

NSFOCUS ADS Release Notes

1. Basic Information

Product Model	<ul style="list-style-type: none"> • ADS NX3-800E • ADS NX3-2020E • ADS NX5-4020E • ADS NX5-6025E • ADS NX3-HD1000 • ADS NX5-HD5000 • ADS NX5-HD6000 • ADS NX3-HD2500 • ADS NX5-HD4500 • ADS NX5-HD6500 • ADS NX5-HD8500 • ADS NX5-8000 • ADS NX5-10000 • ADS NX5-12000 • ADS NX5-20000 • ADS NX1-VN01
Software Version	V4.5R90F06 Build: 49460
Upgrade File	<ul style="list-style-type: none"> • update_ADS_x86_V4.5R90F06_20241227.zip MD5:2247ca56cfac0c3ebaeca8f68e506f90 SHA256:1ff6b213e329dc74e32bd77e54aa01248d3220a75a536e1a8de179a8d7437df9 • update_ADS_arm_V4.5R90F06_20241227.zip MD5:94994f4e2a30ef638e41eed64536184c SHA256:0c6b1d6ee9d126d306a1a86dc8254b0533155256599679bc05ccacf9bdeac4e8 • update_ADS_hygon_V4.5R90F06_20241227.zip MD5:535511b8a78969d36bcb24fc38fb916 SHA256:f65ce4649391f7f3fee83f855a2e089e2c03d3dc3c6d892427489f32a84b374f
Release Date	2025-1-2
How to Obtain	Obtain the upgrade file from the upgrade system or contact NSFOCUS technical support.

2. Version Mapping

Source Software Version	V4.5R90F06
Product Model	X86 platform: 800E, 2020E, 4020E, 6025E, HD1000, HD5000, HD6000, HD2500, HD4500, HD6500, HD8500, 8000, 10000, 12000, and 20000
Management Platform	<ul style="list-style-type: none"> • ADS M: V4.5R90F06 • ADBOS: V4.5R90F06 • ISOP: V3.0R01F08SP01 • NPAI: 3.2.0
Software Client	None
Browser	<ul style="list-style-type: none"> • Firefox • Edge • Chrome
Documentation	<ul style="list-style-type: none"> • NSFOCUS ADS V4.5R90F06 User Guide • NSFOCUS ADS V4.5R90F06 Deployment 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
ADS-52605	Normal	Defect	Manual traffic diversion	Query of manual diversion routes (Extend selected during configuration) on the router finds that the network ID and broadcast address are missing.
ADS-54768	Normal	Defect	SNMP trap	HA logs are sent via SNMP traps at the specified interval even if no change is made to HA.
ADS-54847	Normal	Defect	Interface	The 1000M optical interfaces of the 4 x optical + 4 x electrical interface board are incorrectly represented with the letter G, which indicates an electrical interface.
ADS-55245	Normal	Defect	SNMP trap	Power status values in SNMP traps are incorrect.
ADS-55439	Normal	Defect	Blocklist	Adding, querying, or deleting IP addresses starting with 0 (0.X.X.X) returns an error message indicating incorrect format.

Bug ID	Severity	Type	Function/Component	Description
ADS-56474	Normal	Defect	Protection group	A protection group created before the engine starts cannot be deleted.
ADS-56503	Normal	Defect	Group-specific ACL	Creating ACL rules failed, with an error indicating the IP address is in use by another group, when actually only the default group exists.
ADS-57401	Normal	Defect	Cluster synchronization	The injection routes repeatedly synchronize.
ADS-57661	Normal	Defect	Protection group	When the total number of IP addresses in protection groups is large, adding/deleting IP addresses to/from a group takes a longer time than expected.

4. Opened Ports

Peer Device	Connection	Protocol	Service	Port	Opened by Default	Configurable
Browser or client	Requesting client – Apache	TCP	Apache	443	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Client	Requesting client – SSH	TCP	CLI	22	<input type="checkbox"/>	<input type="checkbox"/>
Client	Requesting client – SSH	TCP	Remote assistance	Random	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Client	Requesting client – SNMP agent	TCP/UDP	SNMP agent	161	<input type="checkbox"/>	<input type="checkbox"/>
Diversion-purpose collaborating device	NTA – ADS	TCP	Diversion scheduling	8342	<input type="checkbox"/>	<input type="checkbox"/>

5. Function Changes

5.1 New Functions

New Function	Description
CLI	The SSD firmware version can be displayed via the CLI.
BGP routing parameters	A BGP neighbor can be configured to work in active (Passive Mode set to No) or passive (Passive Mode set to Yes) mode.
SNMP configuration	Allowed access IP addresses can be configured for SNMP agents.
SSL/TLS keyword checking	The Server Name Indication (SNI) field is added in SSL/TLS

