ACOS 6.0.9
New Features and Enhancements

July, 2026

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at: a10-virtual-patent-marking.

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: a10-trademarks

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc.. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting www.a10networks.com.

Table of Contents

Enhancements in ACOS 6.0.9

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.9 release:

For new features and enhancements prior to ACOS 6.x release, see the recent prior ACOS New Features and Enhancements.

The following topic is covered:

Network Configuration

ACOS 6.0.9 introduces the following new feature and enhancement for the Network Configuration:

NOTE: For configuration, refer *Network Configuration Guide* and for specific CLI commands, refer *Command Line Reference Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topic is covered:

Updates to A10 Reserved Subnet

In ACOS, the A10 reserved subnet 169.254.0-127.x/17 is available for use with the following considerations:

For multi-PU Platforms:

- No changes.

For Non-multi-PU Platforms:

- The reserved IP can only be used if IP Unnumbered or BGP Unnumbered is not configured.
- If any reserved IP is configured, IP Unnumbered or BGP Unnumbered is disabled.

Limitation

If static routes are configured with a reserved subnet, BGP Unnumbered can still be configured, however, the interface will not be operational.

See Also:

- Network Configuration Guide

VLAN-ID Based MAC Address

ACOS allows to assign a unique virtual MAC addresses for each VLAN. When this feature is enabled and a unique MAC tag is set for a VLAN, a unique virtual MAC address is derived for the associated VE interface. The VLAN-based virtual MAC address is used for traffic forwarding and Gratuitous ARP (GARP) by the floating IP, virtual IP (VIP), and NAT addresses associated with the tagged VLAN.

This feature allows each VLAN to advertise a unique MAC address, which helps to interoperate with network environments that require unique MAC addresses per VLAN.

CLI Configuration

- To enable vlan based mac address, use the following command:

```
ACOS(config)# vlan-global enable-vlan-based-mac
```

- To associate the tag with VLAN ID, use the following commands:

```
ACOS(config)# vlan 612
ACOS(config-vlan:612)# mac-tag 10
```

Show Command

To display the MAC address and associated tags, use the following command:

```
show vlan mac-address
```

Limitations

- Only 31 L3V and Shared partition IDs are supported.
- This feature cannot be enabled if an L3V with a partition ID greater than 31 exists.
- After the feature is enabled, partition IDs greater than 31 cannot be created.
- If the feature is enabled or disabled, you must save the configuration and reload the device. This ensures that the correct MAC addresses are advertised.
- The tag can be modified only before the VE interface is created. To update an existing tag, first remove the VE interface.
- The MAC tags 1-31 are allocated system-wide and not per partition.

See Also:

- Network Configuration Guide
- Command Line Interface Reference

System and Security

ACOS 6.0.9 introduces the following new features and enhancements for system and security:

NOTE: For more information and details, refer *System Configuration and Administration Guide*.

The following topics are covered:

Enhancements to SSH Control-Plane Security

ACOS supports enhancing the control-plane security to prevent credential theft, lateral movement, unauthorized communication, data exfiltration, reducing attack surface,

X11-related vulnerabilities, reducing automated attacks, and avoiding brute-force attempts.

The following SSH functionalities are disabled using the CLI options to enhance security:

- SSH Agent Forwarding
- SSH TCP Port Forwarding
- SSH X11 Forwarding
- Changing Default SSH TCP Port

NOTE: These settings apply globally across the ACOS system.

CLI Configuration

- To disable SSH Agent Forwarding, use the following command:

```
ACOS(config)# sshd-config disable-agent-forwarding
```

- To disable SSH TCP Forwarding, use the following command:

```
ACOS(config)# sshd-config disable-tcp-forwarding
```

- To disable SSH X11 Forwarding, use the following command:

```
ACOS(config)# sshd-config disable-x11-forwarding
```

- To change the SSH port number, use the following command:

```
ACOS(config)# sshd-config tcp-port <22, 1025-64999>
```

See Also:

- System Configuration and Administration Guide
- Command Line Interface Reference

Security Updates

The following security vulnerabilities are addressed in this release:

- DDoS Vulnerability
  - CVE-2025-58188: A denial-of-service vulnerability in the Go crypto/x509 package. When validating a certificate chain containing DSA public keys, the library performs an invalid interface type assertion that assumes the key implements the Equal method.
- OpenSSH Vulnerability
  - CVE-2023-38408: A critical OpenSSH vulnerability that allows remote code execution in the **`ssh-agent`** process through the PKCS#11 feature when SSH agent forwarding is enabled, and the forwarded agent is exposed to a malicious host. Affected versions are OpenSSH releases prior to 9.3p2.
  - CVE-2025-32728: A vulnerability in OpenSSH (before version 10.0) where the DisableForwarding directive fails to properly disable X11 and agent forwarding.
- OpenSSL Vulnerability
  - CVE-2026-45447: A use-after-free vulnerability exists in OpenSSL PKCS#7 signature verification when processing specially crafted PKCS#7 or S/MIME signed messages. It may cause application crashes, memory corruption, or potentially remote code execution.
  - CVE-2025-69419: It is out-of-bounds write vulnerability in OpenSSL's PKCS12_get_ friendlyname() API when processing a specially crafted PKCS#12 file containing a malformed UTF-16BE (BMPString) friendly name.
  - CVE-2026-28389: A NULL pointer dereference vulnerability in OpenSSL allows a specially crafted CMS EnvelopedData message with KeyAgreeRecipientInfo to cause an application crash during CMS decryption.
  - CVE-2026-28390: A NULL pointer dereference vulnerability in OpenSSL may allow a specially crafted CMS EnvelopedData message using KeyTransportRecipientInfo with RSA-OAEP encryption to cause an application crash during CMS decryption.
  - CVE-2026-7383: A heap buffer overflow vulnerability in OpenSSL's ASN.1 multibyte string handling may allow memory corruption, application crashes, or potentially arbitrary code execution when applications process extremely large attacker-controlled Unicode input using the affected ASN.1 APIs.

- CVE-2026-9076: A heap out-of-bounds read vulnerability in OpenSSL's CMS password-based decryption may allow a specially crafted CMS message to cause an application crash, resulting in a denial-of-service condition.
- CVE-2026-34180: An integer truncation vulnerability in OpenSSL's ASN.1 decoder may cause a heap buffer over-read when processing specially crafted DER-encoded ASN.1 data containing primitive elements larger than 2 GB. Applications that decode untrusted ASN.1 data using the affected **`d2i_*`** APIs on 64-bit Unix and Unix-like platforms may experience application crashes or unintended memory reads.
- CVE-2026-42766: A NULL pointer dereference vulnerability in OpenSSL may allow a specially crafted password-encrypted CMS message to cause an application crash during CMS decryption, resulting in a denial-of-service condition.

- libxml Vulnerability
  - CVE-2025-32415: A vulnerability in the **`libxml2`** library where a crafted XML document causes the system to read memory, potentially leading it to crashes or information leaks.
  - CVE-2025-32414: An out-of-bounds memory access vulnerability exists in **`libxml2`** before 2.13.8 and 2.14.x before 2.14.2. The flaw affects the Python bindings (xmlPythonFileRead and xmlPythonFileReadRaw) due to incorrect handling of return values caused by differences between bytes and characters.
- Jinja Sandbox Vulnerability
  - CVE-2025-27516: A vulnerability in the Jinja templating engine that allows arbitrary Python code execution bypassing sandbox restrictions through the **`attr`** filter. Exploitation requires an attacker to control template content in applications that process untrusted templates. Affected versions are Jinja releases prior to 3.1.6.
- Tar Path Traversal Vulnerability
  - CVE-2025-45582: A path traversal vulnerability in GNU Tar versions up to and including 1.35. It may allow attackers to overwrite critical files by using symbolic links during archive extraction.
- Apache HTTP Server Command Execution Vulnerability

- CVE-2025-58098: A vulnerability in Apache HTTP Server that affects versions 2.4.65 and earlier. It allows command execution through the SSI **`#exec`** directive due to improper query string handling when SSI and **`mod_cgid`** are enabled.

- A10 Vulnerabilities
  - A10-2024-0003: SSH TCP port forwarding is currently enabled by default on ACOS. This is the default OpenSSH behavior.
  - A10-2025-0002: A command injection vulnerability exists in the **`/axapi/v3/hotfix/apply`** endpoint. An authenticated user with write privileges can execute unauthorized system commands through specially crafted file parameters, potentially leading to privilege escalation, unauthorized access to data, configuration changes, or full system compromise (CVSS 8.7 – High).
  - A10-2025-0003: An arbitrary file read/write vulnerability exists in the ACOS axAPI export endpoint (**`/axapi/v3/export`**). An authenticated user with write privileges can exploit a path traversal issue.
  - A10-2025-0004: A blind command injection vulnerability exists in the SSL certificate export process. When a user exports an SSL certificate, the **`object_id`** parameter is passed directly to a shell command without proper validation. Since the parameter is used in a **`cp`** command executed through **`/bin/sh -c`**, an attacker can inject shell metacharacters such as **`;`**, **`|`**, **`&&`**, **`or`** **`||`** to execute unauthorized commands on the system. This occurs because user-supplied input is concatenated into the command without being properly escaped.
  - A10-2025-0005: A vulnerability exists in the **`/axapi/v3/file/ssh-pubkey`** endpoint allows users with write privileges to upload SSH public keys for other system accounts. This could enable an authenticated user to gain unauthorized SSH access to another account and potentially take control of it.
  - A10-2025-0007: The endpoint **`/gui/system/diagnostics/showtech/`** does not enforce proper Role-Based Access Controls (RBAC), allowing read-only users to export showtech logs through a direct POST request. Though the GUI may not display the export option to read-only users, the backend endpoint still processes the request.
  - A10-2025-0009: The SCP remote-file protocol used in most import or export functionality allows shell command execution if a user has valid credentials on the

host. A malicious attacker could break out of the web environment if remote authentication is not possible.

- A10-2025-0011: The axAPI incorrectly trusts the **`X-Forwarded-For`** HTTP header, allowing an attacker to spoof a loopback address and remotely authenticate as the local-only **`a10ch`** user.
- A10-2025-0012: A vulnerability caused by hardcoded passwords, tokens, and encryption keys in application source files. If exposed, these secrets could be misused by an attacker to gain unauthorized access and remain valid until they are changed.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.8

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.8 release:

The following topics are covered:

Application Access Management

ACOS 6.0.8 introduces the following new feature and enhancement for Application Access Management (AAM):

The following topic is covered:

Expand JWT Cache Capacity

ACOS now supports configuring the JWT (JSON Web Token) cache capacity at the global or system-level. Depending on the platform memory and system-level cache capacity, you can set the cache limit up to 1024000 entries using `system resource-usage jwt-cache-entry`.

Additionally, ACOS extends SNMP monitoring support to include operational statistics for the JWT cache. This enhancement allows you to monitor the number of tokens currently cached, cache hits, and maximum cache capacity through SNMP polling.

CLI Configuration

To configure the JWT cache capacity by entering a value between 102400 and the system supported maximum value, use the following command:

```
ACOS(config)# system resource-usage jwt-cache-entry 819100
```

Show Command

To verify the configured JWT cache capacity, use the following command:

```
ACOS(config)#show system resource-usage
Resource                              Current     Default     Minimum
Maximum
------------------------------------------------------------------------
-----
l4-session-count                      67108864    67108864    16777216
134217728
nat-pool-addr-count                   2000        2000        500
10000
class-list-ipv6-addr-count            4096000     4096000     4096000
8192000
class-list-ac-entry-count             3072000     3072000     3072000
6144000
auth-portal-html-file-size            20          20          4           120
auth-portal-image-file-size           6           6           1           80
max-aflex-file-size                   32          32          16
1024
aflex-table-entry-count               102400      102400      102400
20971520
max-aflex-authz-collection-number     512         512         256
4096
radius-table-size                     8000000     8000000     4000000
8000000
monitored-entity-count                131584      131584      3840
162816
authz-policy-number                   128         128         32
2000
ram-cache-memory-limit                12288       12288       3072
12288
ipsec-sa-number                       10000       10000       40
10000
auth-session-count                    419424      419424      41942
419424
class-list-entry-count                8192000     8192000     8192000
16384000
ngwaf-cache-entry                     4800000     4800000     480000
4800000
jwt-cache-entry                     819100      102400      102400      819200
```

SNMP OID

A new SNMP MIB module, jwtCacheModule (1.3.6.1.4.1.22610.2.4.8.594), has been introduced to provide SNMP support for JWT cache operational statistics and detailed cache entry information.

SNMP OID	Description
1.3.6.1.4.1.22610.2.4.8.594.1.2	Provides the overall JWT cache operational summary, including token count, cache hits, and maximum cache capacity (cacheOperTable).
1.3.6.1.4.1.22610.2.4.8.594.1.3	Provides detailed per-token cache information, including issuer, subject, audience, client IP, and TTL (cacheOperCacheListTable).

See Also:

- Application Access Management
- Command Line Interface Reference
- SNMP MIB Reference

Customizable JWT Response Code

ACOS supports customizing the response code error for HTTP 4XX status code (400–499) client when JWT (JSON Web Token) validation fails for scenarios such as expired, invalid, or missing JWT tokens.

This feature enables API gateways and applications to return consistent, standards-aligned error codes for JWT authentication failures, improving client behavior and simplifying troubleshooting.

CLI Configuration

To configure the JWT response code, use the following command:

```
ACOS(config)# aam jwt-authorization j1
ACOS(config-jwt-authz:j1)# client-error-resp-code <400-499>
```

See Also:

- Application Access Management
- Command Line Interface Reference

Application Delivery Controller

ACOS 6.0.8 introduces the following new features and enhancements for Application Delivery Controller (ADC):

The following topics are covered:

Enhanced Shared DNS Cache Management

ACOS introduces new CLI capabilities to view and clear DNS cache entries stored in the shared table of an SLB DNS template configured with **`enable-cache-sharing`**.

Previously, DNS cache management was limited to virtual port–specific operations. With this enhancement, ACOS provides dedicated commands to manage DNS cache entries at both the DNS template level and virtual-server/virtual port level.

Key Features

- Enable granular visibility and control over cached DNS responses, simplify cache maintenance across shared services, and improve operational efficiency in large DNS deployments.
- Shared cache entries used across multiple virtual ports or VIPs referencing the same DNS cache template can be cleared collectively.

- DNS cache clearing supports targeted filtering based on dns-class, dns-type, and domain.
- DNS cache visibility supports additional display options such as dns-class, dns-type, domain-name, all-entries, brief, and detail filters.
- All filter options may be used individually or in any combination.
- Consistent with the existing behavior, only one DNS cache-clear operation can be executed at a time
- If the specified virtual server, virtual port, or DNS template does not exist, the system returns no output.

