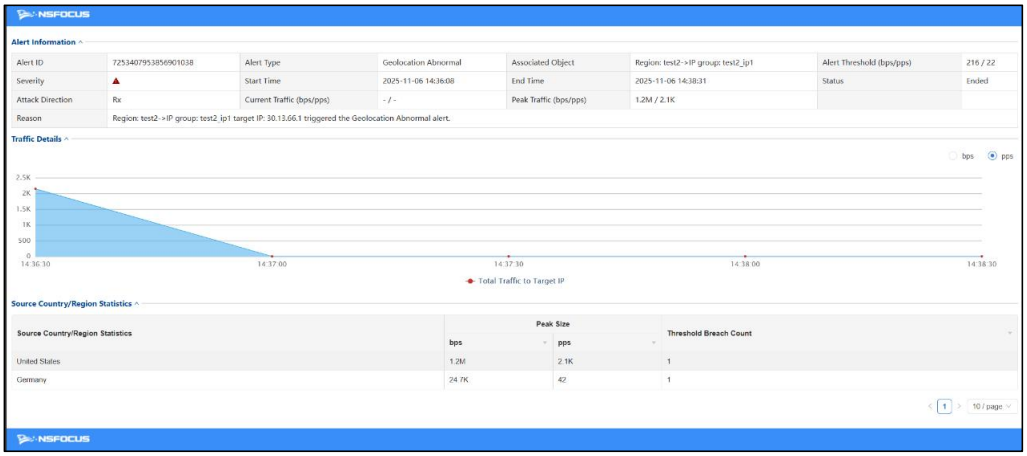


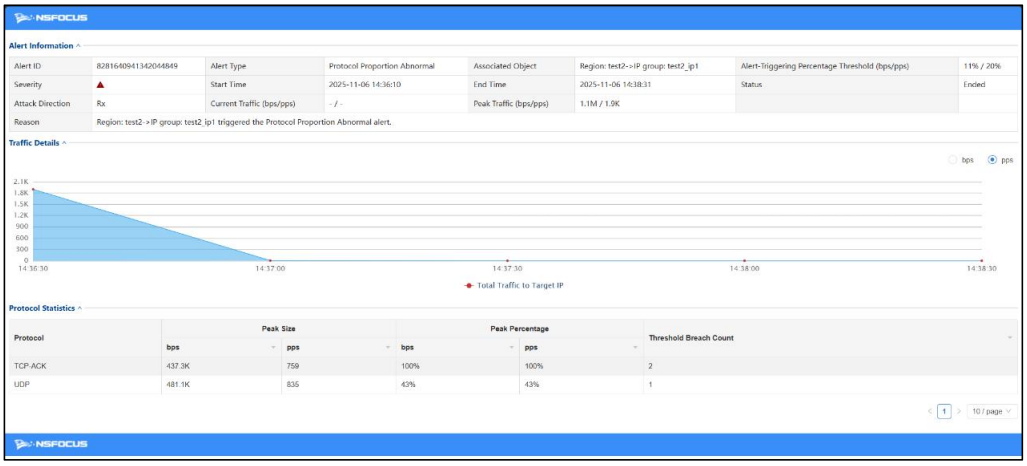
Choose **Alert > Search** to query these five types of traffic anomaly alerts. You can query source IP access frequency abnormal alerts, geolocation abnormal alerts, and protocol proportion abnormal alerts by **Ongoing**, **Ended**, or **Any**, and query attack signature detected alerts and threat access abnormal alerts by **Ended** or **Any**.