New Function	Description
	keyword checking rules.
Group-specific DNS protection policy	For a DNS protection policy, two CNAME protection algorithms (5-DNS_CNAME and 6-DNS_NS&CNAME) are added, and the original 3-DNS_CNAME is renamed to 3-DNS_NS.
Group-specific HTTPS protection policy	HTTPS fingerprint protection is added.
Protection group configuration	The policy configured for a protection group can be saved as a group policy template.
IP addresses in protection groups	When an IP address included in a new group is in use by another group, it can be automatically added to the exception IP list of the latter group.
Carpet bombing protection	Carpet bombing protection is moved from Anti-DDoS > Protection Groups and Access Control to become an independent element under Anti-DDoS , allowing users to configure different rules as required.
DNS subdomain allowlist	Both the global and group-specific DNS subdomain allowlists support auto-learning based on settings.
Syslog configuration	Custom information can be added to syslog messages.
Web API	The built-in bypass function can be controlled via web APIs of ADS in in-path mode.
Automatic packet capture	The PCAP files obtained from an attack-triggered packet capture task can be directly uploaded to ADS M.
System resources	The disk status is indicated in the System Resources area of the Real-Time Monitoring page and disk exception alerts can be sent.

5.2 Deleted Functions

Function	V4.5R90F05	V4.5R90F06	Impact	Reason for Deletion
Carpet bombing protection	Carpet bombing protection	Deleted	If the function worked for groups and was only enabled for some groups in the earlier version, the default carpet bombing protection rule is disabled after the upgrade to the new version and needs to be manually enabled.	The function in the earlier version is implemented with policies. The new version changes it to an independent module, allowing users to configure different rules as required. This makes the protection more precise and extensive.

5.3 Modified Functions

Function	V4.5R90F05	V4.5R90F06	Impact
Group-specific DNS protection	DNS_CNAME algorithm	DNS-NS algorithm	None

Function	V4.5R90F05	V4.5R90F06	Impact
policy			

6. Detailed Description of Function Changes

6.1 Active and Passive Mode Options Added for BGP

Configuration

Function Description

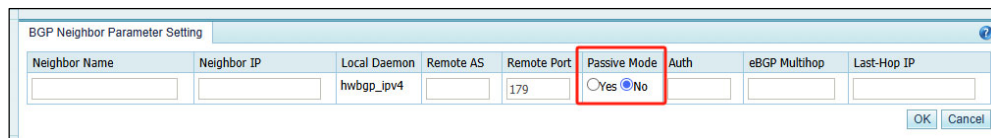
A BGP neighbor can be configured to work in passive mode so that ADS will not actively initiate a connection to the peer device.

This configuration is useful in the following scenarios:

- When ADS connects to a router as a BGP neighbor, if active BGP is enabled at both ends, BGP negotiation may fail. Changing the BGP mode to passive at either end can avoid this problem. (The H3C CR16K router is known to have this problem.)
- When it is necessary to disconnect the BGP connection without deleting the BGP neighbor configuration on ADS, the BGP mode can be set to passive at both ends.

Configuration

Choose **Diversion & Injection > Diversion Routes > BGP Routes** and set **Passive Mode** to **Yes** or **No** when adding or editing a BGP neighbor.



The screenshot shows a window titled "BGP Neighbor Parameter Setting". It contains several input fields: "Neighbor Name", "Neighbor IP", "Local Daemon" (pre-filled with "hwbgp_ipv4"), "Remote AS", "Remote Port" (pre-filled with "179"), "Passive Mode" (with radio buttons for "Yes" and "No", where "Yes" is selected), "Auth", "eBGP Multihop", and "Last-Hop IP". "OK" and "Cancel" buttons are at the bottom right.

Post-upgrade Notes

After the upgrade, the passive mode of all BGP neighbors is **No** by default.

6.2 Allowed Access IP Configurable for SNMP Agent

Function Description

Allowed access IP addresses can be configured for the SNMP agent to allow only listed IP addresses to access the SNMP agent. If no IP address is specified, all IP addresses can access the SNMP agent.

Configuration

Choose **System > Log Services > SNMP > SNMP Agent**, click **Edit**, and set allowed access IP addresses.

The screenshot shows the 'Modify SNMP Agent Settings' dialog box. It has a table with two columns: 'Item' and 'Value'. The 'Run SNMP Agent at Startup' is set to 'Yes', 'SNMP Version' is set to '2c', and 'Community' is set to 'collapsar'. Below the table, there is a text area labeled 'Allowed Access IP' which is highlighted with a red rectangle. At the bottom right, there are 'OK' and 'Cancel' buttons.

Item	Value
Run SNMP Agent at Startup	<input checked="" type="radio"/> Yes <input type="radio"/> No
SNMP Version	<input checked="" type="radio"/> 2c <input type="radio"/> 3
Community	collapsar

Allowed Access IP

OK Cancel

Post-upgrade Notes

After the upgrade, the allowed access IP list is empty, indicating that all IP addresses can access the SNMP agent.

6.3 Server Name Indication Field Added to SSL/TLS Keyword

Checking Rules

Function Description

In an SSL/TLS keyword checking rule, if a custom template is selected, a new field, **Server Name Indication** (SNI), appears. After the field is configured, ADS will check the SNI field in client hello packets.

Note the following when configuring this field:

- Fuzzy matching is used for this field. In other words, when the configured value hits one substring of the SNI field in a packet, the SNI field is considered a match.
- The field setting can be reversed so that ADS will take all packets that do not contain this value in the SNI extension as the matching ones.
- This field cannot be configured when **HandShakeType** is set to **Server hello**.