CLI Configuration

To clear all shared cache entries for a specific DNS cache template, use the following command:

```
ACOS(config)# clear dns cache template template_name
```

To clear shared cache entries for a specific DNS cache template that match the specified filters, use the following command:

```
ACOS(config)# clear dns cache template template_name <filter_name_1 filter_1> <filter_name_2 filter_2>
```

To clear all DNS cache entries associated with a specific virtual server, virtual port, and port type, use the following command:

```
ACOS(config)# clear dns cache virtual-server <virtual_server_name> <virtual_port> <port_type>
```

To clear cache entries associated with a specific virtual server, virtual port, and port type that match the specified filters, use the following command:

```
ACOS(config)# clear dns cache virtual-server <virtual_server_name> <virtual_port> <port_type> <filter_name_1 filter_1> <filter_name_2 filter_2>
```

Show Commands

To display the shared cached entries for the specified DNS cache template (up to 10,000 entries), use the following command:

```
ACOS(config)# show dns cache template template_name
```

To display the shared cache entries for a specific DNS cache template that match the specified filters, use the following command:

```
ACOS(config)# show dns cache template template_name <filter_name_1 filter_1> <filter_name_2 filter_2>
```

To display the cached entries associated with a specific virtual server, virtual port, and port type, use the following command:

```
ACOS(config)# show dns cache virtual-server <virtual_server_name> <virtual_port> <port_type>
```

To display the cache entries associated with a specific virtual server, virtual port, and port type that match the specified filters, use the following command:

```
ACOS(config)# show dns cache virtual-server <virtual_server_name> <virtual_port> <port_type> <filter_name_1 filter_1> <filter_name_2 filter_2>
```

See Also:

- Application Delivery Controller Guide
- Command Line Interface Reference

Enhanced DNS Request Logging with RPZ Filter

ACOS supports Response Policy Zone (RPZ)-based request logging filters to ensure that logging is limited to DNS requests associated with RPZ-triggered actions. This provides more granular control over DNS logging behavior and helps reduce unnecessary log volume.

A new **standard-log** option and the **log-filter RPZ** capability have been added under the SLB DNS logging template. This enhancement enables selective logging of DNS request events based on RPZ policy actions. The **log-filter RPZ** is supported for both standard and custom DNS logging.

CLI Configuration

To enable RPZ-based logging under a standard DNS logging template, use the following commands:

```
ACOS(config)# slb template dns-logging log_template_name
ACOS(config-dns-logging)# standard-log request
ACOS(config-dns-logging-standard-log:request)# log-filter RPZ
```

To enable RPZ-based logging under a custom DNS logging template, use the following commands:

```
ACOS(config)#slb template dns-logging log_template_name
ACOS(config-dns-logging)# custom-log request
ACOS(config-dns-logging-custom-log:request)# log-filter RPZ
```

Sample Log Messages

The following examples show sample custom log entries generated when RPZ filtering is applied:

SYSLOG Example

Request Log

```
Dec 4 16:13:57 ACOS a10lb:[ACOS]<6> rcode=NoError arcount=1 ancount=0
qdcount=1 recordcounters=1|0|0|1 queryclass=IN src=1.1.0.206
dst=1.1.0.211 dpt=53 proto=UDP queryname=localdata88.com querytype=A\n
```

Request Log

```
Dec 4 16:13:57 ACOS a10lb:[ACOS]<6> responsesrc=rpz\n
```

CEF Example

Request Log

```
Dec 4 15:54:09 ACOS CEF:0|A10|CFW|6.0.8|486715327594364929|Custom DNS
request log|2|cs1=NoError cs1Label=Rcode Name cn1=1 cn1Label=ARCOUNT
cn2=0 cn2Label=ANCOUNT cn3=1 cn3Label=QDCOUNT cs2=1|0|0|1
cs2Label=qd|an|ns|ar cs3=IN cs3Label=Query Class src=1.1.0.206
dst=1.1.0.211 spt=44962 dpt=53 proto=UDP dhost=localdata88.com cs4=A
cs4Label=Query Type\n
```

Response Log

```
Dec 4 15:54:09 ACOS CEF:0|A10|CFW|6.0.8|486715327594364930|Custom DNS
response log|2|cs1=rpz cs1Label=Response Source\n
```

The following examples show sample standard log entries generated when RPZ filtering is applied:

SYSLOG Example

Request Log

```
Dec 4 16:13:57 ACOS a10lb:[ACOS]<6> UDP 1.1.0.206 55196 1.1.0.211 53
Type=Query QueryId=16008 Opcode=Query HeaderFlag=RD|AD QDCount=1
ANCount=0 NSCount=0 ARCount=1 dhost=localdata88.com QueryType=A
QueryClass=IN\n
```

Response Log

```
Dec 4 16:13:57 ACOS a10lb:[ACOS]<6> UDP 1.1.0.211 53 1.1.0.206 55196
Type=Response source=rpz QueryId=16008 Opcode=Query HeaderFlag=RD|AD
RCODE=00 QDCount=1 ANCount=1 NSCount=0 ARCount=0 response=Answer section
[localdata88.com A IN 3600 1.1.1.10;] \n
```

CEF Example

Request Log

```
Dec 4 15:54:09 ACOS CEF:0|A10|CFW|6.0.8|48671531470946304 3|Log DNS
Request Header and Questions|2|proto=UDP src=1.1.0.206 spt=44962
dst=1.1.0.211 dpt=53 cs1=Query cs1Label=Query cn1=34652 cn1Label=Query
ID cs2=Query cs2Label=Opcode cs3=RD|AD cs3Label=Header Flag cn2=1
cn2Label=Question Count cn3=0 cn3Label=Answer Record Count cn4=0
cn4Label=Authority Record Count cn5=1 cn5Label=Additional Record Count
dhost=localdata88.com cs4=A cs4Label=Query Type cs5=IN cs5Label=Query
Class\n
```

Response Log

```
Dec 4 15:54:09 ACOS CEF:0|A10|CFW|6.0.8|486715314709463052|Log ipv4 DNS
Response Header and Answer with Rcode|2|proto=UDP src=1.1.0.211 spt=53
dst=1.1.0.206 dpt=44962 cs1=Response cs1Label=Response cs2=rpz
cs2Label=Response Source cn1=34652 cn1Label=Query ID cs3=Query
cs3Label=Opcode cs4=RD|AD cs4Label=Header Flag cs5=00 cs5Label=RCODE
cn2=1 cn2Label=Question Count cn3=1 cn3Label=Answer Record Count cn4=0
cn4Label=Authority Record Count cn5=0 cn5Label=Additional Record Count
cs6=Answer section [localdata88.com A IN 3600 1.1.1.10;]
cs6Label=response content\n
```

See Also:

- Application Delivery Controller Guide
- Command Line Interface Reference

Enhanced DNS Custom Logging with Response Timeout Events

ACOS extends its custom DNS logging capabilities to include timeout event logging. It provides greater visibility into DNS queries that fail to respond within the configured timeout period.

A new **`timeout`** custom trigger reason has been added under the SLB DNS logging template.

Key Features

- Supports customizable timeout log formats using predefined keywords.
- Independent of standard DNS logging behavior.
- Triggers when DNS queries exceed configured timeout values.
- Timeout values are based on the configured TCP or UDP template settings (default 120 seconds).
- Timeout logs are sent exclusively to remote syslog servers unless local logging is explicitly configured through the **`acos-event`** route.

CLI Configuration

To configure a custom timeout log format, use the following commands:

```
ACOS(config)# slb template dns-logging log_template_name
ACOS(config-dns-logging)# custom-log timeout
ACOS(config-dns-logging-custom-log:timeout)# format "Djtimeout
$src$#$spt$ $dst$#$dpt$ $snatinfo$ $proto$ $queryid$ $recordcounters$
$opcode$ $headerflag$ $queryinfo$ $qdcount$ $ancount$ $nscount$
$arcount$"
ACOS(config-dns-logging-custom-log:timeout)# enable
```

Sample Log Messages

The following examples show sample custom log entries generated for a timeout event:

SYSLOG Example

```
Dec 2 15:32:40 TH4440S-1 a10lb:[ACOS]<6> partition-id<2> <l3v> Djtimeout
2002::11:11:11:9#53335 2002::11:11:11:28#53 2002::21:21:21:99#2055 UDP
B6B3 1|0|0|1 0 RD|AD xyz.com A IN 1 0 0 1\n
```

CEF Example

```
Dec 2 15:39:10 TH4440S-1 CEF:0|A10|CFW|6.0.8|486715327594364931|Custom
DNS timeout log|2|src=2002::11:11:11:9 spt=40055 dst=2002::11:11:11:28
dpt=53 flexString1=2002::21:21:21:99#2065 flexString1Label=SNAT Info
proto=UDP cs1=5B54 cs1Label=Query ID cs2=1|0|0|1 cs2Label=qd|an|ns|ar
cs3=0 cs3Label=Opcode cs4=RD|AD cs4Label=Header Flag cs5=xyz.com A IN
cs5Label=Query Info cn1=1 cn1Label=QDCOUNT cn2=0 cn2Label=ANCOUNT cn3=0
cn3Label=NSCOUNT cn4=1 cn4Label=ARCOUNT\n
```

Show Command

To view the available keywords for the custom timeout event log, use the **show slb dns-custom-logging-keywords timeout** command.

See Also:

- Application Delivery Controller Guide
- Command Line Interface Reference

Configurable Maximum UDP Payload Size for DNS responses

ACOS supports configuring the maximum UDP payload size for DNS responses sent to clients and specifying the UDP payload size in EDNS(0) OPT record of recursive-resolution (RR) queries. This enhancement provides granular control over DNS response sizing, reduces UDP fragmentation, and avoids potential packet loss for large DNS responses.

- New commands **dns-max-udp-size** and **max-udp-size**, and **edns-udp-size** provide control over maximum UDP payload sizes globally, per DNS template, and for the EDNS(0) UDP buffer-size field used in recursive-resolution (RR) queries.
- New counters **TC Response Sent Due to max-udp-size** and **Recursive Resolution TC Response Received** are added to track DNS responses truncated (TC bit set) due to exceeding the configured max-udp-size for UDP and truncated responses received from upstream servers during recursive resolution.

CLI Configuration

To configure a global maximum UDP payload size, use the following commands:

```
ACOS(config)# slb common
ACOS(config-common)# dns-max-udp-size <512-4096>
```

To configure the maximum UDP payload size in a DNS template, use the following commands:

```
ACOS(config)# slb template dns <template-name>
ACOS(config-dns)# max-udp-size <512-4096>
```

To configure the EDNS(0) UDP payload size for recursive DNS resolution, use the following commands:

```
ACOS(config)# slb template dns <template-name>
ACOS(config-dns)# recursive-dns-resolution
ACOS(config-dns-recursive-dns-resolution)# edns-udp-size <512-4096>
```

Show Command

To view the new counters, use the following command:

```
ACOS(config)# show slb virtual-server <name> <port-num> dns-<udp/tcp>
application-statistics
```

Limitations

DNS queries and responses handled by GSLB are not supported for the maximum UDP payload size options.

See Also:

- Application Delivery Controller Guide
- Command Line Interface Reference

aXAPI

ACOS 6.0.8 introduces the following new features and enhancements for aXAPI:

The following topic is covered:

Support Batch Operations

ACOS support batch API to send multiple axAPI requests in a single call, which reduces round-trip time and improves performance.

The following two endpoints are implemented:

- Batch-Get (`/axapi/v3/batch-get`) - for grouping multiple GET requests
- Batch-Post (`/axapi/v3/batch-post?ignore-errors={true|false}`) - for grouping multiple POST, PUT, DELETE requests.

See Also

- axAPIv3 Reference Guide

Carrier Grade NAT

ACOS 6.0.8 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

The following topic is covered:

NAT Pool Utilization Statistics

ACOS has enhanced the visibility of NAT pool resource utilization at the NAT pool level for dynamic NAT. It helps to efficiently manage subscribers across different devices, particularly in Scaleout deployments where IPs are distributed across multiple nodes.

With this enhancement, detailed TCP and UDP port utilization and user utilization metrics are available for each NAT pool. These statistics help in making decisions regarding scaling, capacity planning, and monitoring.

Show Command

- To view the NAT pool utilization statistics, use the following command. This is applicable only to LSN. The output displays TCP and UDP port utilization and user utilization statistics for each NAT pool.

```
ACOS(config)#show cgnv6 nat pool utilization
NAT Pool Usage/Utilization Statistics:
----------------------------
Pool Name     Tot. TCP Port  Used TCP Port  TCP Usage %   Tot. UDP
Port  Used UDP Port  UDP Usage %   Users allowed  Current Users  User
Occ. %
-------------------------------------------------------------------------
-----------------------------
nat_pool_1    16515072       129024         0             16515072
  129024         0             1024           2

 0
nat_pool_10   1032192        0              0             1032192
  0              0             1032192        0

 0
nat_pool_2    16515072       0              0             16515072
  0              0             16515072       0

 0
```

```
nat_pool_3    16515072        0               0               16515072
  0               0             110080          0

 0
nat_pool_4    1032192         0               0               1032192
  0               0             1032192         0

 0
nat_pool_5    1032192         0               0               1032192
  0               0             1032192         0

 0
nat_pool_7    1032192         0               0               1032192
  0               0             0               0

 0
--------------------------------------------------------------------------
------------------------------
```

- To view the IP addresses owned by the device in the Scaleout mode, use the following command. The output displays statistics for IP addresses that belong exclusively to the device under the Scaleout mode.

```
ACOS(config)#show cgnv6 nat pool statistics
LSN Address Pool Statistics:
----------------------------
Pool Name   Total IPs   Total Users   Free IPs     Used IPs   Total
IPs in cluster
--------------------------------------------------------------------------
-------------------
p1               1          1             0            1            1
p2               1          0             1            0            1
--------------------------------------------------------------------------
-------------------


p1 Address     Users  ICMP  Freed  Total  UDP   Freed  Total  Rsvd
 TCP  Freed  Total Rsvd
```

```
------------------------------------------------------------------------
------------------------------
   20.1.1.150  1      0     0      0      49920 768    50688  50000  0
   0      0     30000

p2 Address     Users  ICMP  Freed  Total  UDP   Freed  Total  Rsvd
TCP  Freed  Total Rsvd
------------------------------------------------------------------------
------------------------------
  20.1.1.151   0      0     0      0      0     0      0      0      0
   0      0     0
```

SNMP OID

The following SNMP OID can be used to view the NAT pool utilization percentage:

1.3.6.1.4.1.22610.2.4.8.717.1.1.1

See Also:

- IPv4-to-IPv6 Transition Solutions Guide
- Command Line Interface Reference

Management Access and Security

ACOS 6.0.8 introduces the following new feature and enhancement for Management Access and Security (MAS):

NOTE: For configuration, refer *Management Access and Security (MAS) Guide* and for specific CLI commands, refer *Command Line Reference Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topic is covered:

TACACS+ over TLS Authentication Support

ACOS supports TACACS+ over Transport Layer Security (TLS) to enhance the security of administrative authentication.

