NTA V4.5R90F00SP02 Release Notes

V4.5R90F00SP02 (2018-02-02)

Contents

1 Basic Information

Product Model	NTA NX3-2000E/1000E
Software Version	V4.5R90F00SP02
Upgrade File	update_nta_V4.5R90F00SP02.180202build26011.bin MD5: 563f69abda78fe8dc768db47319bc623
Release Date	2018-02-02
How to Obtain	Obtain the upgrade file from the upgrade system or contact technical support personnel of NSFOCUS.

2 Version Mapping

Product Model	NTA NX3-2000E/1000E (NSF-2800)
ADS M	V4.5R90F00SP01
ADS	V4.5.88.15 V4.5R90F00SP01
Threat Analysis and Traceback System (TAT)	V2.0.0
Client Browser	Chrome Firefox IE 10
Documentation	NSFOCUS NTA Installation Guide/User Guide (V4.5R90F00)

3 Satisfied Requirements

No.	Requirement Description
1	Process status monitoring should be added.
2	Descriptions should be added to interface configuration.
3	Interface traffic should be displayed on the web-based manager.
4	Region and IP group names should be editable.
5	For the IP address range of a region, the new version should supports addition of consecutive IP segments.
6	Configuration of custom alerts should be optimized.
7	Alert query should be optimized.
8	The port for web-based management of NTA should be changed to another one.
9	During loading of data, the loading progress should be displayed dynamically.
10	For the traffic trend graph, traffic at a certain point of time should be displayed wherever the mouse is hovered.
11	For flow handling, netstream_v9 should be available for selection.
12	The CPU temperature, mainboard temperature, and fan status should be via SNMP GET requests.
13	The license error message on the web-based manager should optimized.
14	As for template application, regions and IP groups should be able to be retrieved by name.
15	The API description document should be updated.
16	Reports should show the statistical period.
17	The syslog alert log should show the object to which an IP address belongs.
18	Some bugs should be fixed.

4 Upgrade Procedure

The source version for the upgrade must be V4.5R90F00 or V4.5R90F00SP01.

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 the upgrade file **update_nta_V4.5R90F00SP02.180202build26011.bin** and click **Upload**.

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

Step 4 Wait 5 minutes for the installation to complete before refreshing the current page. Click **About** in the upper-right corner of the web-based manager to check the current system version. If **Product Version** is **V4.5R90F00SP02**, the upgrade succeeded. If not, the upgrade failed and you need to contact NSFOCUS technical support.

----End

It is normal that the following situations arise during upgrade:

1. The SSH client is disconnected.
2. The web-based manager displays an error message "502 Bad Gateway" or directly denies your access request.
3. All engines stop working.

The installation takes about 5 minutes. Later, you need to manually refresh the page.

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

5 Function Changes

5.1 Addition of Process Status Monitoring

Scenario

A key process such as nginx and memcached may fail during NTA maintenance. Due to the lack of automatic recovery means, users have to turn to NSFOCUS's R&D personnel, who will troubleshoot and restore the process in the background. Also, logs should be recorded once a key process fails.

Configuration and Use

Process status monitoring is added in the NTA background so that NTA, every five minutes, checks the status of key processes such as nginx, memcached, ttserver, postgres, HA, and collaboration with BSA. For vNTA, monitoring of the A interface daemon used for cloud-based authentication is added in addition to process status monitoring.

If one of the preceding key processes exits, start the process.

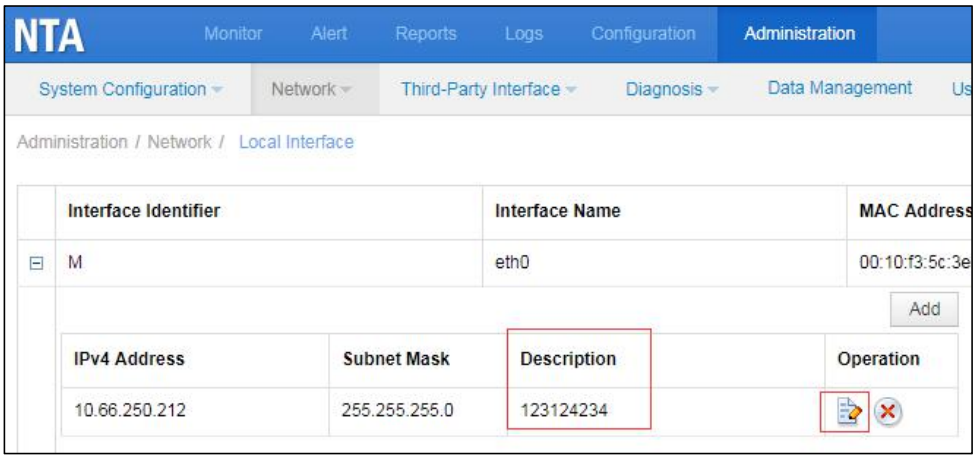
5.2 Description Added for Interface Configuration