Configuration

Choose **Policy > Access Control > SSL/TLS Keyword Checking**, click **Add**, select a custom keyword template, and set **Server Name Indication**.

SSL/TLS Keyword Checking

Prefix Length/Netmask

Src/Dst Port

443

(For the handshake type of client hello or the JA3 template, the destination port is matched. For the handshake type of server hello or the JA3S template, the source port is matched.)

Keyword Template

☐ JA3

☐ JA3S

☒ Custom

Help

Keyword

HandshakeType

Client hello

Invert

☐ SSLVersion

☐ Random

☐ Session ID

☐ Cipher Suites

☐ Cipher Suites Numbers

min

(0-256)

max

(0-256)

☐ Yes

☒ No

☐ Extensions Numbers

min

(0-256)

max

(0-256)

☐ Yes

☒ No

☐ Custom Extension 1

☐ Custom Extension 2

☐ Custom Extension 3

☐ Server Name Indication

Type a character string, such as 123.com.)

☐ Yes

☒ No

Post-upgrade Notes

None. This keyword is not checked by default in existing rules.

6.4 Algorithms Added for the Group-specific DNS Protection Policy

Function Description

The existing DNS protection algorithms are optimized and new ones are added, involving the following changes:

- The original 3-DNS_CNAME algorithm is renamed to 3-DNS-NS, which is more accurate.
- The processing procedure of the 3-DNS-NS algorithm is optimized to enhance its compatibility, especially in scenarios where the customer has multiple authoritative servers for load sharing.
- The 5-DNS_CNAME algorithm is added to provide additional support for scenarios where 3-DNS-NS may be unable to work due to compatibility issues.
- The 6-DNS-NS&CNAME algorithm can intelligently select between the above two algorithms, thus providing stronger compatibility.
- Indicative information is added on the UI to indicate the server types each algorithm is applicable to.

Configuration

Choose **Policy > Anti-DDoS > Protection Groups** and edit the DNS protection policy of a group by selecting an appropriate algorithm.

DNS Protection Policy [except@cluster]

Protection Type	Enable	Parameter Configuration
DNS Query	<input checked="" type="radio"/> Yes <input type="radio"/> No	Protection Algorithm ⓘ Reverse Detection Rate Protection Algorithm Action
DNS Response	<input type="radio"/> Yes <input checked="" type="radio"/> No	

TCP Control Parameters [except@cluster]

Targeting

☒ Destination IP/Port ☐ Dst IP

DNS Control

☒ DNS Time-Sensitive Check ☐ Yes ☒ No

2-TCP_BIT

1-Default
2-TCP_BIT
3-DNS_NS
4-DNS retransmission
5-DNS_CNAME
6-DNS_NS&CNAME

Algorithm 2-TCP_BIT is applicable to DNS cache servers.
(pps)

Post-upgrade Notes

After the upgrade, the algorithm of groups originally set to **3-DNS_CNAME** changes to **3-DNS-NS**, with the actual processing procedure remaining unchanged.

6.5 Fingerprint Protection Added in the Group-specific HTTPS Protection Policy

Function Description

To initiate an HTTPS connection request, a client needs to send a client hello packet in the handshake phase. This packet contains fixed data, from which fingerprints can be extracted to identify a specific type of traffic. When the fingerprint carried by the client hello packets sent to a destination IP address meets both the number and proportion of visits configured within a statistical period, ADS will take action on these packets as configured to protect against HTTPS attacks. This function has the following advantages:

- In scenarios where there are no obvious anomalies at the network layer and HTTPS packets cannot be decrypted, fingerprint protection provides a new means of protection.
- In scenarios where source IP addresses are sparsely scattered, fingerprint protection can effectively improve the efficiency of HTTPS protection.
- Can identify anomalous traffic during the connection setup phase to avoid difficulties in protecting against attack traffic that cannot be decrypted after the connection is established.

Configuration

Choose **Policy > Anti-DDoS > Protection Groups** and edit the HTTPS protection policy by configuring fingerprint protection parameters.