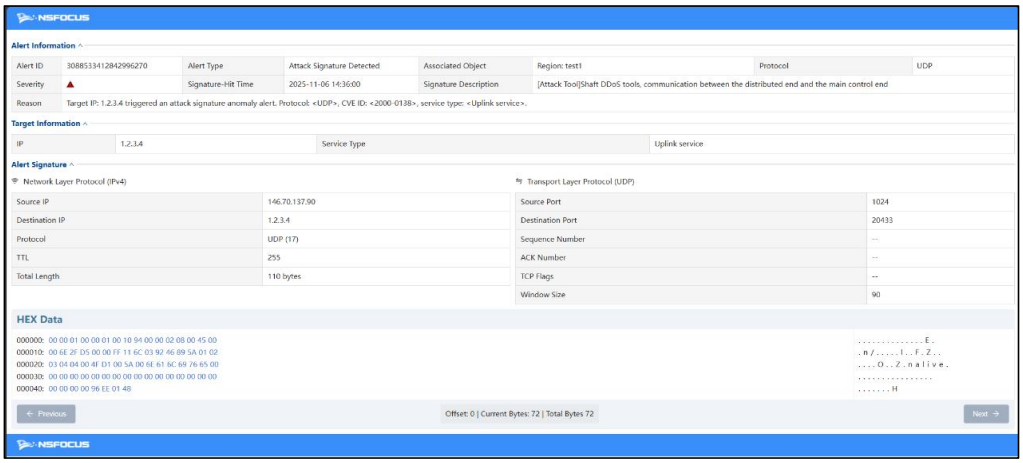


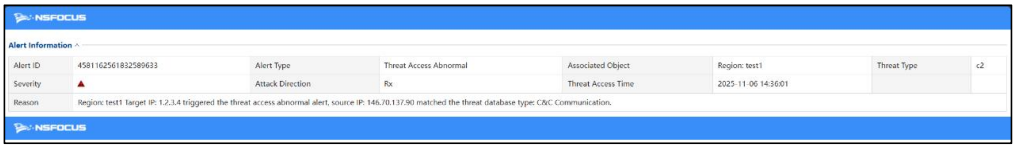
Choose **Alert > View/Search**. On the **View** or **Search** page, click an alert ID in the alert list to view alert details.


NSFOCUS
Alert Information
Alert ID 203769942525630826
Alert Type Src IP Access Frequency Abnormal
Associated Object
Region: test2->IP group: test2_ip1
Alert Threshold (bps/pps) 104 / 11
Severity
Start Time 2025-11-06 14:36:09
End Time 2025-11-06 14:38:31
Status Ended
Attack Direction Rx
Current Traffic (bps/pps) - / -
Peak Traffic (bps/pps) 1.2M / 2.1K
Reason Region: test2->IP group: test2_ip1 target IP: 30.13.66.1 triggered the Src IP Access Frequency Abnormal alert.
Traffic Details
bps pps
Total Traffic to Target IP
Source IP Statistics
Top 10 Source IPs by Access Count
Source IP
Peak Size
bps
pps
192.85.136.167 12.3K 21
192.85.64.68 12.3K 21
192.85.166.166 12.3K 21
192.85.6.236 12.3K 21
192.85.69.55 12.3K 21
192.85.151.175 12.3K 21
192.85.115.106 12.3K 21
192.85.24.101 12.3K 21
192.85.104.226 12.3K 21
192.85.0.215 12.3K 21


NSFOCUS
Alert Information
Alert ID 7253407953856901038
Alert Type Geolocation Abnormal
Associated Object
Region: test2->IP group: test2_ip1
Alert Threshold (bps/pps) 216 / 22
Severity
Start Time 2025-11-06 14:36:08
End Time 2025-11-06 14:38:31
Status Ended
Attack Direction Rx
Current Traffic (bps/pps) - / -
Peak Traffic (bps/pps) 1.2M / 2.1K
Reason Region: test2->IP group: test2_ip1 target IP: 30.13.66.1 triggered the Geolocation Abnormal alert.
Traffic Details
bps pps
Total Traffic to Target IP
Source Country/Region Statistics
Source Country/Region Statistics
Peak Size
bps
pps
Threshold Breach Count
United States 1.2M 2.1K 1
Germany 24.7K 42 1
NSFOCUS


NSFOCUS
Alert Information
Alert ID 828164094134204849
Alert Type Protocol Proportion Abnormal
Associated Object
Region: test2->IP group: test2_ip1
Alert-Triggering Percentage Threshold (bps/pps) 11% / 20%
Severity
Start Time 2025-11-06 14:36:10
End Time 2025-11-06 14:38:31
Status Ended
Attack Direction Rx
Current Traffic (bps/pps) - / -
Peak Traffic (bps/pps) 1.1M / 1.9K
Reason Region: test2->IP group: test2_ip1 triggered the Protocol Proportion Abnormal alert.
Traffic Details
bps pps
Total Traffic to Target IP
Protocol Statistics
Protocol
Peak Size
Peak Percentage
Threshold Breach Count
bps
pps
TCP-ACK 437.3K 759 100% 100% 2
UDP 481.1K 836 43% 43% 1
NSFOCUS





After you configure the management platform under **Administration > Third-Party Interface**, these five types of alerts can be forwarded to ADS M. You can also configure a cloud scrubbing platform with **Send Syslog** enabled under **Administration > Third-Party Interface** to forward alerts to ADBOS.