Scenario

Interface descriptions (such as interface uses, peer device name and interface, and peer IP address) are added to facilitate operation and maintenance (O&M).

Configuration and Use

Choose **Administration > Network > Local Interface**. Click **Add** to add an IP address for an interface. You can add and edit interface descriptions.



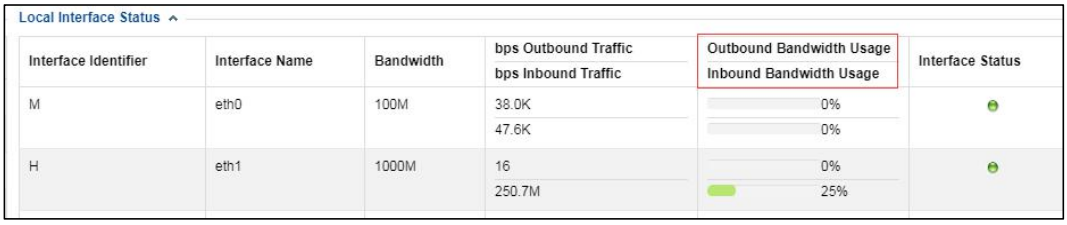
5.3 Interface Traffic Displayed on the Web-based Manager

Scenario

Sometimes, NTA monitors multiple routers, and therefore needs to analyze a great number of flows. In case a management interface is used to receive flows at the speed of 100 Mbps negotiated with low-performance peer switches, congestion may even occur due to the limited bandwidth of the interface. If interface traffic is displayed on the web-based manager, users will be able to make the wise choice of using more interfaces or 10 Gb interfaces to receive flows before they become too large to be handled by the current interface.

Configuration and Use

Choose **Monitor > Machine Status**. The **Local Interface Status** area shows the inbound traffic (bps), outbound traffic (bps), and bidirectional bandwidth usage.



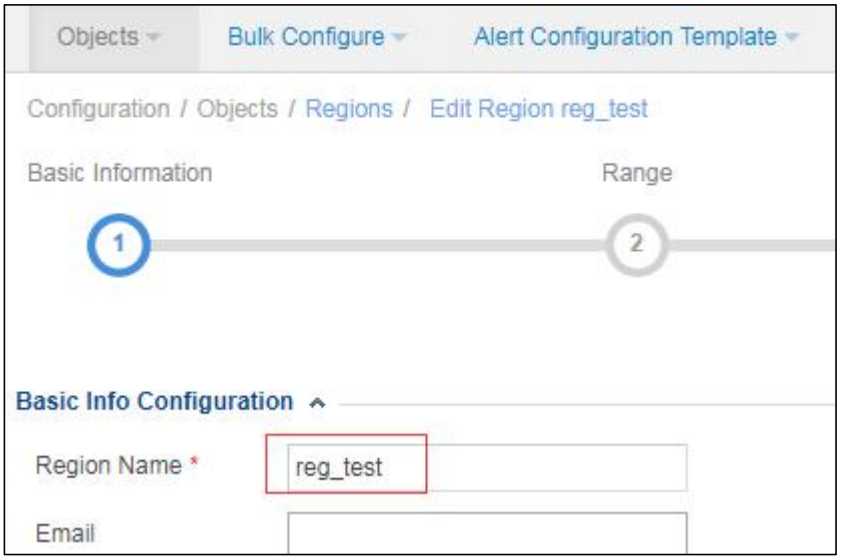
5.4 Region and IP Group Names Being Editable

Scenario

Once a region is defined, its name cannot be changed. In this case, if related business is adjusted, the user must first delete the existing region and then create a new one. This makes O&M inconvenient.

Configuration and Use

Choose **Configuration > Objects > Regions**. Click in the **Operation** column of a region to edit region settings. You can see that the region name is editable.