HTTPS Protection Policy [except@cluster]												
HTTPS Protection		Configuration										
		Protection Port <input type="text" value="443"/>	Protection Threshold <input type="text" value="1000"/> (pps)									
Enable <input type="radio"/> Yes <input checked="" type="radio"/> No		Policy Connection Protection – Renegotiation Protection										
		Parameter Configuration Per Source IP Renegotiation Rate Limit <input type="text" value="16000"/> (0-16000) (pps) Add Abnormal Source IP to Blocklist <input type="radio"/> Yes <input checked="" type="radio"/> No										
<input checked="" type="radio"/> Yes <input type="radio"/> No		<table border="1"> <tr> <td> Connection Protection – Fingerprint Protection </td> <td> Statistical Period <input type="text" value="4"/> (s) (1-3600) Number of Visits <input type="text" value="400"/> (1-1000000) Proportion of Visits <input type="text" value="1"/> (%) (1-100) Action <input type="text" value="Limit rate"/> <input type="text" value="0"/> (pps) (0-6000000) Execution Time <input type="text" value="10"/> (min) (1-3600) </td> </tr> </table>		Connection Protection – Fingerprint Protection	Statistical Period <input type="text" value="4"/> (s) (1-3600) Number of Visits <input type="text" value="400"/> (1-1000000) Proportion of Visits <input type="text" value="1"/> (%) (1-100) Action <input type="text" value="Limit rate"/> <input type="text" value="0"/> (pps) (0-6000000) Execution Time <input type="text" value="10"/> (min) (1-3600)							
Connection Protection – Fingerprint Protection	Statistical Period <input type="text" value="4"/> (s) (1-3600) Number of Visits <input type="text" value="400"/> (1-1000000) Proportion of Visits <input type="text" value="1"/> (%) (1-100) Action <input type="text" value="Limit rate"/> <input type="text" value="0"/> (pps) (0-6000000) Execution Time <input type="text" value="10"/> (min) (1-3600)											
<input type="radio"/> Yes <input checked="" type="radio"/> No		<table border="1"> <thead> <tr> <th>Enable</th> <th>Protection Type</th> <th>Parameter Configuration</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>Access Rate-based Protection</td> <td> Number of Visits <input type="text" value="100"/> (1-10000) Statistical Period <input type="text" value="4"/> (s) (1-3600) Consecutive Abnormal Cycles <input type="text" value="3"/> (1-10) </td> </tr> <tr> <td><input type="checkbox"/></td> <td>Resource-specific Access Protection</td> <td> Proportion of Visits <input type="text" value="90"/> (%) (1-100) Number of Visits <input type="text" value="10"/> (1-10000) Statistical Period <input type="text" value="10"/> (s) (1-3600) Consecutive Abnormal <input type="text" value="1"/> (1-10) </td> </tr> </tbody> </table>		Enable	Protection Type	Parameter Configuration	<input type="checkbox"/>	Access Rate-based Protection	Number of Visits <input type="text" value="100"/> (1-10000) Statistical Period <input type="text" value="4"/> (s) (1-3600) Consecutive Abnormal Cycles <input type="text" value="3"/> (1-10)	<input type="checkbox"/>	Resource-specific Access Protection	Proportion of Visits <input type="text" value="90"/> (%) (1-100) Number of Visits <input type="text" value="10"/> (1-10000) Statistical Period <input type="text" value="10"/> (s) (1-3600) Consecutive Abnormal <input type="text" value="1"/> (1-10)
Enable	Protection Type	Parameter Configuration										
<input type="checkbox"/>	Access Rate-based Protection	Number of Visits <input type="text" value="100"/> (1-10000) Statistical Period <input type="text" value="4"/> (s) (1-3600) Consecutive Abnormal Cycles <input type="text" value="3"/> (1-10)										
<input type="checkbox"/>	Resource-specific Access Protection	Proportion of Visits <input type="text" value="90"/> (%) (1-100) Number of Visits <input type="text" value="10"/> (1-10000) Statistical Period <input type="text" value="10"/> (s) (1-3600) Consecutive Abnormal <input type="text" value="1"/> (1-10)										

Post-upgrade Notes

This function is disabled by default.

6.6 Carpet Bombing Protection

Function Description

Some low-and-slow DDoS attack methods do not focus attack traffic on one or several protected IP addresses, but instead target the entire network segment in a carpet bombing manner. In this type of attack, traffic to a single IP address may be too small to trigger the device to enter into the protection state, resulting in negative positives. Carpet bombing protection resolves this problem thanks to the following advantages:

- Suitable for scenarios where traffic to a single IP address is too small to trigger protection.
- The network segment protection threshold can be set based on its traffic volume.
- Different rules can be set for different network segments to achieve the effect of network segmentation.
- In scenarios where quite a few network segments are involved, IP addresses can be automatically aggregated according to the configured netmask/prefix length.
- Behavior-based protection limits the range of destination IP addresses, resulting in more accurate detection.

Note the following when using this function:

- The **Enable** switch controls all functions in a rule. If **No** is selected, all functions in the rule are turned off.
- Only network segments are allowed for the IP range of a rule.
- Threshold 1 of DDoS policy-based carpet bombing protection determines whether related protection is triggered. A specific type of flood is protected against with the corresponding policy of the group covering the destination IP address.
- **Destination IPs** in behavior-based carpet bombing protection is a subset of the IP range configured for the rule.

- The **Add to the blacklist** action of the behavior-based policy actually adds source IP addresses to the blacklist of the group covering the related destination IP address.

Configuration

Choose **Policy > Anti-DDoS > Carpet Bombing Protection**, click **Add**, and configure parameters.