Post-Upgrade Notes

Only NTA in DPI mode supports the five types of traffic anomaly alerts. After NTA is upgraded to V4.5R90F07, the global switch for the five alert plug-ins is disabled by default, and the individual switches for these alert plug-ins are also disabled for the configured region or IP group.

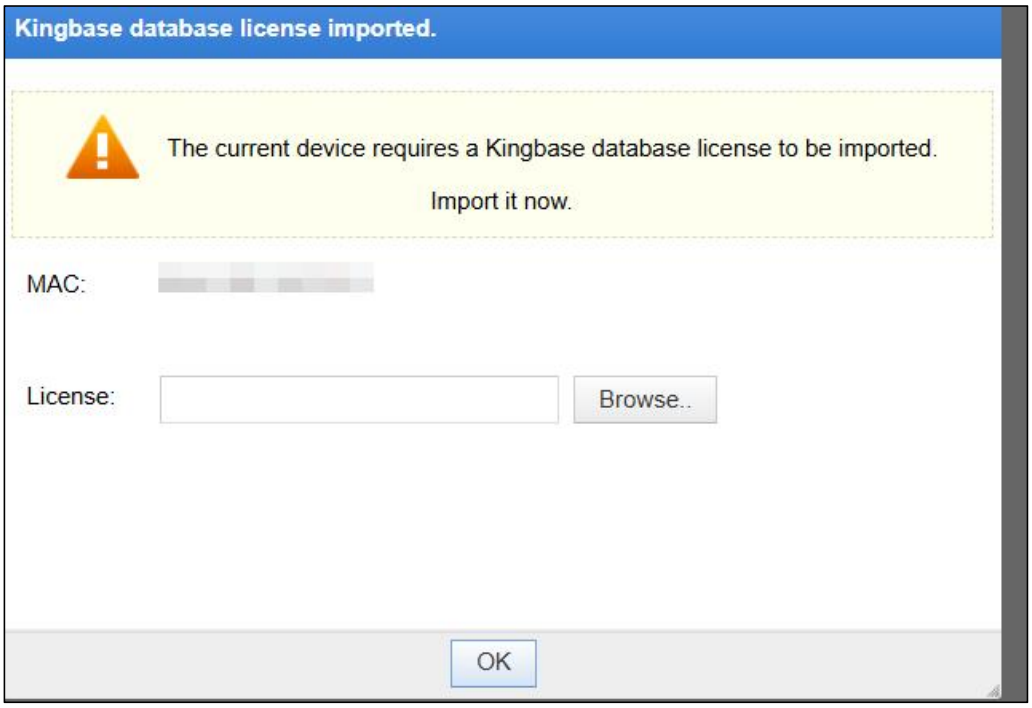
6.2 Support for the Kingbase Database to Handle China's Homegrown Device Data

Function Description

The support for the Kingbase database is added to handle China's homegrown device data. NTA HFB3000, HFB6000, HFB8000, and HFG10000 allow selecting either Kingbase or PostgreSQL during production. After production, the selected database cannot be changed.