This feature encrypts all TACACS+ communication between the ACOS device and the Cisco Identity Services Engine (ISE) server using TLS 1.3 certificates and keys, ensuring that credentials and session data are protected from interception or tampering.

This feature is supported for deployments using Cisco ISE 3.4 Patch 2 or later only.

CLI Configuration

TACACS+ over TLS authentication can be configured with or without Certificate Authority (CA) verification, depending on the security requirements.

To configure the TACACS+ over TLS authentication with CA verification

```
ACOS(config)#tacacs-server host 10.19.4.210 secret 1 port 6049 over-tls
cert TH_test private-key TH_test custom-ca  X_CA
```

To configure the TACACS+ over TLS authentication without CA verification

```
ACOS(config)# tacacs-server host 10.19.4.210 secret 1 port 6049 over-tls
cert TH_test private-key TH_test skip-cert-verification
```

Show Command

To verify if the TACACS+ over TLS authentication configuration:

```
ACOS(config)#show running-config tacacs-server
```

See Also:

- Management Access and Security Guide
- Command Line Interface Reference

MIB

ACOS 6.0.8 introduces the following new features and enhancements for SNMP MIB:

The following topic is covered:

SNMP Support for PSU Metrics

ACOS has extended SNMP monitoring support to include Power Supply Unit (PSU) metrics.

The SNMP OIDs `1.3.6.1.4.1.22610.2.4.1.5.11.1` and `1.3.6.1.4.1.22610.2.4.1.5.12.1` are enhanced to include input voltages, current, and power readings for each PSU.

The values are updated every 60 seconds by default, and the interval is configurable. This enhancement allows external network monitoring systems to check the PSU status remotely without CLI access.

See Also:

- SNMP MIB Reference

SNMP Support for Common Operational Interfaces

ACOS extends SNMP monitoring support for common operational interface statistics, including physical Ethernet ports, logical interfaces, and Small Form-factor Pluggable (SFP) transceivers.

This enhancement also enables the retrieval of SFP module health and performance data, such as Transmit (TX) Power, Receive (RX) Power, Current, Voltage, and Temperature through SNMP polling.

The SNMP polled data for SFP transceiver interfaces matches the output of the show interfaces transceiver command.

SNMP OID

A new SNMP MIB module, interfaceCommonModule (1.3.6.1.4.1.22610.2.4.8.200), has been introduced in the ACOS-INTERFACE-COMMON-MIB.txt file to provide SNMP support for common operational interface statistics.

The following OID is defined under this module:

SNMP OID	Description
1.3.6.1.4.1.22610.2.4.8.200.1.4	Provides transceiver-level operational data (commonOperInterfacesTransceiversInfoTable).

CLI Configuration

To allow SNMP monitoring for common operational interface statistics, enable the new CM subagent and SNMP service:

```
ACOS(config)# snmp-server enable schema-agent
ACOS(config)# snmp-server enable service
```

See Also:

- SNMP MIB Reference
- Command Line Interface Reference

Network Configuration

ACOS 6.0.8 introduces the following new feature and enhancement for the Network Configuration:

NOTE: For configuration, refer *Network Configuration Guide* and for specific CLI commands, refer *Command Line Reference Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topic is covered:

Support for Class E Addressing and BGP Advertisements

ACOS supports the Class E address (240.0.0.0/4) configuration and advertises it through the Border Gateway Protocol (BGP). The IETF has reserved the Class E addresses for experimental purposes and future use. However, they are used in

private datacenters and public clouds for seamless integration with environments that use Class E address space.

A new system-level command **`system ip class-e-address-range-enable`** has been introduced. Once the command is enabled, you can assign the Class E addresses to interfaces such as the management interface, data interface, and virtual ethernet interface. The addresses are advertised through BGP, and the routes are installed into the Routing Information Base (RIB) and Forwarding Information Base (FIB).

Additionally, the routing protocols, such as OSPF, IS-IS, BFD, and static routing are supported.

CLI Configuration

To enable Class E address configuration, use the following command:

```
ACOS(config)# system ip class-e-address-range-enable
```

NOTE: For changes to take effect, a system reload is required.

See Also:

- Network Configuration Guide
- Command Line Interface Reference

Enhanced IPv6 Next-Hop Selection in BGP

ACOS supports selecting the global IPv6 address as the preferred next hop in BGP route advertisements when IPv6 global address and IPv6 link-local are received for the route.

In earlier releases, ACOS always used the IPv6 link-local next hop address for forwarding when both a link-local and a global IPv6 next hop address were received for a route.

CLI Configuration

The following commands configure global IPv6 address as the preferred next hop address:

```
ACOS(config)#router bgp 100
```

```
ACOS(config-bgp:100)#bgp router-id 100.100.100.100
ACOS(config-bgp:100)#neighbor 3340::197 remote-as 197
ACOS(config-bgp:100)#address-family ipv6
ACOS(config-bgp:100-ipv6)#nexthop prefer-global
ACOS(config-bgp:100-ipv6)#neighbor 3340::197 activate
```

Limitation

This feature is applicable only for the IPv6 address family.

See Also:

- Network Configuration Guide
- Command Line Interface Reference

Platforms

ACOS 6.0.8 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

DNS Cache Capacity Expansion for Large Memory Platforms

ACOS has now increased the maximum DNS cache capacity on Thunder platforms with 128 GB or more memory. This allows up to 4,194,304 (4 million) entries system-wide. The total cache capacity across all global, per-template, and per virtual port DNS caches shares the 4 million limit.

When DNS caching is used with DNS load balancing in large-scale deployments, the cache requirement often exceeds the previous maximum limit which is 2 million

entries. In such scenarios, the 2 million limit is inadequate for efficient and effective operation.

This enhancement enables Thunder platforms with more memory to accommodate up to 4 million cache entries. Thereby, maintaining better performance and stability.

NOTE: The maximum limit for DNS cache entry size varies depending on the platform RAM capacity.

The following table lists the maximum number of supported DNS cache entries based on the memory allocated to the platform:

Allocated RAM	Maximum DNS Cache Entries
≤ 4 GB	65,535
4 GB – 16 GB	512,000
16 GB – 128 GB	2,097,152
≥ 128 GB	4,194,304

CLI Configuration

To configure the maximum number of DNS cache entries per VIP, use the following commands:

```
vThunder(config)# slb template dns test
vThunder(config-dns)# max-cache-size <0-4194304>
```

On Thunder platforms with 128 GB or higher memory, the configurable range for this command has been increased, with the maximum supported limit set to 4 million (4M) entries.

See Also:

- Command Line Interface Reference

Capacity FlexPool License Enables Core Allocation Based on Bandwidth

ACOS supports core allocation based on licensed bandwidth for Capacity FlexPool licenses on the TH1060S device. This enhancement enables the TH1060S to automatically adjust CPU core allocation based on the licensed bandwidth capacity managed through A10 Control.

NOTE: The NGWAF feature bandwidth is not used when evaluating the bandwidth for threshold changes, only the licensed FlexPool bandwidth is considered.

The following table shows the bandwidth and core mapping for the TH1060S device:

Platform	Bandwidth Range	Cores
TH1060S	≥10G and <25G	9 cores
TH1060S	≥25G	20 cores

NOTE: The bandwidth to core mapping aligns with the TH1060S modular licensing tiers. For example, TH1060S below 25G uses 9 cores, and 25G or above uses 20 cores.

When the configured bandwidth crosses a core-restricted threshold, TH1060S would require a reboot to apply the updated core configuration. If the bandwidth threshold was crossed but a reboot was not performed, a subsequent reload will also trigger a reboot so that the core change can take effect. Bandwidth changes that remain within the same threshold are applied immediately without a reboot.

NOTE: If the configured bandwidth crosses a core-restricted threshold, a reboot is required for the updated core configuration to take effect.

See Also:

- Capacity FlexPool
- A10 Control Documentation

Support for AWS IMDSv2

ACOS now supports AWS Instance Metadata Service v2 (IMDSv2) for vThunder instances deployed in Amazon Web Services environments.

With IMDSv2 support, ACOS can:

- Comply with AWS security standards
- Improve reliability and prevent metadata-related service interruptions

To enable IMDSv2 for vThunder instances, configure the following EC2 metadata options:

- Metadata accessible - **Enabled**
- Metadata version - Select **V2 only (token required)**

See Also:

- Installing vThunder on Amazon Web Services (AWS)

Enhanced Thunder 8665(S) Platform

Thunder 8665(S), a high-end 6th-generation FTA platform, supports ADC deployments. This is offered with CFW license.

See Also:

- Platform Compatibility Matrix
- Release Notes

Enhanced axdebug File Size

The axdebug utility is used to capture trace packets on ACOS devices. The capture file size has been extended from 300 MB to 6000 MB, allowing larger trace captures. The default file size remains 300 MB.

For multi-PU devices, ACOS can generate separate debug files for PU1 and PU2, each with a maximum size of 6000 MB. This enhancement offers greater flexibility in trace data collection and helps optimize disk space usage.

CLI Configuration

- To set the axdebug buffer file, use the following command:

```
ACOS(config)#axdebug
ACOS((axdebug)#file-size <300-6000>
```

- To set the axdebug buffer file in multi-PU, use the following command:

```
log in to PU1
ACOS-PU1(config)#axdebug
ACOS-PU2(config)#file-size <300-6000>
....
log in to PU2
ACOS-PU2(config)#axdebug
ACOS-PU2(config)#file-size <300-6000>
```

See Also:

- Command Line Interface Reference

Scaleout

ACOS 6.0.8 introduces the following new feature and enhancement for Scaleout:

The following topics are covered:

BGP Distribution of Transparent Firewall Prefixes in Scaleout

ACOS has enhanced the Scaleout traffic redirection for Firewall deployments. This enhancement minimize unnecessary traffic redirection by dividing the Scaleout traffic into user-groups and advertising the routes at the user-group level via BGP.

In deployments where the same IPv4 or IPv6 prefix is used for both Firewall traffic and CGN traffic (for example, IPv6 prefix for accessing IPv6 networks (Firewall) and using the same prefix for NAT64 traffic when accessing IPv4 networks (CGN)), the same client can be NATed or not NATed depending on its destination. To support such scenarios, ACOS allows applying the user-group-assignment template to CGN traffic.

NOTE: This is a beta feature, intended for evaluation only. Contact your sales representative for further assistance.

Firewall Deployment Configuration

CLI Configuration

- To divide traffic among user-groups based on the IP prefix (IPv4 or IPv6), configure the user-group assignment template using the following command:

```
ACOS(config)# scaleout user-group-assignment-template template-name
ACOS(config-template:temp-name)# ipv4-prefix | ipv6-prefix[
assignment-prefix-length prefix-len ]
```

  The specified IPv4 or IPv6 prefix is divided into subnets, and each subnet is sequentially assigned to a user-group. By default, traffic is assigned to user-groups at the single IP level (/32). You can use **assignment-prefix-length***prefix-len* to group multiple IPs into larger subnet blocks.

- To activate a specific user-group assignment template, use the following command:

```
ACOS(config)# scaleout active-user-group-assignment template_name
```

  The user-group assignments defined in the active template set the traffic map. After the activation, the Scaleout cluster begins forwarding packets based on this traffic map.

  NOTE: Only one template can be activated per-partition at a time, and the active template cannot be modified.

- To advertise traffic routes are advertised via BGP to the neighbours, use the following command:

```
ACOS(config)# router bgp <num>
ACOS(config-bgp:num)# redistribute public-ip
```

  For example, if there are two nodes in the Scaleout cluster, and the IP prefix configured on the activated **user-group-assignment-template** is *178.245.136.0/21***assignment-prefix-length***29*, the advertised routes will inform neighbors that packets destined for 178.245.136.0/29 will be forwarded to node1, while packets for 178.245.136.8/29 will be forwarded to node2.

Show command

To view the user-group assignment information for a specified template, use the following command:

```
ACOS(config)# show scaleout user-group-assignment template template_name
```

CGN Deployment Configuration

CLI Configuration

- To divide traffic among user-groups based on the IP prefix (IPv4 or IPv6), configure the user-group assignment template using the following command:

```
ACOS(config)# scaleout user-group-assignment-template template-name
ACOS(config-template:temp-name)# ipv4-prefix | ipv6-prefix
[assignment-prefix-length | assignment-prefix-auto | private-ip |
service-config-template | user-group-range]
```

The specified IPv4 or IPv6 prefix is divided into subnets, and each subnet is sequentially assigned to a user-group. By default, traffic is assigned to user-groups at the single IP level (/32).

NOTE:

- A maximum of eight templates can be configured in a system.
- IP address overlapping is forbidden between any two prefix assignments.
- This command takes effect only when the template is activated.

- To associate a user-group assignment template with service-config template, use the following command:

```
ACOS(config)# scaleout user-group-assignment-template tp1
ACOS(config-template:tp1)#178.245.136.0/21 assignment-prefix-length
/29 service-config template traffic-slice 1
ACOS(config)#scaleout active-user-group-assignment tp1
```

The service-config template under user-group-assignment must match the one configured under NAT pools for CGN traffic.

Traffic slicing decisions occur before application logic. Misalignment between slicing and application configuration can result in packet drops.

NOTE: Only one template can be activated per-partition at a time, and the active template cannot be modified.

- To advertise routes created without NAT using BGP-based route advertisement. The client's IP must be configured under user-group-assignment template and must not be marked as "private-ip". If you do not want to advertise the client's IP through BGP, mark the assignment as "private-ip, configure the following command:

```
ACOS(config)# router bgp <num>
ACOS(config-bgp:num)# redistribute public-ip
```

Show commands

- To view the user-group assignment information for a specified template, use the following command:

```
show scaleout user-group-assignment template template_name
```

- To view the user-group assignment information for a specific IP, use the following command

```
show scaleout user-group-assignment inside-user ipv4_address
show scaleout user-group-assignment inside-user ipv6_address
```

See Also:

- Scaleout Configuration Guide
- Command Line Reference

Support for Scaleout Failure-Domain

ACOS has introduced a failure-domain mechanism in Scaleout deployments to improve cluster resiliency and traffic continuity. This enhancement provides a way to group cluster nodes together to create failure domains and ensures that nodes within the same failure domain do not become a backup or standby for each other.

This is particularly useful for virtual deployments where multiple instances can be hosted on the same server and can fail together in case the host restarts.

A new command, **`failure-domain <id-string>`** is introduced to implement failure domains for the nodes in the cluster. Nodes with the same failure-domain "string" belong to the same failure domain. By default, the node uses the Scaleout device-id as its failure-domain if there is no explicit failure-domain configuration.