Item	Value
Name	
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
IP Range	
IP Aggregation	IPv4 Netmask: 24 IPv6 Prefix Length: 120
DDoS Policy-based Carpet Bombing Protection	
Anti-DDoS	Threshold 1
SYN Flood	2000 (pps) Yes
ACK Flood	8000 (pps) Yes
UDP Flood	8000 (pps) Yes
ICMP Flood	4000 (pps) Yes
HTTP Get Flood	1000 (pps) No
HTTP Post Flood	1000 (pps) No
HTTPS Flood	1000 (pps) No
Traffic Control by Dst Segment	10000 (kpps) No
Behavior-based Carpet Bombing Protection	

Post-upgrade Notes

- After the upgrade, a default rule named **default** is listed, whose status is described as follows:
 - If carpet bombing protection is disabled before the upgrade, the default rule is disabled after the upgrade.
 - If carpet bombing protection is enabled and globally effective before the upgrade, the default rule is enabled after the upgrade.
 - If carpet bombing protection is enabled and effective for groups before the upgrade, the status of the default rule after the upgrade depends on whether this protection is enabled for all groups. If yes, the default rule is enabled. If not, the default rule is disabled.
- If the default rule is enabled after the upgrade, it is advisable to adapt the default thresholds for triggering carpet bombing protection to the actual business needs. Alternatively, users can create a new rule for a specific network segment.

6.7 Auto-learning Supported for the DNS Subdomain Allowlist

Function Description

The DNS subdomain auto-learning feature is designed to address random subdomain attacks. With this feature, ADS can automatically learn "good" subdomain requests and dynamically

generate the allowlist. Based on this allowlist, ADS can effectively filter out suspicious requests, protecting websites from potential attacks. This function has the following advantages:

It can effectively deal with the impossibility of creating an exhaustive subdomain allowlist by dynamically generating an automatic subdomain allowlist.

Configuration

- Global DNS subdomain allowlist:

Choose **Policy > Access Control > DNS Subdomain Allowlist**, enable the auto-learning function, and configure related parameters.

Item	Value
Enable	Yes

Primary Configuration Items

Item	Value
Action for Unmatched DNS Requests	Default

Subdomain Allowlist Auto-Learning

Item	Value
Enable	Yes
Auto-learning Type	DNS query
Min Source IPs	2 (2-256)
Statistical Period	30 (s)(1-3600)
Max Domain Levels	0 (0-16, 0 indicates no limit)
Uppercase Restriction	Yes
Auto Allowlist Duration	120 (min)(0-8000000, 0 indicates no limit)

OK Cancel

- Group-specific DNS subdomain allowlist:

Choose **Policy > Anti-DDoS > Protection Groups**, click **DNS Subdomain Allowlist**, enable the allowlist function and auto-learning function successively, and configure related parameters.

Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Operation
default_protection_group	Protect		Allowlist	Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started	all_users	
except@cluster	Protect		Allowlist	Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started	except	
dns@cluster	Protect		Allowlist	Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started	dns	
learnDns@cluster	Protect		Allowlist	Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started	dnlearn	
heyand@cluster	Protect		Allowlist	Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		Not started	subdomain	

Delete Create Group

DNS Subdomain Allowlist ?

DNS Subdomain Allowlist [default_protection_group]

Item	Value
Enable	Yes ▾

Primary Configuration Items

Item	Value
Primary Domain ?	<input type="text"/> (Leaving this field empty indicates that all DNS requests are deemed to be a match.) ?
Action for Unmatched DNS Requests ?	Default ▾

Subdomain Allowlist Auto-Learning

Item	Value
Enable	Yes ▾
Auto-learning Type ?	DNS query ▾
Min Source IPs	<input type="text"/> 3 (2-256)
Statistical Period	<input type="text"/> 30 (5-3600)
Constraints	Max Domain Levels <input type="text"/> 0 (0-16. 0 indicates no limit.)
	Uppercase Restriction Yes ▾
Auto Allowlist Duration	<input type="text"/> 120 (min)(0-8000000. 0 indicates no limit.)

OK Cancel

Post-upgrade Notes

- The function is disabled by default.
- **DNS query** is applicable to the diversion and in-path modes. ADS in diversion mode automatically learns subdomain names from DNS query packets on all interfaces. ADS in in-path mode automatically learns subdomain names only from DNS query packets on the IN interface.
- **DNS response** is applicable to the out-of-path mode. ADS in this mode automatically learns subdomain names from DNS response packets received on the OUT interface. **DNS response** is preferred when ADS is in in-path mode. When **DNS response** is selected, **Action for Unmatched DNS Requests** cannot be set to **Drop**.

6.8 Custom Information Supported for Syslog Messages

Function Description

A new field, **Custom Information**, is added in syslog configuration. If this field is configured, syslog messages will contain this custom information. If this field is left empty, no custom information will be contained in syslog messages.

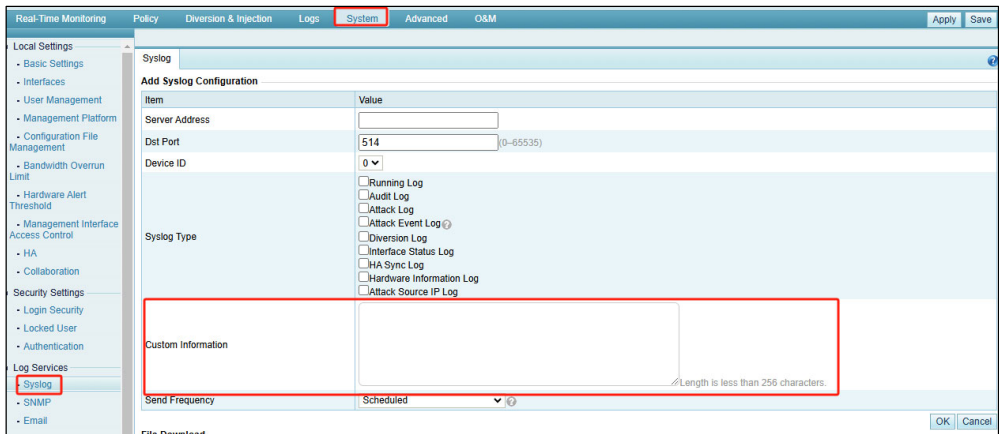
For example, if **TEST** is configured as custom information, the syslog message sent will contain this information, as shown in the following figure.