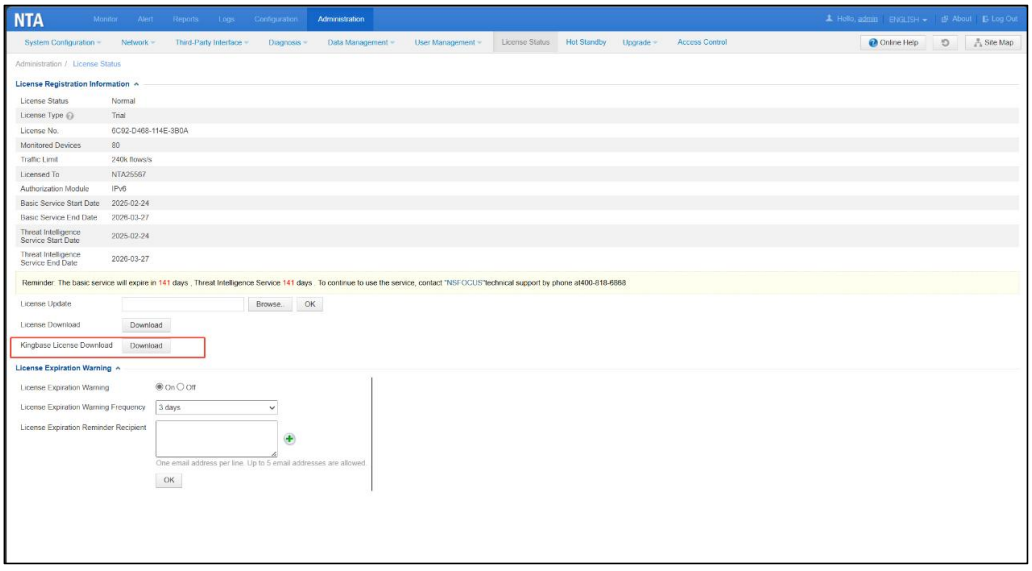
Configuration

NTA produced with the Kingbase database can function normally only if a valid Kingbase database license is imported.



To download the Kingbase database license, do as follows:

Choose **Administration > License Status**. In the **License Registration Information** area, click **Download** to download it.



Post-Upgrade Notes

After NTAs prior to V4.5R90F07 are upgraded to V4.5R90F07, they continue to use the PostgreSQL database.

6.3 Displaying the SSD/CF Card Status

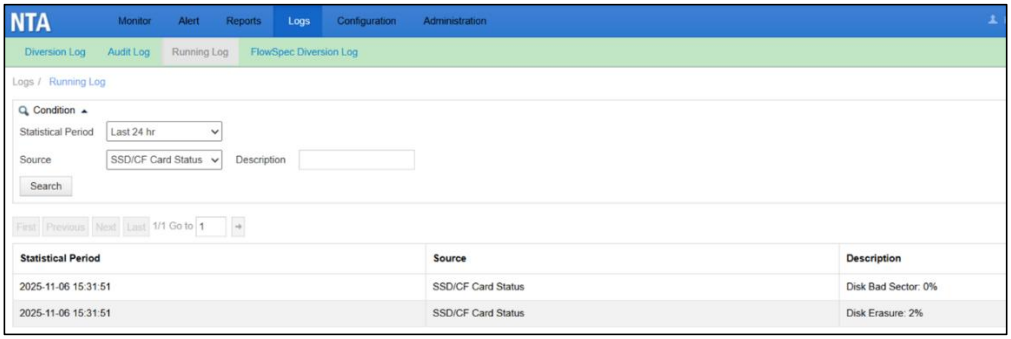
Function Description

- The **show diskhwinfo** command is added to display the SSD version information via the CLI. For details, see *NTA V4.5R90F07 Command Line User Guide*.
- The SSD/CF card status is also displayed in the web-based manager.

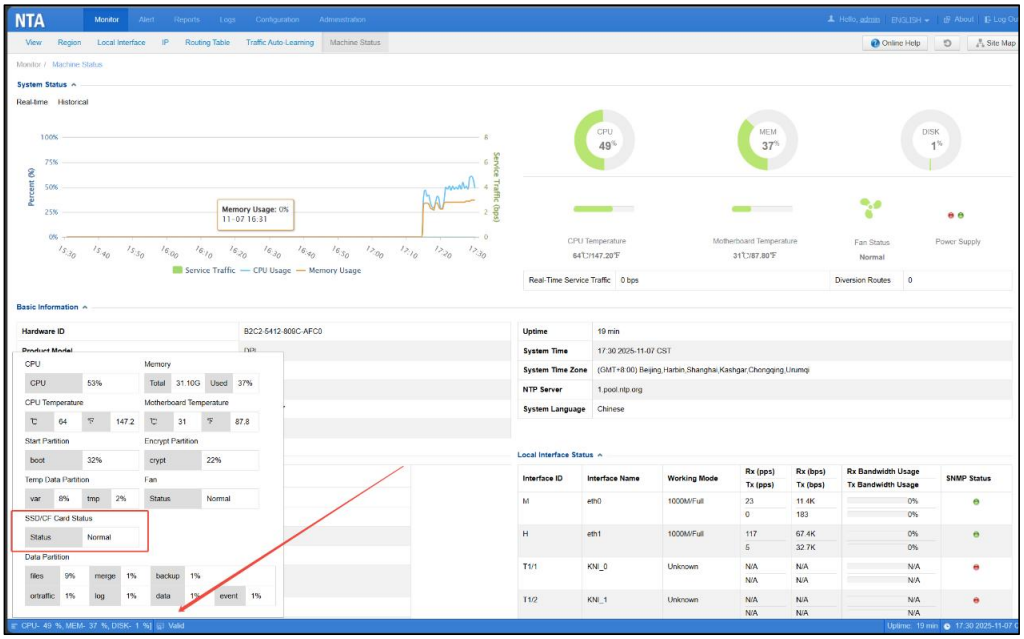
Configuration

No configuration is required.