5.5 Addition of Consecutive IP Segments for a Region

Scenario

The IP address range of a region, for example, 1.2.3.4–1.2.100.200, which cannot be specified with the netmask, needs to be split into several segments. It is really a cumbersome process.

Configuration and Use

Choose **Configuration > Objects > Regions**. An IP address range which involves more than one IP segment (must be within a /24 subnet) can be specified in the format of start IP address-end IP address, for example, 1.2.3.4-1.2.100.200.

5.6 Optimization of Custom Alert Configuration

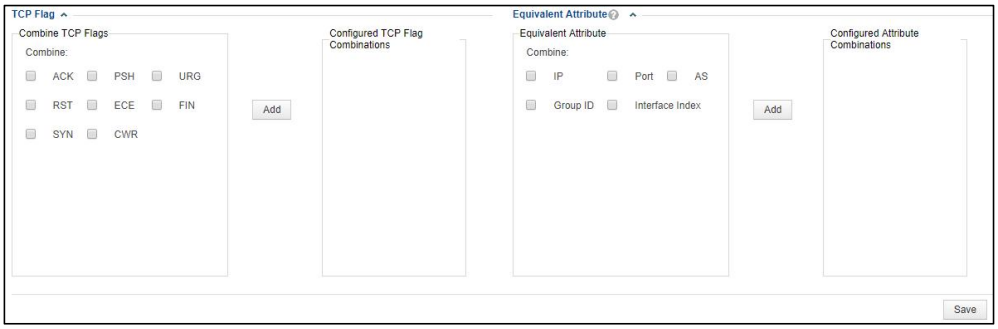
Scenario

For custom attack alerts, the way TCP flags and equivalent attributes are configured is not easy to understand and should be optimized.

Configuration and Use

Choose **Configuration > Global Alert Settings > Alert Plug-in Management**. In the **Custom Attack Alerts** area, click in the **Operation** column of an alert. On the **Add Feature** page, the **TCP Flag** and **Equivalent Attribute** areas are optimized.

If you point to next to **Equivalent Attribute**, the system prompts "The equivalent attribute indicates that values of the source and destination attributes, such as source and destination IP addresses or source and destination ports, are the same."



5.7 Alert Query Optimization

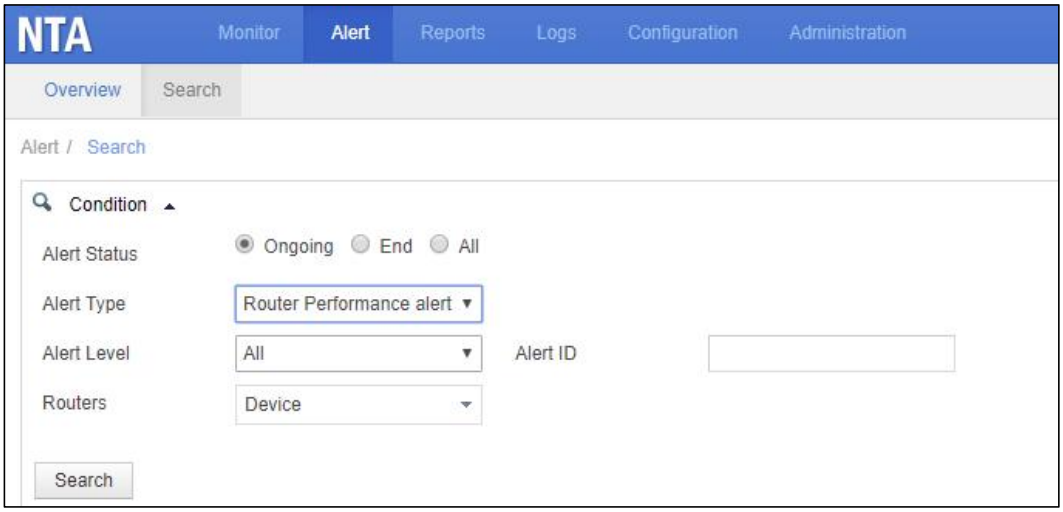
Scenario

When a specific alert type is selected, certain irrelevant query conditions are also displayed, which may confuse and mislead users. Therefore, the display of alert query conditions should be optimized.