View... Grid... Reverse Sort Refresh Auto-refresh: 1 s Next Page Loaded 95 messages from period: 2024/11/01 00:00:00 - 2024/11/01 17:31:58

Received	Originator	Severity	Facility	Message
2024/11/01 17:30:56...	10.66.242.124	Informational	local0	TEST] Portinfo(Port, State, rx Kpps, tx Kpps, rx Mbps, tx Mbps) : 0 V4/1 up 0 0 0 0
2024/11/01 17:30:56...	10.66.242.124	Informational	local0	TEST] Hardware CPU: 50 C Board: 50 C Fan: 0 Disk: 0 SN: E16F-C52F-B2C2-A9BC M
2024/11/01 17:31:27...	10.66.242.124	Informational	local0	TEST] Collapsar load: 5% Mem: 84% Disk: 16%. SN: E16F-C52F-B2C2-A9BC Macid:
2024/11/01 17:31:27...	10.66.242.124	Informational	local0	TEST] Portinfo(Port, State, rx Kpps, tx Kpps, rx Mbps, tx Mbps) : 0 V4/1 up 0 0 0 0
2024/11/01 17:31:27...	10.66.242.124	Informational	local0	TEST] Hardware CPU: 50 C Board: 50 C Fan: 0 Disk: 0 SN: E16F-C52F-B2C2-A9BC M
2024/11/01 17:31:58...	10.66.242.124	Informational	local0	TEST] Collapsar load: 5% Mem: 84% Disk: 16%. SN: E16F-C52F-B2C2-A9BC Macid:
2024/11/01 17:31:58...	10.66.242.124	Informational	local0	TEST] Portinfo(Port, State, rx Kpps, tx Kpps, rx Mbps, tx Mbps) : 0 V4/1 up 0 0 0 0

Configuration

Choose **System > Log Services > Syslog**, click **Add**, and configure parameters.



The screenshot shows the 'Add Syslog Configuration' dialog in the NSFOCUS ADS interface. The 'System' tab is selected. The 'Log Services' section is expanded, and 'Syslog' is highlighted. The 'Add Syslog Configuration' dialog is open, showing the following fields:

- Server Address: [Empty]
- Port: 514 (Range: 0-65535)
- Device ID: 0
- Syslog Type: ☐ Running Log, ☐ Audit Log, ☐ Attack Log, ☐ Attack Event Log, ☐ Diversion Log, ☐ Interface Status Log, ☐ HA Sync Log, ☐ Hardware Information Log, ☐ Attack Source IP Log
- Custom Information: [Empty text area, highlighted with a red box. Note: Length is less than 256 characters.]
- Send Frequency: Scheduled

Buttons: OK, Cancel

Post-upgrade Notes

None.

6.9 Auto PCAP Files Allowed to Be Uploaded to ADS M

Function Description

The new version optimizes attack-triggered auto-capture by providing the function of automatically uploading PCAP files to ADS M, thus improving the availability and relevance of packet capture data. It has the following advantages:

Improves the centralized management and utilization efficiency of data and enables traceback analysis and closed-loop management of events.

Configuration

Choose **Advanced > Packet Capture > Auto Capture**, click **Edit**, and select **ADSM** for **Upload Method**.

Modify Attack-triggered Packet Capture

Status

Item	Value
Enable	<input type="radio"/> Yes <input checked="" type="radio"/> No

Trigger Condition

Item	Value
Trigger Rate	100 pps (1-4294967295)

Parameter Settings

Item	Value
Max Time	20 (1-300)
Max Packets	3000 (1-30000)
Packet Sampling Rate	1 (1-65535) (*Example: 1000, indicating that one in 1000 packets is captured. The value 1 indicates that no sampling is conducted.)
Upload Method	ADSM
ADSM	<div><input type="checkbox"/> 10.66.253.55:443 <input type="checkbox"/> 10.66.253.85:443 <input type="checkbox"/> 10.66.253.177:443 <input type="checkbox"/> 10.44.0.240:443</div>

OK Cancel

Post-upgrade Notes

Users can select 0–2 IP addresses of ADS M. If no IP address is selected, the system will automatically select the first available ADS M from the management platforms configured.

6.10 Generation of Policy Templates from Group Policies

Function Description

In practice, policies configured for a certain group may deliver a good protection effect. Therefore, users want to use the same policies for other assets providing similar services. However, it is quite troublesome to create a group and configure parameters one by one. In the new version, a button is added in the **Operation** column of the protection group list. By clicking this button, users can directly generate a policy template, which can be selected for use during group creation.