Choose **Logs > Running Log** to query abnormal SSD/CF card status logs.



You can view the SSD/CF card status in the lower-left corner of NTA's web-based manager.



Post-Upgrade Notes

After the hardware model is upgraded to V4.5R90F07, the SSD/CF card status is displayed automatically.

6.4 Displaying the Common Patch Version

Function Description

The common patch version (H version) is released to address two scenarios:

- A single common upgrade package can upgrade NTA from multiple versions to the target version, simplifying the release workflow and reducing O&M and upgrade management complexity.
- Critical vulnerabilities or defects can be quickly fixed through an upgrade, reducing security risks.

The release notes should clearly describe the fixed bugs and specify the upgrade package to be used. Upgrading the common patch version should not affect the display of the system software version, and the patch version should be shown separately. The common patch version should be incorporated into the latest released F or SP version. For the same baseline version, a maximum of five common patch versions can be released consecutively.

Configuration

Choose **Administration > Upgrade > System Software Upgrade** to upload the common patch upgrade package for upgrade. After the upgrade, the **Software Version** parameter in the upgrade history list, which formerly showed an F type, can now show either an F or an SP version. Additionally, the previous **Patch Version** parameter, which showed an SP version, is renamed to **Common Patch Version** and now shows an H version.

Choose **Monitor > Machine Status > Basic Information**. The **Software Version** parameter, which previously showed an F version, can now show either an F or an SP version. The previous **Patch Version** parameter, which showed an SP version, is renamed to **Common Patch Version** and now shows an H version. If there are multiple H versions, the latest one is displayed, and you can click  to view the remaining ones.

Post-Upgrade Notes

Upgrading the common patch version is not supported for NTA versions prior to V4.5R90F07. Once NTA is upgraded to V4.5R90F07, the common patch version can be upgraded.

6.5 Optimizing Device Reliability

Function Description

The fault diagnosis and serial port reliability functions are added to NTA V4.5R90F07. In addition, monitoring of NTA software and hardware components is added to support future fault analysis.

Configuration

No configuration is required.

Post-Upgrade Notes

None.

6.6 Removing the Requirement That the Start Time of the New License Must Be Later Than That of the Existing License

Function Description

The previous restriction on importing a new license under **Administration > License Status** is removed. When users import a new license to NTA, it can be imported successfully even if its start time is earlier than that of the existing license.

Configuration

No configuration is required.

Post-Upgrade Notes

None.

7. Version Application

7.1 Upgrade

7.1.1 Version Upgrade

Applicable Device Models

HD2100, HD2200, HD3000, HD3500, VM, HFB6000, HFB8000, and HFB3000

Constraints

Upgrades must be performed from base version V4.5R90F06 or later. If the current version is lower than V4.5R90F06, first upgrade it to V4.5R90F06 or later according to the required upgrade route; otherwise, the upgrade will fail.

Impact

The network connection will be interrupted during the upgrade. Before upgrading a custom version, check whether customized functions will be affected by the upgrade.

Procedure

Step 1 Choose **Administration > Upgrade > System Software Upgrade**.

Step 2 In the **System Upgrade** area, browse to **update_nta_x86_V4.5R90F07.251125build52467.bin, update_nta_hygon_V4.5R90F07.251125build52467.bin**, or **update_nta_arm_V4.5R90F07.251125build52467.bin** and click **Upload**.

Step 3 Read release notes and, if nothing is wrong, 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.

If **Product Version** is **V4.5R90F07.251125build52467**, the upgrade succeeded. If not, the upgrade failed and you need to contact NSFOCUS technical support for help.

----End

It is normal that the following situations arise during the upgrade:

- The web-based manager displays an error message "502 Bad Gateway" for or directly denies your access request.
- All services are unavailable.
- 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 upgrade is complete.

7.1.2 Version Rollback

After the upgrade, NTA cannot be rolled back to the previous versions.

7.2 Constraints

None.