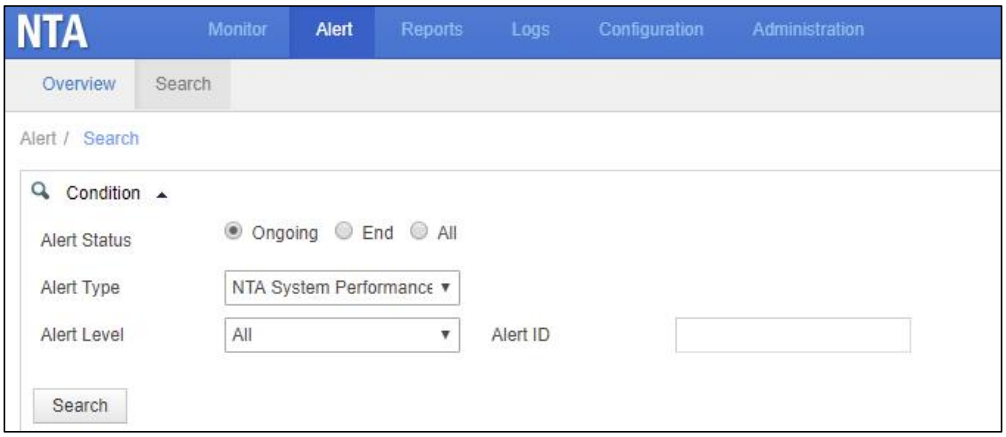
Configuration and Use

On the alert query page, only query conditions that are relevant to the selected alert type are displayed.

Choose **Alert > Search**. When **Router Performance Alert** or **Router Interface Bandwidth Alert** is selected for **Alert Type**, only **Alert Level**, **Alert ID,** and **Routers** are displayed for alert filtering.



If **NTA System Performance Alert** is selected for **Alert Type**, only **Alert Level** and **Alert ID** are displayed for alert filtering.



If other alert types are selected, default query conditions are displayed for alert filtering.

5.8 Port for Web-based Management Being Editable

Scenario

On NTA, port 443 is used for web-based management, which cannot be changed. However, according to compliance requirements, port 443 cannot be used for web-based management, and therefore another port should be able to be specified.

Configuration and Use

Choose **Administration > System Configuration > Basic Information**. The **Web Port Management** area is added to allow users to specify a port for web-based management.

After a new port is specified, the system prompts you to restart the web service.

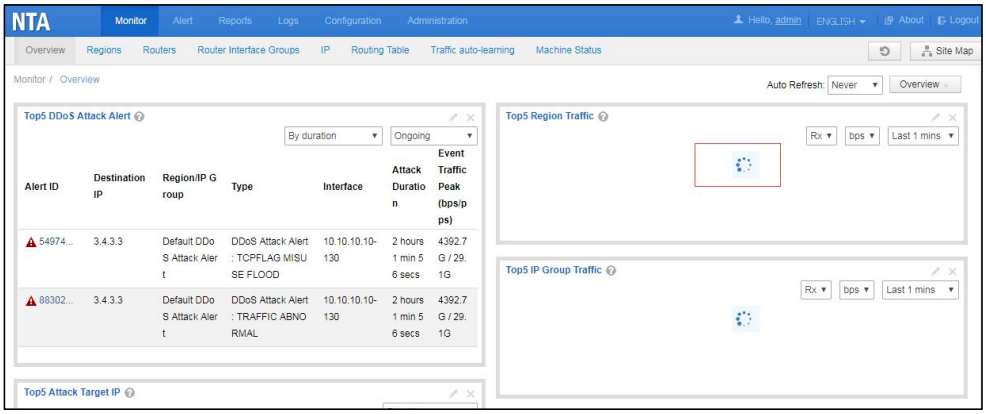
5.9 Dynamic Loading Progress Displayed During Loading of Data

Scenario

Sometimes, when the **Overview** page under **Monitor** is opened, panels are blank due to the slow data loading. This is easily mistaken for no data or a function failure. To make the web-based manager more user-friendly, the dynamic loading progress is displayed.

Configuration and Use

Choose **Monitor > Overview**. During the loading of data on panels, the system displays the dynamic loading progress.