Configuration

Choose **Policy > Anti-DDoS > Protection Groups**, click  in the **Operation** column, and set the template name and description.

Real-Time Monitoring Policy Diversion & Injection Logs System Advanced O&M

Anti-DDoS

Protection Groups

Group Policy Template

Carpet Bombing Protection

Advanced Global Parameters


Response Page

Protection Group

Group Name or IP

Running Mode All Filter

First Previous Next Last 1/1 Go to

Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Operation
default_protection_group	Protect			Allowlist Access Control Rules Blocklist GeoIP Rules TI DNS Subdomain Allowlist		-	all_users	

Post-upgrade Notes

None.

6.11 Conflicting IP Address/Segment Added to the Exception IP List of the Involved Group

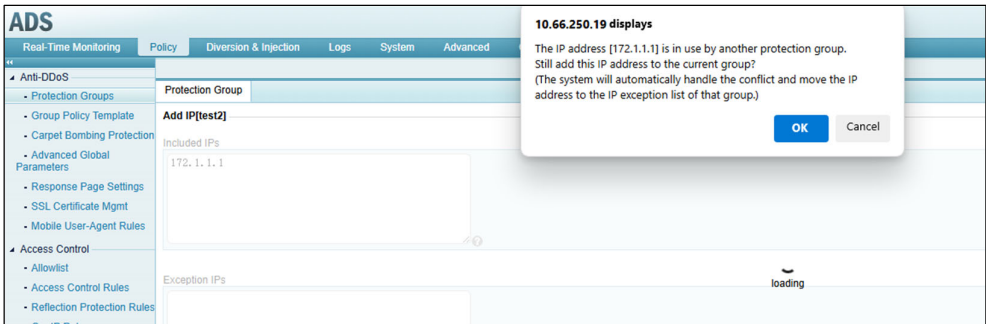
Function Description

When a user adds IP addresses/segments during group creation or editing, if an IP address/segment is already included in another group, this conflicting IP address/segment can still be added. The processing logic is as follows:

The system handles the conflict by adding the conflicting IP address/segment to the exception IP list of the involved group.

Configuration

Choose **Policy > Anti-DDoS > Protection Groups** and edit the IP list of a group, or create a group and add IP addresses/segments.



Post-upgrade Notes

The system can handle only one conflict at a time. When there is more than one conflicting IP address/segment, the IP address configuration will fail, with no message displayed to prompt automatic conflict handling.

6.12 Disk Status Shown in the System Resources Area of the Real-Time Monitoring Page

Function Description

When the number of disk write or erasion operations exceeds the limit, the disk may become unavailable, affecting the normal operation of the device. In the new version, the disk status is shown in the **System Resources** area of the **Real-Time Monitoring** page. When there are bad blocks or the write/erasion limit is about to be exceeded, users will be alerted. This function has the following advantages:

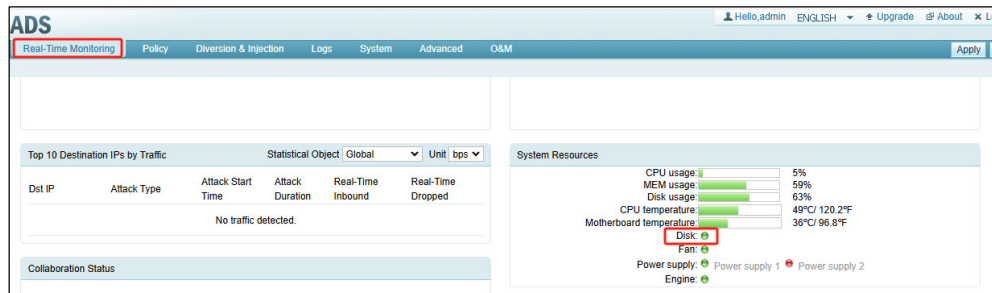
- Lets users know the disk status in real time.

- Alerts users to exceptions.

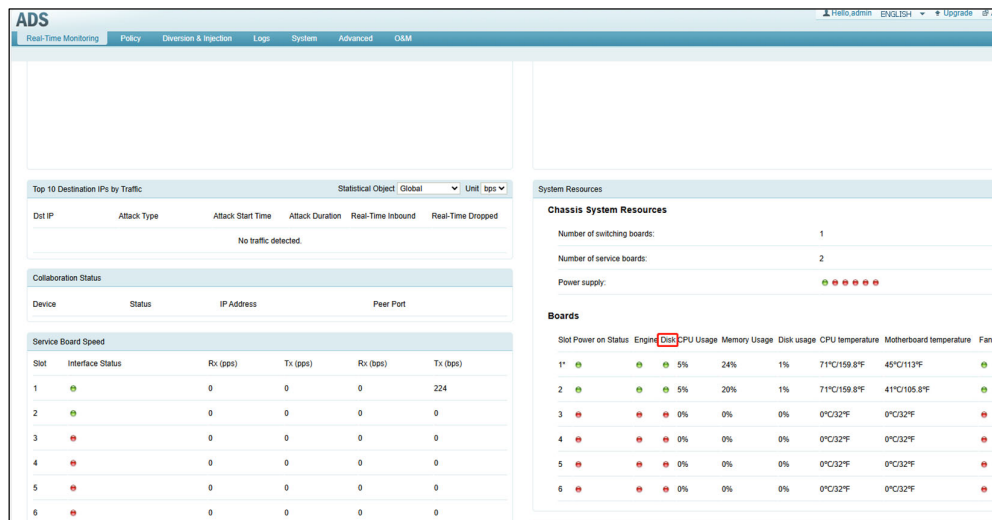
Configuration

This function involves **Real-time Monitoring** and **System** modules.