CLI Configuration

To configure failure-domain on nodes, use the following commands:

```
ACOS(config)#scaleout 1
ACOS(config-cluster:1)#local-device
ACOS(config-cluster:1-local-device)#priority 100
ACOS(config-cluster:1-local-device)#failure-domain <id-string>
ACOS(config)#scaleout app enable
```

Show command

To view a list of all nodes and the failure-domain information, use the following command:

```
show scaleout failure-domain
```

Limitations

This feature has following limitations:

- The failure domain is configurable only from the shared partition.
- The Scaleout on the node must be disabled before changing the failure-domain configuration. Else, the command will not be accepted.

See Also:

- Scaleout Configuration Guide
- Command Line Interface Reference

SSL Insight

ACOS 6.0.8 introduces the following new feature and enhancement for SSL Insight (SSLi):

NOTE: For SSLi configuration steps, refer *SSL Insight Configuration Guide*. Similarly, for CLI commands, refer *Command Line Reference Guide*.

The following topic is covered:

Web Category SDK Verification Updates

ACOS has enhanced the SSL Insight (SSLi) web categorization performance and compatibility by upgrading the BrightCloud Web Category SDK from version 4.40 to 5.38.

This upgrade provides faster lookups, improved classification accuracy, and native support for HTTPS only communication between ACOS and BrightCloud servers. A new show command show web-category license has been introduced view or verify the configured SDK type (Legacy or New).

Show Command

To view the configured SDK type value, use the following command:

```
ACOS#show web-category license
Module Type                    : New/Legacy
Module Status                  : Disabled
License Status                 : License is valid
License Type                   : show license-info for webroot type
License Expiry                 : show license-info for expiration
Remaining Period               : show license-info for expiration
Grace Period Status            : show license-info for grace period
Grace Period                   : show license-info for grace period
UUID/SN                        : TH33075E21040038
```

System and Security

ACOS 6.0.8 introduces the following new features and enhancements for System Configuration and Administration:

NOTE: For more information and details, refer *System Configuration and Administration Guide*.

The following topics are covered:

Introduced Configuration Synchronization Between A10 Control and ACOS

A configuration synchronization mechanism is introduced to synchronize the configurations from ACOS devices to A10 Control. Instead of relying on periodic manual scans, ACOS now pushes real-time updates to A10 Control using a Kafka-based notification channel.

When any changes are made directly on ACOS devices—whether through CLI or aXAPI—the devices notify A10 Control with the updated configuration version. A10 Control receives the notification and provides an option to synchronize the configuration to send an alert. This ensures that the latest device configuration is visible, reducing the risk of mismatched settings.

CLI Configuration

- To track or view the configuration changes per partition, the **`system config-version`** command is used. The parameters of this command are non-configurable and their values are incremented automatically when the configuration changes. The values can be viewed using the **`show running-config`** command:

```
ACOS(config)# show running-config system config-version
!Section configuration: 102 bytes
!
 system config-version
   version 0.22
   updated-at "09-01 17:36:27 IST 2025"
   modified-by admin
!
```

NOTE: The **version** and **updated-at** parameters can be set using aXAPI.

- To configure the interval (in seconds) for the Kafka-based notifications, use the following command:

```
ACOS(config)# system config-mgmt notifications
ACOS(config-notifications)# period <0-60>
```

Limitation

VCS, High Availability, and GSLB cluster deployments are not supported.

See Also:

- A10 Control Integration Guide
- Command Line Interface Reference
- A10 Control Documentation

Enhancement to Device Configuration Encryption

ACOS supports a dynamic hash-key mechanism along with symmetric encryption to ensure that each device configuration is encrypted based on unique device properties. This enhancement allows to set a custom passphrase for encrypting the password. To maintain security and privacy, customers will have complete control over the passphrase.

Additionally, to ensure uniform security across all devices within VCS or VRRP clusters, the same encryption passphrase must be used on all nodes.

NOTE: Once the passphrase is set, downgrading to software versions that do not support this feature is not supported.

CLI Configuration

To set the new passphrase, use the following command:

```
ACOS(config)# system update-passphrase
Note: After changing to a new passphrase, you cannot downgrade to the
previous release. Do you want to continue with updating to new
passphrase? [yes/no]: yes
Please enter your new passphrase (minimum 8 characters): passwords
```

Show Commands

The following show commands are enhanced to display the newly encrypted passwords:

- `show run`
- `show startup-config`

Limitations

This feature has the following limitations:

- The 'no' CLI functionality is not supported.
- The copying of external configuration to the running configuration is not supported because it is not in an interactive mode.
- aXAPI is not supported.

See Also:

- System Configuration and Administration Guide
- Command Line Interface Reference

Disk Encryption Support

ACOS introduces support for Disk Encryption to protect data stored on the device by converting readable data into an unreadable format called *ciphertext*.

When disk encryption is enabled, data-at-rest becomes inaccessible to unauthorized users unless they provide a valid passphrase or decryption key. This enhances data security and helps prevent unauthorized access.

Supported Devices

- Thunder 3745
- Thunder 3350
- Thunder 5960
- Thunder 1060

License Requirement

Requires a valid Disk Encryption license. For more information, reach out to the *A10 Sales team*.

CLI Configuration

To encrypt the disk, use the following command:

```
ACOS(config)#system enable-disk-encryption cipher {aes | serpent |
twofish} {passphrase <passphrase_string> | passphrase-base64 <base64_
format_passphrase>}
```

Limitations

- Upgrading or downgrading is supported only if the disk encryption feature is available in the target ACOS version.
- Both primary and secondary boot images must support disk encryption.

See Also:

- Global Licensing Manager (GLM)
- System Configuration and Administration Guide
- Command Line Interface Reference

Automatic System Reboot When Disk Becomes read-only

ACOS has introduced a new failsafe mechanism that automatically reboots a device when the disk goes into a read-only state. The read-only state causes device

instability, such as login failure, ping failure, reload loops, no varlog, or resembling a hung state. In these scenarios, the automatic reboot starts. This process stops all running services and restarts all core system components on the device.

The logs generated on the console and syslog server indicate disk read-only detection and reboot initiation.

CLI Configuration

To enable auto-reboot when disk becomes read-only, use the following command:

```
ACOS(config)# system reboot-disk-read-only <minutes>
```

You can specify the range between 0 to 1440 minutes. By default, it is set to “0”, which is disabled.

Restore ACOS Device License After System Reset

ACOS supports restoring an ACOS device license after the device is reset to its factory default settings. This feature helps to reapply or reactivate the A10 license after the system is reset. This capability is available only on the ACOS devices that use modular licensing.

It supports all the Thunder and vThunder devices.

CLI Configuration

To restore the ACOS device license, use the following command:

```
ACOS(config)# system-reset preserve-license
```

Show Command

To verify the restored ACOS device license, use the following command:

```
show license-info
```

Limitation

This feature has the following limitations:

- It does not support cThunder devices.
- It does not support ACOS devices that use Perpetual license.

See Also:

- System Configuration and Administration Guide
- Command Line Interface Reference

Threat Protection System

ACOS 6.0.8 introduces the following new feature and enhancement for Threat Protection System (TPS):

NOTE: For TPS-related configuration, refer to DDoS Mitigation Guide. Similarly, for TPS-related CLI commands, refer to DDoS Command Line Reference Guide.

The following topic is covered:

Security Updates

The following security vulnerabilities are addressed in this release:

Cross-Site Scripting (XSS) Vulnerabilities:

- CVE-2016-10735: It is a Cross-Site Scripting (XSS) vulnerability that affects Bootstrap versions prior to 3.4.0 and 4.0.0-beta.2. The vulnerability is caused by improper handling of the data-target attribute.
- CVE-2018-14040: It is a Cross-Site Scripting (XSS) vulnerability that affects Bootstrap versions prior to 4.1.2. The vulnerability exists in the collapse plugin due to improper handling of user input in the data-parent attribute.
- CVE-2018-14041: It is a Cross-Site Scripting (XSS) vulnerability that affects Bootstrap versions prior to 4.1.2. The vulnerability exists in the ScrollSpy component due to improper handling of the data-target attribute.
- CVE-2018-14042: It is a Cross-Site Scripting (XSS) vulnerability that affects Bootstrap versions prior to 4.1.2. The vulnerability exists in the tooltip component due to improper handling of user input in the data-container property.

- CVE-2018-20677: It is a Cross-Site Scripting (XSS) vulnerability that affects Bootstrap. The vulnerability is caused by improper validation of user input in the affix configuration target property.
- CVE-2019-8331: It is a Cross-Site Scripting (XSS) vulnerability that affects Bootstrap. The vulnerability exists in the tooltip and popover components due to improper sanitization of the data-template attribute.
- CVE-2021-40975: It is a Cross-Site Scripting (XSS) vulnerability that affects Bootstrap. The vulnerability exists in jQuery versions 3.0 to 3.2.1, and jQuery 3.7.1.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.7-P2

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.7-P2 release:

The following topics are covered:

Enhancement to Device Configuration Encryption

ACOS supports a dynamic hash-key mechanism along with symmetric encryption to ensure that each device configuration is encrypted based on unique device properties. This enhancement allows to set a custom passphrase for encrypting the password. To maintain security and privacy, customers will have complete control over the passphrase.

Additionally, to ensure uniform security across all devices within VCS or VRRP clusters, the same encryption passphrase must be used on all nodes.

NOTE: Once the passphrase is set, downgrading to software versions that do not support this feature is not supported.

CLI Configuration

To set the new passphrase, use the following command:

```
ACOS(config)# system update-passphrase
Note: After changing to a new passphrase, you cannot downgrade to the
previous release. Do you want to continue with updating to new
passphrase? [yes/no]: yes
Please enter your new passphrase (minimum 8 characters): passwords
```

Show Commands

The following show commands are enhanced to display the newly encrypted passwords:

- `show run`
- `show startup-config`

Limitations

This feature has the following limitations:

- The 'no' functionality is not supported.
- The copying of external configuration to the running configuration is not supported because it is not in an interactive mode.
- aXAPI is not supported.

See Also:

- System Configuration and Administration Guide
- Command Line Interface Reference

Threat Protection System

ACOS 6.0.7-P2 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to DDoS Mitigation Guide. Similarly, for TPS-related CLI commands, refer to DDoS Command Line Reference Guide.

Enhancements in ACOS 6.0.7-P1

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.7-P1 release:

The following topic is covered:

Threat Protection System

ACOS 6.0.7-P1 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to DDoS Mitigation Guide. Similarly, for TPS-related CLI commands, refer to DDoS Command Line Reference Guide.

Enhancements in ACOS 6.0.7

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.7 release:

The following topics are covered:

Application Delivery Controller

ACOS 6.0.7 introduces the following new features and enhancements for Application Delivery Controller (ADC):

The following topics are covered:

Increased RPZ File Entries Capacity

ACOS has increased the RPZ (Response Policy Zone) file entry capacity from 64K (with a limit of 8K entries per file and a maximum of 8 files per DNS template) to 1.5

million. These entries can be added to a single RPZ file or distributed across multiple RPZ files, but the total number of entries across the system cannot exceed 1.5 million.

This enhancement provides enhanced network security and greater traffic control.

Show commands

- To view the list of RPZ file(s) currently on the system along with their associated DNS templates, use the **`show rpz`** command.
- To view the contents of a specific RPZ file, use the **`show rpz`** *`[filename]`* command.

See Also:

- DDoS Mitigation Guide (For ADC)
- Command Line Interface Reference

Enhanced Custom Logging in DNS Logging Template

The Custom logging format for ACOS is enhanced to provide customizable DNS logging to improve usefulness and precision of DNS traffic logs. This feature allows you to customize the logging configurations by selecting specific fields, defining sequence, and content.

The **`custom-log`** command is added to the SLB DNS logging template to configure a custom logging format for the ACOS.

CLI Configuration

The following example configures the **`custom-log`** in the DNS logging template:

```
ACOS(config)#slb template dns-logging dns180
ACOS(config-dns-logging)# custom-log request
ACOS(config-dns-logging-custom-log:request)# format "queryid is
$queryId$ opc is $opcode$ rcode is $rcode$ rcode string is $rcodestr$"
ACOS(config-dns-logging-custom-log:request)# enable
ACOS(config-dns-logging-custom-log:request)# custom-log response
```

```
ACOS(config-dns-logging-custom-log:response)# format "querid is
$queryId$ opc is $opcode$ Response src is $respsrc$ Rcode is $rcode$ NAT
info is $snatinfo$"
ACOS(config-dns-logging-custom-log:response)# enable
```

Sample Log Messages

Following is the example of custom message strings and corresponding logs generated:

- For request and response logs:

SYSLOG:

```
Syslog 174 LOCAL0.INFO: Mar 26 10:53:06 TH4440S-1 a10lb:[ACOS]<6>
partition-id<2> <l3v> queryid is DEA5 opc is 0 rcode is 0000 rcode
string is NoError\n
Syslog 205 LOCAL0.INFO: Mar 26 10:53:06 TH4440S-1 a10lb:[ACOS]<6>
partition-id<2> <l3v> querid is DEA5 opc is 0 Response src is backend
Rcode is 0000 NAT info is 21.21.21.99#2050\n
```

CEF:

```
Syslog 238 Mar 26 10:54:59 TH4440S-1
CEF:0|A10|CFW|6.0.7|486715327594364929|Custom DNS request log|2|cs1=1FA7
cs1Label=Query ID cs2=0 cs2Label=Opcode cs3=0000 cs3Label=RCODE
cs4=NoError cs4Label=Rcode Name\n
Syslog 300 Mar 26 10:54:59 TH4440S-1
CEF:0|A10|CFW|6.0.7|486715327594364930|Custom DNS response
log|2|cs1=1FA7 cs1Label=Query ID cs2=0 cs2Label=Opcode cs3=backend
cs3Label=Response Source cs4=0000 cs4Label=RCODE
flexString1=21.21.21.99#2056 flexString1Label=SNAT Info\n
```

Show command

To view the available keywords for custom log, use the **`show slb dns-custom-logging-keywords`** command.

See Also:

- Application Delivery Controller Guide
- Command Line Interface Reference

Increased the Maximum HTTP Header Name Length

ACOS has increased the maximum limit of HTTP header name length from 64 to 8191 bytes for HTTP traffic. HTTP header name length for TPS, SIP, and HTTP template modules remain the same as 64 bytes.

This change allows you to process HTTP header names that are longer than previously allowed in HTTP traffic, which is important for advanced web applications.

See Also:

- Application Delivery Controller Guide

Match SNI Domain Name in SSL Certificate

ACOS supports an option for Server Name Indication (SNI) validation in the system to prevent unnecessary information leak to the client.

When this feature is enabled, ACOS verifies if the SNI matches any domain name listed in the server certificates Common Name (CN) or SAN DNS fields. If not matched, the ACOS immediately disconnects the client without disclosing any certificate or server-related information.