5.10 Hovering the Mouse Over a Certain Point of Time to Show Traffic Information on a Traffic Trend Graph

Scenario

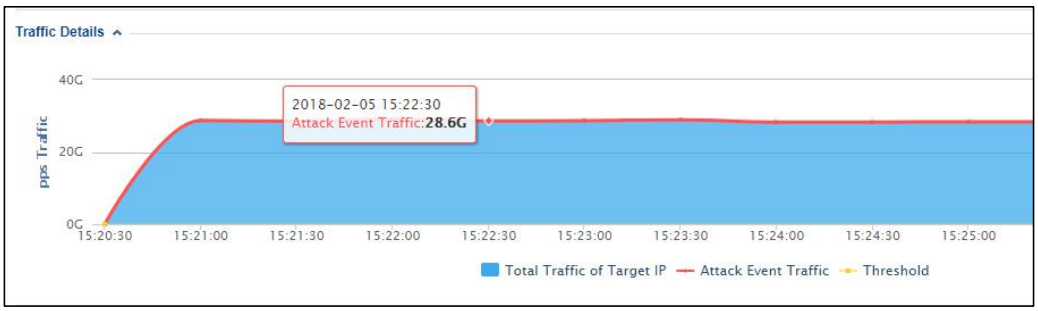
On a traffic trend graph panel under **Monitor**, hovering the mouse over a certain point of time does not show related traffic information, making it inconvenient to use.

Configuration and Use

For traffic trend graphs on the following pages, traffic at a certain point of time is displayed wherever the mouse is hovered:

- **Routers**, **Router Interface Groups**, and **IP** pages under **Monitor**
- **Basic Information** page and top 5 statistics pages that open upon a click on an alert
- **DDoS Attack Report** page

For example, click an alert to open the **Basic Information** page. In the **Traffic Details** area of this page, when the mouse is hovered over a certain point of time, related traffic information is displayed.



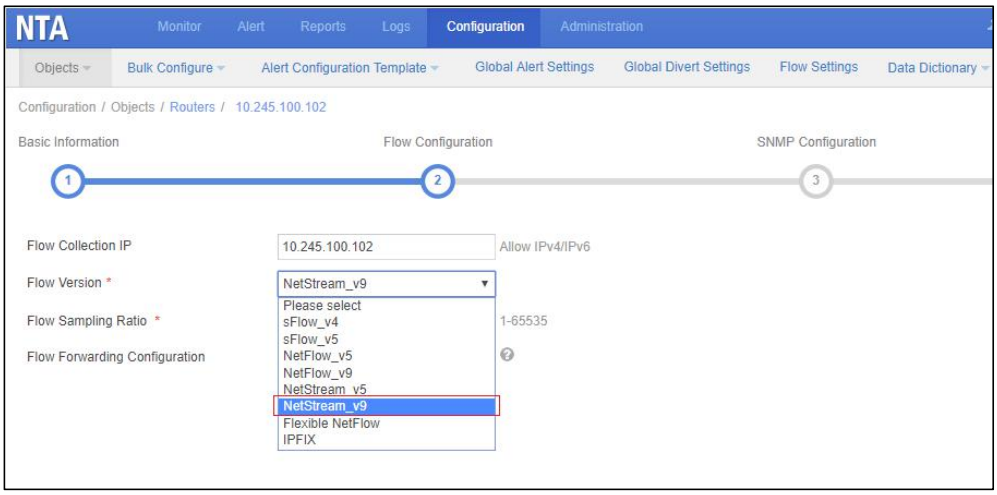
5.11 NetStream V9 Available for Flow Handling

Scenario

Huawei NetStream V9 has exactly the same format as Cisco NetFlow V9. As there is no NetStream V9 option on the web-based manager, users have to select **NetFlow_v9** for parsing of NetStream V9 flows. Therefore, NetStream V9 should be added as an option for flow handling.

Configuration and Use

Choose **Configuration > Objects > Routers**. Click a router name and then click **Edit**. Under **Flow Configuration**, **NetStream_v9** is added for **Flow Version**.



5.12 CPU Temperature, Mainboard Temperature, and Fan Status Obtained via SNMP GET Requests

Scenario

As the network management platform needs to monitor the status of all devices under it, such devices should allow the platform to obtain the CPU temperature, mainboard temperature, and fan status via SNMP GET requests.

Configuration and Use

The CPU temperature, mainboard temperature, and fan status are added as leaf nodes whose values can be obtained via SNMP GET requests.

- CPU temperature: 1.3.6.1.4.1.19849.4.6.2.4
- Mainboard temperature: 1.3.6.1.4.1.19849.4.6.2.5
- Fan status: 1.3.6.1.4.1.19849.4.6.2.6

For details, choose **Administration > Third-Party Interface > SNMP Service** and download the SNMP description document.