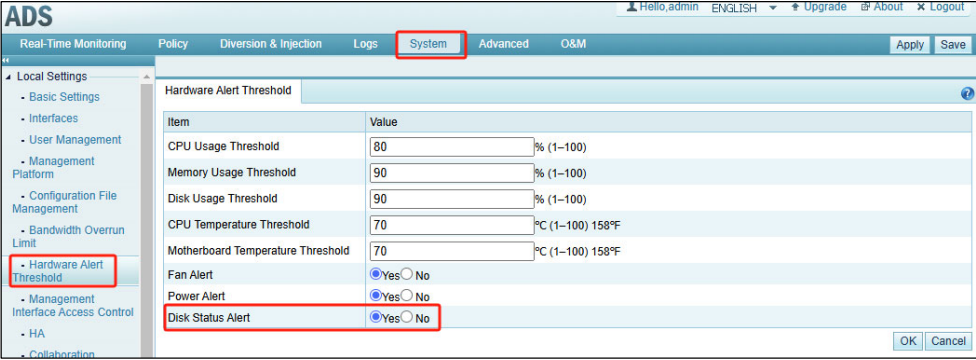
On the **Real-Time Monitoring** page of a box-type device, the disk status is displayed in the **System Resources** area.



For a chassis-type device, the disk status of each board is displayed in the **Boards** area.



Under **System > Local Settings > Hardware Alert Threshold**, set **Disk Status Alert** to **Yes**.



Post-upgrade Notes

None.

7. Version Application

7.1 Upgrade

7.1.1 Version Upgrade

Applicable Device Models

ADS NX3-800E, ADS NX3-2020E, ADS NX5-4020E, ADS NX5-6025E, ADS NX3-HD10000, ADS NX5-HD5000, ADS NX5-HD6000, ADS NX3-HD2500, ADS NX5-HD4500, ADS NX5-HD6500, ADS NX5-HD8500, ADS NX5-8000, ADS NX5-10000, ADS NX5-12000, ADS NX5-20000, and ADS NX1-VN01

Constraints

Upgrades must be based on V4.5R90F05 or later. If the current version is lower than V4.5R90F05, first upgrade it to V4.5R90F05 or later along the required upgrade route; otherwise, the upgrade would fail.

Impact

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

Procedure

- Step 1** Choose **System > Local Settings > Configuration File Management**. In the **Configuration File** area, click **Export** to save the configuration file to a local disk drive.

- Step 2** On ADS V4.5R90F05 or later, choose **System > Others > System Upgrade**, upload update_ADS_x86_V4.5R90F06_20241227.zip (MD5: 2247ca56cfac0c3ebaeca8f68e506f90), and perform the upgrade.
- Step 3** After the system prompts upgrade success, restart the device.
- Step 4** After the device is restarted, verify the upgrade result. For details, see [Upgrade Success Verification](#).
- End

Note: If the upgrade failed, contact NSFOCUS technical support.

Upgrade Success Verification

Log in to the web-based manager and choose **System > Others > System Upgrade**. In the **Upgrade History** list, verify that the target version is V4.5R90F06. Then go to **System > Others > System Info**, verify that the software version is V4.5R90F06.

What to Do in the Case of Upgrade Failure

If the upgrade failed, try using **Rollback system** in the console user interface or logging in to the CLI to perform a rollback operation.

7.1.2 Version Rollback

Applicable Device Models

ADS NX3-800E, ADS NX3-2020E, ADS NX5-4020E, ADS NX5-6025E, ADS NX3-HD10000, ADS NX5-HD5000, ADS NX5-HD6000, ADS NX3-HD2500, ADS NX5-HD4500, ADS NX5-HD6500, ADS NX5-HD8500, ADS NX5-8000, ADS NX5-10000, ADS NX5-12000, ADS NX5-20000, and ADS NX1-VN01

Procedure

To roll back the device from version V4.5R90F06 to the previous version, follow these steps:

Log in to the console user interface and select **Rollback system**, or log in to the CLI and run the **update rollback** command.

Rollback Success Verification

Log in to the web-based manager and choose **System > Others > System Upgrade**. In the **Upgrade History** list, verify that the target version is V4.5R90F05. Then go to **System > Others > System Info**, verify that the software version is V4.5R90F05.

Impact

The network connection will be interrupted in the rollback process.

What to Do in the Case of Rollback Failure

If the rollback failed, contact NSFOCUS technical support.

7.2 Constraints

None.