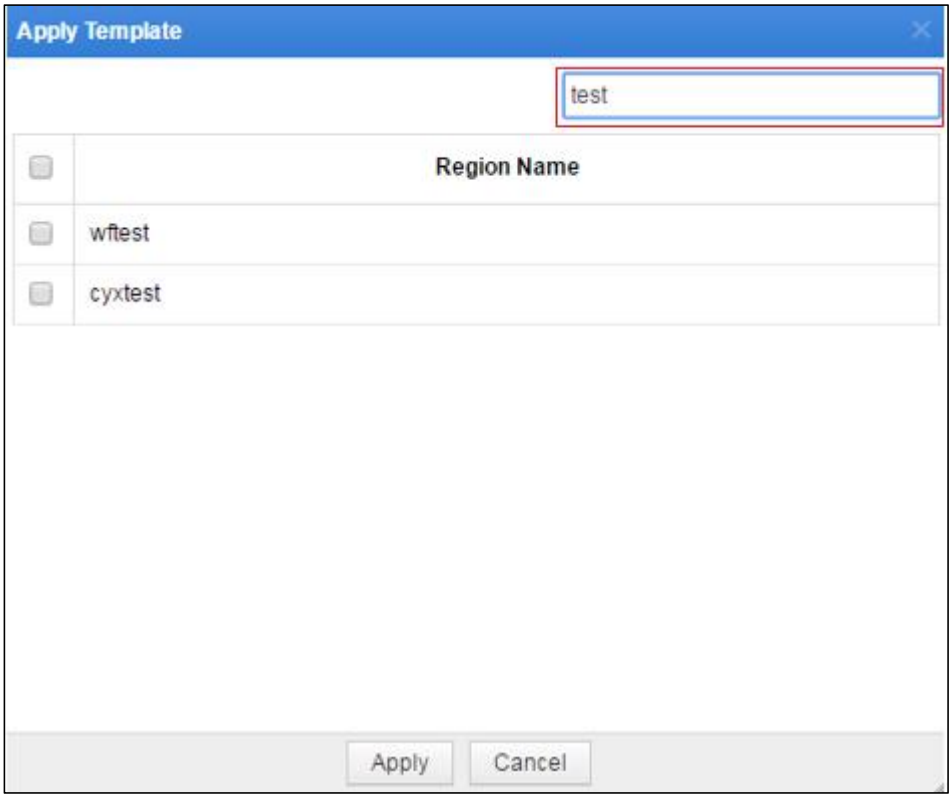
5.13 Support for Search for Regions and IP Groups by Name During the Application of an Alert Configuration Template

Scenario

During the application of an alert configuration template for a region or an IP group, users can only find the desired region or IP group with the unaided eye. In the case of a great many regions or IP groups, it is difficult to spot the desired one. Therefore, the page should support the search for regions or IP groups.

Configuration and Use

Choose **Configuration > Alert Configuration Template > Region Alert Template/IP Group Alert Template**. Click in the **Operation** column of an alert template to apply it. In the **Apply Template** dialog box, you can easily find the desired region or IP group by typing the keyword in the search box.



5.14 Updated API Description Document

The API that obtains the region list is updated.

The API and example for diversion setting modification are updated.

The following prompt is added: A default policy is available for all types of diversion and can be modified only. This default policy does not specify the traffic range, but only specifies the diversion type and protection device.

5.15 Statistical Period Shown in Reports

Scenario

The start time and end time of data query should be indicated in reports.

Configuration and Use

In traffic reports and DDoS attack reports, the statistical period is added below the statistical object to make it clear on which period of data this report is based.

5.16 Syslog Alert Log Showing the Object to Which an IP Address Belongs

Scenario

The object (for example, a region name) to which an attacked IP address belongs should be added to syslog alert logs so that users can determine which service is under attack.

Configuration and Use

The **Alert Object** field is added to syslog alert logs to indicate the object to which the attacked IP address belongs. The following is an example of a default DDoS attack alert sent via syslog:

Default DDoS Attack Alert; Region: test

6 Fixed Bugs

Bug 120290: As the system root directory disappears and cannot be mounted, the system reports the "NSF file handle" error.

Bug 133458: sFlow statistics on Huawei's high-end series of switches are incorrect.

Bug 133482: The source version for update is not properly displayed.

Bug 133478 Cloud-based authentication issues.

7 Compatibility

Browser: Chrome, Firefox, and Internet Explorer 10, with the former two recommended

ADS: V4.5R90F00SP01 and V4.5.88.15

ADS M: V4.5R90F00SP01

TAT: V2.0.0