CLI Configuration

To match the CN and SAN DNS fields in the configured certificates, use the following command:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# require-sni-cert-matched
```

NOTE: A maximum of three certificates can be configured with different algorithm in the client-ssl template.

Limitations

This feature has the following limitations:

- Supported SSL Modules: software-tls13 module and QAT module.
- The maximum number of SAN DNS type entries in the certificates configured in the client ssl-template is 16.
- Due to infrastructure limitation, replacing a valid certificate with an invalid certificate of the same name via the import command may cause unexpected problems.
- Wildcard certificates are supported. However, only with the complete left-most label and single wildcard (e.g DNS=*.a10networks.com).
- Fragment (DNS=ww*.a10networks.com) or part of the label other than the left-most label (e.g. DNS=www.*.a10networks.com) or their combinations is not supported.

See Also:

- Application Delivery Controller Guide
- Command Line Interface Reference

Performance Improvement for Per Virtual Port DNS Caching

The per virtual port DNS cache is enhanced to support a larger lookup table size. This enhancement improves the performance of DNS cache processing at the virtual-port level, by reducing the overall lookup cost.

NOTE: The new lookup table size correlates with system memory capacity.

See Also:

- Application Delivery Controller Guide

aFleX

ACOS 6.0.7 introduces the following new features and enhancements for aFleX.

NOTE: For more information, refer *aFleX Scripting Language Reference*.

The following topics are covered:

HTTP/2 Proxy Support in Web Category Lookup in aFleX

ACOS has enhanced the web category and reputation feature in aFlex to support the HTTP/2 proxy. With this enhancement, ACOS first attempts to retrieve the web category or reputation data from its local cache. If the required data is not available and if this feature is enabled, ACOS initiates a real-time query with the BrightCloud server. During this time, the aFlex process pauses temporarily, until it receives a response.

This feature is only applicable to HTTP_REQUEST and HTTP_REQUEST_DATA events.

NOTE: Ensure that there is a valid active Webroot license , and a properly downloaded web-category database.

Limitation

This feature is not supported when an SLB template DNS over HTTP/HTTPS (doh) is bound to an SLB virtual port.

See Also:

- aFleX Scripting Language Reference Guide

Carrier Grade NAT

ACOS 6.0.7 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

The following topics are covered:

Enhancement to CGN NAT Session Logging

ACOS supports CGN NAT session logging specifically for designated destination IP address ranges. You can configure a list of address prefixes to enable logging only for those destinations. This enhancement provides greater flexibility in logging behavior.

Also, logging for specific destination IP addresses can now be enabled or disabled using the firewall logging template.

CLI Configuration

- To enable the CGN NAT logging for the TCP port and UDP port, use the following commands:

```
ACOS(config)# cgnv6 template logging temp
ACOS(config-logging:temp)#enable-log-by-destination
ACOS(config-logging:temp-filter)# tcp port 10000 to 20000
ACOS(config-logging:temp-filter)# udp port 1 to 65535
```

- To enable the logging of TCP port and UDP port using the Firewall logging template, use the following commands:

```
ACOS(config)# fw template logging temp
ACOS(config-logging)#enable-log-by-destination
ACOS(config-logging-filter)# tcp port 10000 to 20000
ACOS(config-logging-filter)# udp port 1 to 65535
```

- To enable the logs by destination IPv4 address using the Firewall logging template, use the following commands:

```
ACOS(config)# fw template logging test
ACOS(config-logging)# enable-log-by-destination
ACOS(config-logging-filter)# udp port 7000
ACOS(config-logging-filter)# icmp
ACOS(config-logging-filter)# 10.2.3.0/24
ACOS(config-logging-filter-ip)# tcp port 80
ACOS(config-logging-filter-ip)# udp port 9000 to 9500
```

- To enable logs by destination IPv6 address using the Firewall logging template, use the following commands:

```
ACOS(config)# fw template logging test
ACOS(config-logging)# enable-log-by-destination
```

```
ACOS(config-logging-filter)# tcp port 80
ACOS(config-logging-filter)# udp port 7000
ACOS(config-logging-filter)# icmp
ACOS(config-logging-filter)# ip6 2001:db8::/32
ACOS(config-logging-filter-ip6)# udp port 5876
ACOS(config-logging-filter-ip6)# tcp port 90
```

- To disable the logging of TCP port and UDP port using the Firewall logging template, use the following commands:

```
ACOS(config)# fw template logging temp
ACOS(config-logging)#disable-log-by-destination
ACOS(config-logging-filter)# tcp port 10000 to 20000
ACOS(config-logging-filter)# udp port 1 to 65535
```

- To disable the logs by destination IPv4 address using the Firewall logging template, use the following commands:

```
ACOS(config)# fw template logging test
ACOS(config-logging)# disable-log-by-destination
ACOS(config-logging-filter)# udp port 8000
ACOS(config-logging-filter)# icmp
ACOS(config-logging-filter)# 10.2.3.0/24
ACOS(config-logging-filter-ip)# tcp port 90
ACOS(config-logging-filter-ip)# udp port 8000 to 8500
```

- To disable logs by destination IPv6 address using the Firewall logging template, use the following commands

```
ACOS(config)# fw template logging test
ACOS(config-logging)# disable-log-by-destination
ACOS(config-logging-filter)# tcp port 80
ACOS(config-logging-filter)# udp port 7000
ACOS(config-logging-filter)# icmp
ACOS(config-logging-filter)# ip6 2001:db8::/32
ACOS(config-logging-filter-ip6)# udp port 5876
ACOS(config-logging-filter-ip6)# tcp port 90
```

See Also:

- Traffic Logging Guide
- Command Line Interface Reference

Forward Zero UDP Checksum Without Recalculation

ACOS is enhanced to forward IPv4 UDP data packets having zero checksum without recalculating the checksum (See RFC 8085). This feature is applicable for any ADC, CGN, and Firewall setup, and can be enabled at the global level.

This can be implemented in the scenario where high-speed networks and real-time applications are used (that use UDP). In this case, the validation of zero UDP checksum is unnecessary. The change ensures that while receiving IPv4 UDP packets with zero checksum, ACOS does not recalculate the checksum. .

CLI Configuration

To forward IPv4 UDP packets with zero checksum without recalculation, use the following command:

```
ACOS(config)# system udp skip-checksum-when-zero
```

NOTE: This command is only applicable for the shared partition and takes effect on the entire system including shared and network partition.

See Also:

- IPv4-to-IPv6 Transition Solutions Guide
- Command Line Interface Reference

MIB

ACOS 6.0.8 introduces the following new features and enhancements for SNMP MIB:

The following topic is covered:

SNMP Support for IPSec Tunnel Interfaces

ACOS extends SNMP monitoring support to IPSec tunnel interfaces. The tunnel interfaces are added to the following SNMP MIB tables:

- A10-AX-MIB::axInterface
- A10-AX-MIB::axInterfaceStat
- ifXTable

SNMP polled data matches the output of the **`show interfaces tunnel`** command. This enhancement is available across all Thunder platform variants.

Limitation

The following SNMP MIB table fields do not populate tunnel interfaces because they are primarily designed for physical interfaces:

- axInterfaceMediaMaxDuplex
- axInterfaceMediaActiveDuplex
- axInterfaceStatMcastIn/Out
- axInterfaceStatDropsIn/Out
- axInterfaceStatCollisions
- axInterfaceStatUtilPercentIn/Out

See Also:

- IP Security Configuration Guide
- Command Line Interface Reference

SNMP Support for IP Anomaly Drop Statistics

ACOS has enhanced SNMP monitoring of IP anomaly drop statistics with a new CM subagent. This enhancement replaces the deprecated a10cmsubagent OID (1.3.6.1.4.1.22610.24.10.55.5.1) for IP anomaly drop statistics and introduces new OIDs for more accurate data representation.

SNMP polled data matches the output of the **`show ip anomaly-drop statistics`** command.

The following SNMP OIDs are introduced to support polling of IP anomaly drop statistics:

- anomalyDropStatsSlotId (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.1)
- anomalyDropStatsLand (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.2)
- anomalyDropStatsEmpFrg (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.3)
- anomalyDropStatsEmpMicFrg (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.4)
- anomalyDropStatsOpt (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.5)
- anomalyDropStatsFrg (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.6)
- anomalyDropStatsBadIpHdrlen (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.7)
- anomalyDropStatsBadIpFlg (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.8)
- anomalyDropStatsBadIpTtl (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.9)
- anomalyDropStatsNoIpPayload (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.10)
- anomalyDropStatsOverIpPayload (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.11)
- anomalyDropStatsBadIpPayloadLen (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.12)
- anomalyDropStatsBadIpFrgOffset (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.13)
- anomalyDropStatsCsum (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.14)
- anomalyDropStatsPod (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.15)
- anomalyDropStatsBadTcpUrgOffset (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.16)
- anomalyDropStatsTcpShtHdr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.17)
- anomalyDropStatsTcpBadIplen (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.18)
- anomalyDropStatsTcpNullFrg (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.19
- anomalyDropStatsTcpNullScan (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.20
- anomalyDropStatsTcpSynFin (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.21)
- anomalyDropStatsTcpXmas (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.22)
- anomalyDropStatsTcpXmasScan (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.23)
- anomalyDropStatsTcpSynFrg (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.24)

- anomalyDropStatsTcpFrgHdr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.25)
- anomalyDropStatsTcpBadCsum (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.26)
- anomalyDropStatsUdpSrtHdr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.27)
- anomalyDropStatsUdpBadLen (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.28)
- anomalyDropStatsUdpKerbFrg (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.29)
- anomalyDropStatsUdpPortLb (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.30)
- anomalyDropStatsUdpBadCsum (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.31)
- anomalyDropStatsRuntIpHdr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.32)
- anomalyDropStatsRuntTcpUdpHdr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.33)
- anomalyDropStatsIpipTnlMsmtch (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.34)
- anomalyDropStatsTcpOptErr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.35)
- anomalyDropStatsIpipTnlErr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.36)
- anomalyDropStatsVxlanErr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.37)
- anomalyDropStatsNvgreErr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.38)
- anomalyDropStatsGrePptpErr (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.39)
- anomalyDropStatsIpv6EhHbh (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.40)
- anomalyDropStatsIpv6EhDest (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.41)
- anomalyDropStatsIpv6EhRouting (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.42)
- anomalyDropStatsIpv6EhFrag (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.43)
- anomalyDropStatsIpv6EhAh (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.44)
- anomalyDropStatsIpv6EhEsp (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.45)
- anomalyDropStatsIpv6EhMobility (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.46)
- anomalyDropStatsIpv6EhNone (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.47)
- anomalyDropStatsIpv6EhOther (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.48)
- anomalyDropStatsIpv6EhMalformed (1.3.6.1.4.1.22610.2.4.8.140.1.1.1.49)

CLI Configuration

To allow SNMP monitoring for IP anomaly drop statistics, enable the new CM subagent:

```
ACOS(config)# snmp-server enable schema-agent
```

See Also:

- SNMP MIB Reference
- DDoS Mitigation Guide (For ADC)
- Command Line Interface Reference

Platforms & Licensing

ACOS 6.0.7 introduces the following new features and enhancements for ACOS Platforms and Licenses:

The following topics are covered:

Duo MFA Support for ACOS Upgrades using SCP

ACOS supports integrating Duo Multi-Factor Authentication (MFA) for ACOS upgrades using SCP. As a two-factor authentication (2FA) application, Duo enhances security by enforcing an additional authentication factor for SSH and SCP sessions. Once you enter the password, you must authenticate via the Duo mobile app to proceed with upgrade.

This release only supports Cisco Duo MFA for SCP-based upgrades across all A10 products running ACOS.

With this enhancement, ACOS detects when a Duo Unix-enabled server requires an additional authentication factor and prompts you to authenticate using one of the following options:

- Direct Passcode: Enter the 6-digit passcode generated in the Duo mobile app.
- Duo Push Notification: Approve the login request in the Duo mobile app.

- SMS Passcode: Enter the passcode received via SMS on the registered phone number.

NOTE: Some authentication methods may not be available depending on the Duo configuration of the remote server.

CLI Example

In the following example, ACOS prompts you for authentication during an image upgrade and you can directly enter the passcode from the Duo app or select either a push notification or SMS passcode option.

```
ACOS(config)# upgrade hd pri use-mgmt-port scp://root@path_to_ACOS_
image.upg
Password []?
Do you want to reboot the system after the upgrade?[yes/no]: no
Getting upgrade package ...
Duo two-factor login for root
Enter a passcode or select one of these options:
1. Duo Push to XXX-XXX-6097
2. SMS passcodes to XXX-XXX-6097

Passcode or option (1-2): 607527
```

If you enter the correct passcode from the Duo app, approve the Duo push notification, or enter the correct SMS passcode, the system displays 'Authentication successful!' message and proceeds with the upgrade.

See Also:

- Upgrade Instructions
- System Configuration and Administration Guide
- Command Line Interface Reference

Enhanced Capacity Flexpool License for Hardware Appliances

ACOS 6.0.7 introduces Capacity Flex Pool license support for additional Thunder Series devices through A10 Control. This enhancement enables dynamic bandwidth allocation, optimizing resource utilization based on licensing requirements.

The following table outlines the minimum and maximum bandwidth (BW) limits required for these platforms:

Table 1 : Capacity Flex Pool License Support

Platform	Minimum BW	Maximum BW
Thunder 1060S	10G	40G
Thunder 3350S	40G	70G
Thunder 5960	100G	300G

To improve Capacity Flex Pool licensing, the registration process with A10 Control now includes the following system details in the axAPI payload. ACOS now sends these details to A10 Control during device registration:

- Max CPUs
- Control CPUs
- Current CPUs
- Minimum Bandwidth

See Also:

- Capacity Flex Pool Licensing Guide
- Release Notes
- A10 Control User Guide

Support for Multi-PU Integration with A10 Control

ACOS supports multi-PU integration with A10 Control to manage and segment device features and analytics across Processing Units (PUs). This enables each PU to independently export the data of metrics, logs, audits, and syslogs into A10 Control.

See Also

- A10 Control User Guide

Scaleout

ACOS 6.0.7 introduces the following new feature and enhancement for Scaleout:

The following topic is covered:

Added Hairpin Traffic Support in Scaleout

ACOS has added support for hairpin traffic between subscribers placed in CGNAT or Firewall Scaleout or Multi-PU deployments. Router redirection is introduced as a unified solution for seamless Scaleout hairpin and Multi-PU hairpin traffic.

This feature introduces the following changes:

- Router Redirection: Harpin traffic between two clients can be first redirected to an external router using the next-hop-follow behavior for IPv4 and IPv6 networks and then directed to the appropriate PU (Multi-PU)/node (Scaleout).
- Bypass Unicast Reverse Path Forwarding (URPF): In cases where the `fw urpf strict` command is configured, the `skip-urpf-check` option is introduced in firewall rules to bypass URPF checks for specific rules.
- Supported Deployment: This enhancement supports hairpin traffic in the following deployments:
  - CGN-to-FW
  - FW-to-CGN
  - FW-to-FW

CLI Configuration

- To configure firewall hairpin for redirecting the traffic to router, use the following command:

```
ACOS(config)# fw hairpin next-hop-follow {IPV4 network | IPV6 network}
```

- To allow a specific firewall rule to skip URPF checks when the fw urpf strict command is configured, use the following command:

```
ACOS(config)#rule-set hairpin_cgn
ACOS(config-rule set:hairpin_cgn)#rule cgn-to-fw
ACOS(config-rule set:hairpin_cgn-rule:cgn-to-fw)#action-group
ACOS(config-rule set:hairpin_cgn-rule:cgn-to-fw-action-gr..)#permit
skip-urpf-check
```

See Also:

- Scaleout Configuration Guide
- Firewall Configuation Guide
- IPv4-to-IPv6 Transition Solutions Guide
- Command Line Interface Reference

Threat Protection System

ACOS 6.0.7 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to DDoS Mitigation Guide. Similarly, for TPS-related CLI commands, refer to DDoS Command Line Reference Guide.

Security Updates

The following security vulnerabilities are addressed in this release:

OpenSSL Vulnerability

- CVE-2024-3596: The vulnerability in RADIUS protocol (RFC 2865) is susceptible to forgery attacks by a local attacker who can forge an authentication response in cases where a Message-Authenticator attribute is not required or enforced. This issue arises from a cryptographically insecure integrity check using MD5, enabling attackers to spoof UDP-based RADIUS response packets

A10 Vulnerability

- A10-2024-0011: A vulnerability on port 41216 exposes weak ciphers on the A10 management IP when VCS is enabled. This port is used for configuration synchronization between vMaster and vBlade. This is resolved in 4.1.4-GR1-P14-SP1.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.6

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.6 release:

The following topics are covered:

Application Delivery Controller

ACOS 6.0.6 introduces the following new features and enhancements for Application Delivery Controller (ADC):

The following topics are covered:

NXDOMAIN Response Rate Limiting

ACOS introduces enhanced protection against DNS water torture DDoS attacks. This attack overwhelms a DNS server with requests for non-existent domains

(NXDOMAIN) which disrupt the server's ability to process legitimate requests.

To mitigate such attacks, NXDOMAIN Response Rate Limiting has been implemented. This enhancement enables you to manage NXDOMAIN traffic both at the virtual port level and for individual clients when needed.

The following are the implementation details:

- Per Virtual Port Rate-Limiting:

  At the SLB DNS Template level, a global rate is configured per virtual port. The system does not begin tracking individual clients until the traffic exceeds this global **`filter-response-rate`** limit. This mechanism provides an initial layer of protection against high query volumes.

- LID-Specific and Template-Level Rate-Limiting:

  When the traffic exceeds the **`filter-response-rate`** limit, the individual client tracking begins and the system applies the configured NXDOMAIN response rates as follows:

  - DNS RRL class-list LID Rate: If the client matches a configured LID (Local Identifier), the new rate limit defined in the LID is applied.
  - SLB DNS Template Rate: If the client does not match a configured LID, the new rate defined in the SLB DNS Template is enforced.

    Additionally, the **`response-rate`** limit range under the DNS RRL class-list has been increased from **`<1-1000>`** to **`<0-16000000>`** responses per configured window, where a value of 0 indicates unlimited responses with no restrictions on the response rate.

Supported Features

- Shared and Private L3V partitions.
- DNS Recursive Resolver and Backend server.
- DNS over UDP (dns-udp), DNS over TCP (dns-tcp), DNS over TLS (dot), and DNS over HTTP/HTTPS (doh) virtual ports.

CLI Configuration

A new **`nx-response-rate`** command is introduced to configure NXDOMAIN rate limit.

- To configure NXDOMAIN response rate limiting at the SLB DNS template per virtual port level, use the following command:

```
ACOS(config)# slb template dns template_name
ACOS(config-dns-response-rate-limiting)# response-rate-limiting
ACOS(config-dns-response-rate-limiting)# nx-response-rate num
```

- To configure NXDOMAIN response rate limiting at DNS RRL class-list LID level, use the following command:

```
ACOS(config)# class-list class-list-name dns
ACOS(config-class list)# dns contains class-list-name lid num
...
...
ACOS(config-dns-response-rate-limiting)# rrl-class-list class-list-
name
ACOS(config-dns-response-rate-limiting-rr...)# lid num
ACOS(config-dns-response-rate-limiting-rr...)# nx-response-rate num
```

A new **source-entry age** command is added at partition-level to manage resource allocation for DNS RRL. This configuration controls NXDOMAIN response rate-limiting without exhausting system resources.
To configure the source-entry age, use the following command:

```
ACOS(config)# slb common
ACOS(config-common)# dns-response-rate-limiting
ACOS(config-common-dns-response-rate-limi...)# source-entry-age num
```

Show command

To view the new T2 counters for NXDOMAIN response rate limiting, use the **show slb virtual-server** *virtual_server_name vport* **dns-udp application-statistics** command.

Limitation

- This feature does not support truncated responses or partial allowance through slip rates. Excess responses are strictly dropped.
- Under heavy traffic conditions, the system is likely to monitor individual clients before they reach the configured filter-response-rate, impacting both NXDOMAIN Rate Limiting and Queries Per Second (QPS).

See Also:

- DDoS Mitigation Guide (for ADC)
- Command Line Interface Reference

Enhanced SNMP Monitoring for DNS Cache

ACOS has enhanced SNMP monitoring for DNS Cache performance. You can view or monitor additional counters such as, DNS Queries Per Second (QPS), DNS cache hit rate, and cache hit ratio in CLI and SNMP.

This feature supports enhanced monitoring capabilities by gaining real time performance insight and resource optimization.

SNMP OID

The following new object IDs (OID) have been added to this release to monitor DNS performance metrics. These OIDs are operational only when the DNS cache is enabled.

SNMP OID	Description
1.3.6.1.4.1.22610.2.4.8.352.1.1.1.25	Tracks DNS cache QPS (Queries Per Second).
1.3.6.1.4.1.22610.2.4.8.352.1.1.1.26	Tracks DNS cache hit rate per second.
1.3.6.1.4.1.22610.2.4.8.352.1.2.1.24	Tracks DNS cache hit ratio percentage per second.

NOTE: The command **`snmp-server enable schema-agent`** is essential for SNMP to poll any OIDs within the range of 1.3.6.1.4.1.22610.2.4.8.

CLI Configuration

To enable the CM schema agent, use the following command:

```
ACOS(config)#snmp-server enable schema-agent
```

Show command

The following example shows the response of the show dns cache rate command:

```
ACOS(config)# show dns cache rate
```

```
Query   rate(QPS)    : 50   per   second
Cache   hit       : 48   per   second
Cache   hit   ratio   : 96%   (cache   hit/Query)
```

Limitations

- For multi-PU platforms, the cache hit ratio counter may not function as expected.
- QPS, cache-hit rate and cache hit ratio values displayed in aXAPI/SNMP and CLI will be different or may not match with each other.
- All the counters in the SNMP table (dnsCacheOperTable) are currently not supported, except the cache hit ratio. Use appropriate filter in the aXAPI to retrieve the specific details.

See Also:

- Application Delivery Controller Guide
- Command Line Interface Reference
- SNMP MIB Reference

Application Delivery Partitions

ACOS 6.0.6 introduces the following new features and enhancements for Application Delivery Partitions (ADP):

The following topics are covered:

Partition Admin Command For L3V Partitions

User accounts for L3V partitions can now be created using the **partition-admin** command, which ensures that the created partition-admin user remains valid even if the creator admin user is removed. This enhancement adds reliability to partition user management.

Partition Admin Command Features:

- The L3V partition is automatically assigned to the user upon creation.
- Users can be granted the privileges **partition-read**, **partition-write**, and **partition-enable-disable**, with **partition-read** being the default privilege.
- The **partition-admin** command is supported only for L3V partitions; service partitions are not supported.
- A partition admin user cannot modify L3V users created using the **admin** command.
- A partition admin user cannot create another user with same name as the system admin or a user in other partition.
- After logging into a partition-admin account, executing the **show admin** command displays only the users of that partition. For example, if you log in as p3-user (under partition p3), you will only see the users of partition p3.

NOTE: The **admin** command can only perform the following actions on partition-admin users: **disable/enable**, **delete**, and **lock/unlock**. For any other changes, the system administrator needs to switch to the corresponding partition and make modifications.

CLI Configuration

The following commands create a partition admin user *user1* with password *1234* in the partition *P1*:

```
ACOS[P1](config)# partition-adminuser1
ACOS[P1](config-partition-admin:user1)# password1234
```

See Also:

- Application Delivery Partition Guide
- Command Line Interface Reference

aFleX

ACOS 6.0.6 introduces the following new features and enhancements for aFleX.

NOTE: For more information, refer *aFleX Scripting Language Reference*.

The following topics are covered:

Increased Maximum File Size of aFlex Script

The maximum supported file size for aFleX scripts on ACOS devices has been increased from 256KB to 1024KB(1MB).

Additionally, a new counter **exceed-time-limit** has been introduced to ensure that aFleX scripts do not run indefinitely or consume excessive system resources. When an aFleX script exceeds its designated execution time, the system aborts its execution, and this counter is incremented.

CLI Configuration

To configure the maximum supported file size for aFleX script, use the following command:

```
ACOS(config)# system resource-usage max-aflex-file-size 1024
```

Show Command

To view the exceed-time-limit counter value, use the following commands:

- **show aflex <script_name>**
- **show techsupport | include exceed_time_limits**

See Also:

- aFleX Scripting Language Reference Guide
- Command Line Interface Reference

Carrier Grade NAT

ACOS 6.0.6 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

The following topics are covered:

Support for Logging by Control CPU

ACOS has introduced a 'logging by control CPU' logging mechanism alongside the existing 'logging by data CPU.'

In the earlier mechanism, ACOS generated a large number of ‘user quotas-exceeded’ or ‘ports unavailable’ logs per CPU per NAT pool when CGN user-quotas and ports were exhausted due to high traffic, leading to the overwhelming volume of logs.

The 'logging by control CPU' mechanism provides the following benefits:

- Generate logs based on the NAT pool.
- Consolidate data for the same NAT pool.
- Generate a single log message for each type of error.

This feature reduces the overall volume of CGN logs, making it easier to analyze and troubleshoot issues while improving system efficiency and scalability.

A new option `cgnv6 logging pool-based-log` has been introduced, which logs the following log types and attributes:

Log Types	Supported Attributes
USER_QUOTA_ICMP_EXCEEDED	Session exceeding logs
USER_QUOTA_UDP_EXCEEDED	
USER_QUOTA_TCP_EXCEEDED	
USER_QUOTA_ESP_EXCEEDED	
EXT_USER_QUOTA_UDP_EXCEEDED	
EXT_USER_QUOTA_TCP_EXCEEDED	
SESSION_QUOTA_EXCEEDED	
NEW_USER_RESOURCE_UNAVAILABLE	Resource Unavailable Logs

Log Types	Supported Attributes
ICMP_NAT_PORT_UNAVAILABLE	NAT Port Unavailable Logs
UDP_NAT_PORT_UNAVAILABLE	
TCP_NAT_PORT_UNAVAILABLE	
FULLCONE_CREATION_FAILED	Creation Failed Logs
USER_QUOTA_CREATION_FAILED	

CLI Configuration

To generate logs based on the NAT pool, use the following command:

```
ACOS(config)# cgnv6 logging pool-based-log cycle <0-1800>
```

This command is only available in the shared partition. Once enabled, it is effective for all NAT pools in all shared and L3V partitions. The logs for L3V partitions will still be logged to their partition.

NOTE: By default, this option is enabled and set to `30` when you upgrade to ACOS 6.0.6. If you want to return to the original behavior (logging by data CPU), then set the `cgnv6 logging pool-based-log cycle` to `0`.

See Also:

- Traffic Logging Guide
- Command Line Interface Reference

Enhancement to CGN Custom Logging Timestamp

The CGN custom logging format now includes three-letter month information in the log timestamp. The default format is `%Y%m%d%H%M%S`. A new configuration option `%o` is introduced to display three-letter month information in the format: `<%Y> <%o> <%d> <%H:%M:%S>`.

NOTE: You can use the new option (`%o`) to configure the timestamp format to display in the three-letter alphabetical month. OR use the option (`%m`) to display the timestamp numerically.

The mapping between the numerical months and their corresponding three-letter month information is as follows:

Numericals	Month
1	Jan
2	Feb
3	Mar
4	Apr
5	May
6	Jun
7	Jul
8	Aug
9	Sep
10	Oct
11	Nov
12	Dec

CLI Configuration

To include three-letter month information in the timestamp, use the following commands:

```
ACOS(config)# cgnv6 template logging cgn_logging
ACOS(config-logging:cgn_logging)# log sessions
ACOS(config-logging:cgn_logging)# format custom
ACOS(config-logging:cgn_logging)# service-group syslog1
```

```
ACOS(config-logging:cgn_logging)# custom message session-created
"Notice: Creating session proto=$proto-name$ rule name=$rule-name$
[$fwd-tunnel$ $fwd-src-ip$ $fwd-dst-ip$]"
ACOS(config-logging:cgn_logging)# custom message session-deleted
"Notice: Deleting session which started at $sesn-start-time$: client
IP=$fwd-src-ip$, session duration=$sesn-dur$, rule name=$rule-name$,
$sesn-start-time$, $sesn-dur$"
ACOS(config-logging:cgn_logging)# custom time-stamp-format "<%Y> <%o>
<%d> <%H:%M:%S>"
```

Log Example

The following is a syslog sample that displays the three-letter month information in the timestamp:

```
25.190765    20.1.1.21 -> 20.1.1.1     Syslog Notice: Deleting session
which started at <2024> <Oct> <21> <08:03:46>: client IP=10.1.1.1,
session duration=27795, rule name=r1, <2024> <Oct> <21> <08:03:46>,
27795Notice: Deleting session which started at <2024> <Oct> <21>
<08:03:48>: client IP=10.1.1.1, session duration=25819, rule name=r1,
<2024> <Oct> <21> <08:03:48>, 25819Notice: Deleting session which
started at <2024> <Oct> <21> <08:03:22>: client IP=10.1.1.1, session
duration=51907, rule name=r1, <2024> <Oct> <21> <08:03:22>, 51907Notice:
Deleting session which started at <2024> <Oct> <21> <08:03:36>: client
IP=10.1.1.1, session duration=37953, rule name=r1, <2024> <Oct> <21>
<08:03:36>, 37953Notice: Deleting session which started at <2024> <Oct>
<21> <08:03:28>: client IP=10.1.1.1, session duration=45967, rule
name=r1, <2024> <Oct> <21> <08:03:28>, 45967Notice: Deleting session
which started at <2024> <Oct> <21> <08:03:44>: client IP=10.1.1.1,
session duration=30012, rule name=r1, <2024> <Oct> <21> <08:03:44>,
30012Notice: Deleting session which started at <2024> <Oct> <21>
<08:03:14>: client IP=10.1.1.1, session duration=60159, rule name=r1,
<2024> <Oct> <21> <08:03:14>, 60159
```

See Also:

- Traffic Logging Guide
- Command Line Interface Reference

Enhancement to User Quota Value

ACOS has added the ability to configure reserve limits for TCP and UDP user-quota sessions separately. The TCP and UDP sessions can each have their separate user-quota and remain usable even during any flood attacks.

This feature ensures that a reserve value is always configured.

CLI Configuration

- To configure user quota for TCP sessions, use the following commands:

```
ACOS(config)# cgnv6 lsn-lid 1
ACOS(config-lsn-lid)# user-quota session-tcp <1-2147483647>
```

- To configure user quota for UDP sessions, use the following commands:

```
ACOS(config)# cgnv6 lsn-lid 1
ACOS(config-lsn-lid)# user-quota session-tcp <1-2147483647>
```

If you configure `user-quota tcp <value>` or `user-quota udp <value>` without configuring `reserve`, ACOS accepts the configuration and displays a warning message as - `Configuration accepted. Applying the configured value to quota 'reserve' as the default setting.`

This indicates that the `reserve` value is not zero but has a default value.

Show Commands

The following show commands are enhanced to display the number of TCP sessions and UDP sessions:

- `show cgnv6 lsn user-quota-session`
- `show cgnv6 lsn enhanced-user-tracking`
- `show cgnv6 nat64 user-quota-session`
- `show cgnv6 nat64 enhanced-user-tracking`
- `show cgnv6 ds-lite user-quota-sessions`

See Also:

- IPv4-to-IPv6 Transition Solutions Guide
- Command Line Interface Reference

Firewall

ACOS 6.0.6 introduces the following new features and enhancements for Firewall:

The following topics are covered:

SYN cookie Protection Per Firewall Rule

ACOS has enhanced the Firewall rule-set by adding the ability to configure the SYN cookie feature per firewall rule. With this change, SYN cookie protection can now be applied to specific components of the traffic along with the global firewall traffic.

Within a firewall rule, the SYN cookie threshold prevents TCP half-open sessions matching the rule from being created. This configuration protects the system from SYN flood attacks, provides security, and offers more flexible and adaptive firewall policies. After the specified timeout, the SYN cookie protection is disabled.

The feature also helps improve the performance for unaffected traffic.

NOTE: The per-rule configuration overrides the global configurations of the **`fw tcp syn-cookie`** and **`cgnv6 ddos-protection syn-cookie`** commands.

Supported deployments:

- Firewall
- Firewall+CGN

CLI Configuration

To configure SYN cookie protection per firewall rule, including the threshold for TCP

half open connections and a timeout, use the following commands:

```
ACOS(config)#rule-set rs1
ACOS(config-rule set:rs1)#rule 2
ACOS(config-rule set:rs1-rule:2)#action-group
ACOS(config-rule set:rs1-rule:2-action-group)#permit tcp syn-cookie
[enable | disable] tcp-half-open on-threshold <number> on-timeout
<number>
```

Show Commands

The following show commands are enhanced with additional counters for this feature:

- To view the half-open sessions counter per rule, use the **show counters rule-set <rule-set> rule <rule>** command.
- To view the statistics related to TCP SYN cookies, use the **show fw tcp syn-cookie statistics** command.
- To view TCP SYN cookie status and related information, use the **show rule-set <rule-set> rule-name <rule>** command.
- To display the statistics for CGN DDoS selective filtering, use the **show cgnv6 ddos-protection statistics** command.

Limitations

- The **fw allow-non-syn-session-create** command cannot be configured if SYN cookie protection is enabled either per rule or at the global level.
- This feature only supports CGN and Firewall; it is not supported for ADC.

See Also:

- Firewall Configuration Guide
- Command Line Interface Reference

Increased Maximum Rate-Limit Value for Throughput

The Firewall template limit-policy is enhanced with the ability to configure the throughput threshold limit in Gigabits (Gbps) per second. The maximum rate-limit

value for throughput is increased from 100000 Mbps to 10 Tbps. The change is applicable for downlink, uplink, and total traffic.

The increased threshold ensures that more traffic can pass through before applying rate-limiting and is particularly useful in case of larger number of users or higher traffic rates.

The burst size can also be specified as a unit in Mbps (default), Kbps, or Gbps.

CLI Configuration

To configure the throughput rate-limit on the uplink, downlink, and total traffic in Gbps, use the following commands:

```
ACOS(config)#template limit-policy 123
ACOS(config-limit-policy)#limit-scope subscriber-prefix 25
aaACOS(config-limit-policy)#limit-throughput downlink 20 Gbps
ACOS(config-limit-policy)#limit-throughput uplink 30 GKbps burstsize 31
Gbps
ACOS(config-limit-policy)#limit-throughput total 60 Gbps
```

Show Command

The **show fw rate-limit** command is enhanced to display the value in Gbps if the Total-Received value is suitably represented in Gbps.

See Also:

- Firewall Configuration Guide
- Command Line Interface Reference

Enhanced Custom Logging in CGN and Firewall

The Custom logging format for CGN and Firewall is enhanced with additional logging attributed to improve the overall log efficiency and provide detailed insight.

The following logging attributes are implemented:

- In Firewall custom logging, new attributes such as timestamp, source zone (src-zone), destination zone (dest-zone), application ID (app-id), and RADIUS attributes

are added for session-created and session-deleted events.

These additional fields are supported in the `[custom string]` section of Firewall logging templates.

- In CGN custom logging, session start time and delete time are now logged in epoch milliseconds (instead of plain text).

CLI Configuration

In a Firewall deployment, the following highlighted keywords can be configured in the custom log format for the following:

- session-created event:

```
ACOS(config)#fw template logging temp1
ACOS(config-logging)#format custom
ACOS(config-logging)#custom message session-created FW_SESSION_
CREATED,$sesn-start-time-epoch$,$time-stamp$,$src-zone$,$dest-
zone$,$app-id$,$radius-msisdn$,$radius-imei$,$radius-imsi$,$radius-
ctm1$,$radius-ctm2$,$radius-ctm3$,$radius-ctm4$,$radius-ctm5$,$radius-
ctm6$
```

- session-deleted event:

```
ACOS(config)#fw template logging temp1
ACOS(config-logging)#format custom
ACOS(config-logging)#custom message session-deleted FW_SESSION_
DELETED,$sesn-start-time-epoch$,$sesn-end-time$,$sesn-end-time-
epoch$,$time-stamp$,$src-zone$,$dest-zone$,$app-id$,$radius-
msisdn$,$radius-imei$,$radius-imsi$,$radius-ctm1$,$radius-ctm2$,$radius-
ctm3$, $radius-ctm4$,$radius-ctm5$,$radius-ctm6$
```

In the CGN deployment, the following highlighted keywords can be configured in the custom log format for the following:

- session-created event:

```
ACOS(config)#cgnv6 template logging temp1
ACOS(config-logging)#format custom
ACOS(config-logging)#custom message session-created FW_SESSION_
CREATED,$sesn-start-time-epoch$
```

- session-deleted event:

```
ACOS(config)#cgnv6 template logging temp1
ACOS(config-logging)#format custom
ACOS(config-logging)#custom message session-deleted FW_SESSION_
DELETED,$sesn-start-time-epoch$,$sesn-end-time$,$sesn-end-time-epoch$
```

Show Commands

The following show commands are added or enhanced:

- In Firewall deployment: To view the logging keywords for session-created and session-deleted events, the **`show fw logging-keywords [session-created | session-deleted]`** command is added.
- In CGN deployment: To view the logging keywords for session-created and session-deleted events, the **`show cgnv6 logging keywords [session-created | session-deleted]`** command is enhanced.

See Also:

- Firewall Configuration Guide
- Command Line Interface Reference

A10 Defend Threat Intelligence Integration

The A10 CGN/Firewall policy model has been enhanced to leverage the threat intelligence capabilities of A10 Defend.

A10 Defend offers IP Blocklists (both predefined and customized), which identify malicious IP addresses originating from suspicious sources. These blocklists can be imported from the A10 Defend site to the ACOS device as class-lists, which can then be used to create IP threat lists. The Firewall employs these threat lists to detect malicious sources and drop the traffic associated with such IP addresses, thereby protecting against cyberattacks. This integration thus helps safeguard both subscribers and ACOS devices from various attacks.

The IP blocklists are available in two formats: Plain IP List and STIX 2.1, both of which are supported in ACOS for importing. However, it is recommended to download the list in STIX 2.1 format, since it has a structured format with rich metadata that provides more threat intelligence information.

CLI Configuration

- To import an A10 Defend IP blocklist in ACOS, obtain the download URL from A10 Defend site, and then execute the following command:
  - For STIX 2.1 format:

```
ACOS(config)# import class-list<class-list-name>use-mgmt-port<IP_
Blocklist_UR
```

    Example command:

```
ACOS(config)# import class-list A10blocklist use-mgmt-
porthttps://defend.a10networks.com/tenant/2/api/v1/threat-
lists/generate/direct-download/A10-Block-Reflectors-Critical-
10K/%3Fcountry=all%26format=ipv4networkhost%26file_format=stix-2-1
```

  - For Plain IP List format:

```
ACOS(config)# import class-list-convert <class-list-name> class-list-
type ipv4 use-mgmt-port <URL>
```

    Example command:

```
ACOS(config)# import class-list-convert A10blocklist class-list-type
ipv4 use-mgmt-port
https://defend.a10networks.com/tenant/2/api/v1/threat-
lists/generate/direct-download/A10-Block-Reflectors-Critical-
10K/?country=all&format=ipv4networkhost&file_format=plain-ip-list
```

NOTE:

- To obtain the URL, you must register on the A10 Defend site and create an Auth User account (with a user ID and password).
- While setting the password for an Auth User, ensure it does not include any of the following special characters: `(blank space) %&'/:<>?@[\]`. These characters are not supported in ACOS while entering the password after executing the **import** or **import-periodic** command.
- After obtaining the URL, replace the characters '?' and '&' with '%3F' and '%26' respectively to ensure proper URL encoding.

- To create a threat-list, bind the imported blocklist (*A10blocklist*) to an IPv4 internet-host list by using the **system ip-threat-list** command. The following configuration demonstrates command usage:

```
ACOS(config)# system ip-threat-list
ACOS(config-ip-threat-list)# ipv4-internet-host-list
ACOS(config-ip-threat-list-ipv4-src)# white-list mywhitelist
ACOS(config-ip-threat-list-ipv4-src)# class-list A10blocklist
```

  The **white-list** option allows you to bind an exception list to the IPv4 internet host list. This exception list (*mywhitelist*) contains IP addresses that are exempted from blocking, i.e., traffic to or from these IPs is always allowed, even if they are included in the blocklist (*A10blocklist*).

NOTE:	You can bind the blocklist to an IPv4 source list, destination list, or internet host list. However, it is recommended to bind it to an IPv4 internet host list, as this list can track malicious IPs in both directions of the data plane.

Limitations

• A10 Defend currently provides only IPv4 threat intelligence information, so only IPv4 addresses are supported.

• If entries overlap across different threat lists, the first matched threat list is used.

• A maximum of 16 different threat-categories are supported, with category names limited to 50 characters.

See Also:

- Firewall Configuration Guide
- Command Line Interface Reference

Global Server Load Balancing

ACOS 6.0.6 introduces the following new features and enhancements forGlobal Server Load Balancing (GSLB).

The following topics are covered:

DNS Sticky Support for EDNS Client Subnet

The DNS sticky feature of GSLB policy has been enhanced to support EDNS client subnet (ECS).

When DNS sticky is combined with ECS, it provides the best sticky result based on ECS subnet information and ensures that future ECS queries are directed to the same IP address. This enhancement provides an additional security layer by selecting the same service IP/subnet.

CLI Configuration

To configure DNS sticky with ECS in GSLB policy, use the following command:

```
ACOS(config-policy:p1)#dns sticky-options
ACOS(config-policy:p1-sticky-options)#edns-client-subnet
ACOS(config-policy:p1-sticky-options)#edns-client-subnet only
```

Limitations

- GSLB service groups are not supported for sticky sessions.
- Local DNS (LDNS) and ECS subnet information rarely match, if they do the default match will align with the first session created.
- Sticky session matching with ECS requires an exact match irrespective of LDNS or ECS lookup.
- The existing sticky subnet mask configuration applies only to LDNS sessions and not to EDNS.

See Also:

- Global Server Load Balancing Guide
- Command Line Interface Reference

Increased the Maximum Limit of Service Matching Rules

ACOS has increased the maximum limit of GSLB service matching rules from 32 to 500 per GSLB zone.

This change allows you to add more conditions in the service matching rules as per the environment.

CLI Configuration

To configure the range of rule sequence numbers, use the following command:

```
ACOS(config)# gslb zone z1
ACOS(config)# gslb service-matching-rules zone z1
ACOS(config-service-matching-rules:z1)# rule <1-500>
```

See Also:

- Global Server Load Balancing Guide
- Command Line Interface Reference

Next Generation Web Application Firewall

ACOS 6.0.6 introduces the following new feature and enhancement for the Next Generation Web Application Firewall (NGWAF):

The following topic is covered:

Introduced NG-WAF Pool License

ACOS has introduced the Next-Gen Web App Firewall Pool license. It is a modular license that allocates a pool of bandwidth that can be shared between multiple Thunder and/or vThunder instances instead of being limited to individual devices.

The license works like a FlexPool license. It can be acquired, activated, assigned, managed, revoked, or unrevoked from the Global Licensing Manager (GLM) dashboard. It provides improved flexibility and offers a cost-effective solution as users do not need to overpay for unused bandwidth.

This license provides the following features:

- **Enables Bandwidth Sharing**

  The license creates a pool of bandwidth that can be applied to multiple Thunder and vThunder devices within the specified pool limit and activation limit. For example, a 20G NG-WAF pool license can be allocated as follows: 10G to a 10G vThunder and the remaining 10G to 10x 1G vThunders.

- **Provides Bandwidth in Gbps**

  The license allows bandwidth allocation in Gbps.

- **Overrides Product License Bandwidth**

  In case a device has both, the product license (ADC) and the NGWAF pool license, the license with the lower supported bandwidth overrides the other license.

- **Displays Activation and Usage Status on Fastly Dashboard**

  The Fastly dashboard displays the NG-WAF license's unique token ID, SKU bandwidth and the number of activations on the devices with their associated ADC bandwidth.

Show Commands

The following show commands have been enhanced:

- To view the NGWAF bandwidth and license token, use the `show license-info` command.
- To display details on the NGWAF server and license information updates, use the `show log` command.

See Also:

- Next-Gen WAF Configuration Guide
- Capacity Flex Pool Licensing Guide
- Global License Manager User Guide

SSL Insight

ACOS 6.0.4 introduces the following new feature and enhancement for SSL Insight (SSLi):

The following topic is covered:

Compatibility with Latest Web Category

The Web category bypass feature of the SSLi solution utilizes the BrightCloud Web Classification Service to determine which URLs should bypass SSLi decryption.

To enhance the web categorization compatibility with ACOS, the web category SDK (Software Development Kit) has been upgraded to version 4.40.1 from 4.40.

See Also:

- SSL Insight Configuration Guide

System Configuration and Administration

ACOS 6.0.6 introduces the following new features and enhancements for System Configuration and Administration:

NOTE: For more information and details, refer *System Configuration and Administration Guide*.

The following topics are covered:

ACL Per-Rule Hit Count for Management Interface

ACOS supports tracking hit counts for Access Control Lists (ACLs) applied to the management interface. This feature provides detailed insights into traffic flow by:

- Monitoring both permitted and denied traffic.
- Recording the total number of hits for each ACL rule.

- Evaluating the effectiveness and usage of ACL configurations.

The hit count is displayed for each ACL line in the `show access-list` command output.

Show Command

To view the hit count of the management interface, use the `show access-list` command:

```
ACOS# show access-list ipv4 50
Management hit count: 175
access-list 50 permit 198.162.12.0 0.0.0.255 Data plane hits:
0, Management plane hits: 175
```

Limitations

- The management hit count is only displayed when the ACL is bound to the management interface.
- If the ACL is unbound from the management interface, the management-related hit count is reset.
- On Thunder 8655, if an ACL is applied to the management interface using `enable-management` and `interface management/management2` commands, the last configuration takes effect and removes the first configuration.

See Also:

- System Configuration and Administration Guide
- Command Line Interface Reference

Detection of Configuration Consistency Across Multiple PUs

ACOS has added a functionality to monitor the synchronization status between PU1 and PU2 in a multi-PU environment, where Processing Unit 1 (PU1) acts as the primary PU and Processing Unit 2 (PU2) as the secondary PU.

Any configuration changes on PU1 are automatically propagated to PU2. However, issues such as no license, insufficient memory, and so on can cause configuration synchronization to fail between PU1 to PU2. This can result in a network outage and other unwanted effects.

To monitor the synchronization status of PU2 with PU1 periodically, a new command – `system config-mgmt pu-sync-detection` is introduced. This command allows you to enable, disable, or set the interval for detecting the status of configuration synchronization between PU1 and PU2.

You can also view inconsistency in the configuration and associated warning message using `show log` command.

NOTE:

- This command applies only to the multi-PU platform.
- By default, the detection is disabled. If enabled, it may affect the control place performance and CPU usage, especially if a large configuration is applied or too many partitions are configured.

CLI Configuration

- To enable or disable the detection of configuration synchronization between PU1 and PU2, use the following commands:

```
ACOS(config)# system config-mgmt pu-sync-detection
ACOS(config-pu-sync-detection)# enable | disable
```

- To set an interval to detect configuration synchronization between PU1 and PU2, use the following commands:

```
ACOS(config)# system config-mgmt pu-sync-detection
ACOS(config-pu-sync-detection)# interval <30-86400>
```

Show Command

To view the warning message on configurations that are not synchronized between PU1 and PU2, use the `show log` command:

```
Nov 27 2024 12:18:04 Info    [CFGMGR]: - PU1 - Partition 'shared' is in
sync now in PU2.
Nov 27 2024 12:17:04 Warning   [CFGMGR]: - PU1 - Partition 'shared' has
2 objects out of sync in PU2, including slb.server(s4,s5).
Nov 27 2024 12:11:45 Warning   [CFGMGR]: - PU1 - Partition 'shared' has
2 objects out of sync in PU2, including slb.server(s4,s5).
```

See Also:

- System Configuration and Administration Guide
- Command Line Interface Reference

Enhanced Trunk Interface Statistics

ACOS supports monitoring the statistics for L2 and L3 trunks based on incoming and outgoing packets. For the multi-PU platforms, the aggregated statistics from PU1 and PU2 are displayed on PU1, and the statistics related to PU2 only on PU2.

A new command `trunk-stats` has been introduced to enable the generation of statistics for trunk interfaces. You can use the `clear statistics interface trunk` command to clear the statistics.

NOTE: This command is available only in the shared partition.

CLI Configuration

To enable the statistics generation for the trunk interface, use the following command:

```
ACOS(config)# trunk-stats enable
```

Show Command

- To view the statistics of the trunk interface for L2 and L3 trunks, use the following command:

  ```
  ACOS(config)# show interfaces trunk
  ```

- To clear the statistics, use the following command:

  ```
  ACOS(config)# clear statistics interface trunk
  ```

Limitation

The interface trunk must be configured along with the trunk-group to view the interface statistics under the `show interface statistics` command.

See Also:

- Network Configuration Guide
- Command Line Interface Reference

Platforms

ACOS 6.0.6 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

Enhancement in Thunder 1060S

Thunder 1060S non-FTA platforms have been optimized to support:

- NGWAF deployments, and NGWAF Thunder devices deployed on Dell PowerEdge R760 servers.
- Flexible bandwidth 40 Gbps tiers through modular licensing, enabling scalable network capacity for ADC and CFW-ADC deployments.
- TPS deployment with modular bandwidth tiers (5, 10 and 20 Gbps) based on inbound traffic.

See Also:

- Next-Gen WAF Configuration Guide
- A10 TH1060S Installation Reference Guide
- Dell Documentation
- Global Licensing Manager Guide

Enhanced Thunder 5960 Platform

Thunder 5960 non-FTA devices have been optimized to support ADC (Layer 4 load balancing) deployments.

See Also:

- A10 TH5960 Installation Reference Guide
- Platform Support Information

Enhancement in vThunder on ESXi

vThunder on VMware ESXi 8.0 has been extended to support CFW, CGN, and TPS deployments. In the earlier releases, the support was limited to ADC and Gi-FW.

See Also:

- Installing vThunder on VMware ESXi

Security Updates

The following security vulnerabilities are addressed in this release:

OpenSSL Vulnerability

- CVE-2023-0464: The vulnerability is related to excessive resource usage for verifying X509 policy constraints resulting in a Denial of Service.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.5

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.5 release:

The following topics are covered:

Application Delivery Controller

ACOS 6.0.5 introduces the following new features and enhancements for Application Delivery Controller (ADC):

The following topics are covered:

Dependency Check to Prevent Referenced Objects Deletion

ACOS introduces a system-level enhancement to prevent accidental deletion of referenced SLB (Server Load Balancer) objects, thereby reducing the risk of unintended service interruptions.

In the earlier releases, ACOS provided super-deletion feature. When a user deleted an SLB template or object such as virtual servers, service groups, and real servers, all associated references were automatically deleted.

A new configuration **system config-mgmt delete-referenced-tagged-objects** is added, which will allow you to choose between automatic or manual deletion.

CLI Configuration

To prevent referenced object deletion, use the following command:

```
ACOS(config)# system config-mgmt delete-referenced-tagged-objects
disable
```

The following example demonstrates an attempt to delete a real server named 's1', which is referenced elsewhere in the system. The system blocks the deletion and prompts the user to remove those references first.

```
ACOS(config)# no slb server s1
This object has other objects referencing this. Please remove references
first.
```

See Also:

- Command Line Interface Reference
- System Configuration and Administration Guide
- Application Delivery Controller Guide

Enhanced DNS Logging with Response Code (RCODE) Information

The ACOS logging infrastructure has been enhanced to include the RCODE (response code) field in the SLB DNS response logs. RCODE is a numeric code in the DNS response that indicates the status of a DNS query, whether it was successful or if there was an error.

Additionally, you can customize the DNS logging to include specific parts of the DNS response, such as:

- all - To log DNS header, answer, authority, and additional section content.
- answer - To log DNS header, and answer section content.

- header – To log DNS header only.

This enhancement improves the SLB DNS monitoring, troubleshooting, and simplifies log analysis. This feature supports both CEF and Syslog formats.

CLI Configuration

To enable the response logging with RCODE, use the following command:

```
ACOS(config)#slb template dns-logging d1
ACOS(config-dns-logging)#response-include-rcode
ACOS(config-dns-logging)#response-section {all | header | answer}
```

Log Examples

CEF Example with response-section (ALL)

```
proto=UDP src=32.100.100.100 spt=60 dst=10.211.10.2 dpt=52050
cs1=Response cs1Label=Response cs2=backend cs2Label=Response Source
cn1=1207 cn1Label=Query ID cs3=Query cs3Label=Opcode cs4=RD|RA
cs4Label=Header Flag cs5=03 cs5Label=RCODE cn2=1 cn2Label=Question Count
cn3=0 cn3Label=Answer Record Count cn4=1 cn4Label=Authority Record Count
cn5=0 cn5Label=Additional Record Count cs6=Authority section SOA IN
10800 a.root-servers.net nstld.verisign-grs.com 2024072400 1800 900
604800 86400;] cs6Label=response content
```

Syslog Example with response-section (ALL)

```
UDP 32.100.100.100 60 10.211.10.2 36545 Type=Response source=backend
QueryId=13984 Opcode=Query HeaderFlag=AA|RD|RA RCODE=00 QDCount=1
ANCount=3 NSCount=2 ARCount=4 response=Answer section [www.example.com
CNAME IN 86400 services.example.com;services.example.com A IN 86400
10.212.2.21;services.example.com A IN 86400 10.212.2.20;] Authority
section [example.com NS IN 86400 dns1.example.com;example.com NS IN
86400 dns2.example.com;] Addition section [dns1.example.com A IN 86400
10.212.2.20;dns1.example.com AAAA IN 86400 aaaa:bbbb::1;dns2.example.com
A IN 86400 10.212.2.22;dns2.example.com AAAA IN 86400 aaaa:bbbb::2;]
```

Limitation

Not all the IANA-defined RCODEs are logged; only the RCODE in the DNS header is supported.

See Also:

- Application Delivery Controller Guide
- Command Line Interface Reference
- Event Logging Guide

Multi-Match Rules Enhancement

The SLB HTTP policy has been enhanced to increase the maximum number of multi-match rules from 64 to 1023.

The SLB HTTP template policy ensures efficient and reliable distribution of HTTP traffic across multiple servers. Administrator can configure this policy for directing requests to the most appropriate server based on the server selection criteria defined in the policy. Multi-match rules are configured based on factors such as URL, headers, and cookies, which are used to route traffic to the appropriate servers. With the increase in the maximum number of rules, a more granular server selection criteria can be defined for precise and efficient traffic routing.

This enhancement supports HTTP/1.1 and HTTP/2 protocols.

Limitation

Parameter matching is not supported under HTTP/1.1 protocol.

See Also:

- Command Line Interface Reference

ACOS Virtual Chassis System

ACOS 6.0.5 introduces the following new feature and enhancement for ACOS Virtual Chassis System (aVCS):

The following topic is covered:

VCS Image Upgrade Using SCP

ACOS supports the transmission of ACOS Virtual Chassis Systems (aVCS) upgrade image to the member nodes in an aVCS cluster using the Secure Copy Protocol (SCP). It supports all aVCS deployments such as multicast, unicast, IPv4, and IPv6.

A new `vcs offload upgrade protocol <scp>` command is introduced for transmitting the upgrade image. During the image upgrade process in an aVCS cluster, the image file is transmitted to the aVCS cluster member nodes using the SCP protocol. It ensures an efficient and reliable transmission, especially when transmitting large upgrade image files.

CLI Configuration

- To transmit the upgrade image using SCP, use the following command:

```
ACOS(config)# vcs offload upgrade protocol scp
```

NOTE: The SSH service must be enabled on the VCS interface port.

See Also:

- Command Line Interface Reference

Carrier Grade NAT

ACOS 6.0.5 introduces the following new feature and enhancement for Carrier Grade NAT (CGN or CGNAT):

The following topic is covered:

TCP MSS Clamping Enhancements

To enhance performance and reduce fragmentation, the TCP Maximum Segment Size (MSS) Clamping is supported with LSN One-to-One NAT, One-to-One NAT64, and Stateless NAT46.

The TCP MSS value is the maximum amount of data a network host can accept in a single TCP segment. The MSS does not include the TCP or IP header. TCP only handles smaller packets that pass without fragmentation. MSS Clamping changes and reduces the MSS value in TCP SYN, ensuring the packets are small enough to pass.

The following enhancements are implemented:

- The `cgnv6 nat46-stateless tcp mss-clamp` command is introduced to support TCP MSS Clamping for Stateless NAT46.
- The existing commands `cgnv6 lsn tcp mss-clamp` and `cgnv6 nat64 tcp mss-clamp` are enhanced to support One-to-One NAT with LSN and NAT64.

CLI Configuration

- To use a fixed maximum value for the TCP MSS, use the following command:

```
ACOS(config)# cgnv6 nat46-stateless tcp mss-clamp fixed 120
```

- To subtract a minimum value from the TCP MSS, use the following command:

```
ACOS(config)# cgnv6 nat46-stateless tcp mss-clamp subtract 20 min 456
```

- To maintain the TCP MSS value unchanged, use the following command:

```
ACOS(config)# cgnv6 nat46-stateless tcp mss-clamp none
```

See Also:

- IPv4-to-IPv6 Transition Solutions Guide
- Command Line Interface Reference

Firewall

ACOS 6.0.5 introduces the following new feature and enhancement for Firewall:

The following topic is covered:

Rate-Limiting Based on Radius Attributes

The Gi Firewall is enhanced to allow domain-based rate-limiting for subscribers by using a RADIUS custom attribute. Using this feature, users sharing the same domain can have individual rate-limits, while the domain can have an aggregated rate-limit. For example, users within the 'example' domain can be restricted to 500 Mbps per user, while the total throughput for the entire 'example' domain can be limited to 50 Gbps.

This enhancement provides the following features:

- Extraction of RADIUS derived attributes: ACOS extracts the information on domain user groups and individual users through RADIUS accounting messages.
- Granular control for dynamic rate-limiting: Rate-limiting policies can be configured for an individual subscriber, or a group of subscribers using hierarchical rate limiting.
- Efficient traffic-control: Traffic control rules can be created to use the subscriber-related derived attributes from the RADIUS server and then be associated to configured rate-limiting policies.
- Supported rate-limiting types: The generic rate-limiting using RADIUS attributes supports connections per second (CPS), throughput, and concurrent sessions.
- Single rule for IPv4 and IPv6: A single rule can be created to handle both IPv4 and IPv6 addresses for users and user groups by using the **ip-version**any option in the traffic-control rule-set.

The enhancement provides flexibility to set customized throughput limits for users or user groups as per requirement. It is useful in scenarios where bandwidth needs to be dynamically allocated as per user profiles and ensures fair network usage among users.

CLI Configuration

- To configure the custom derived attributes for user ID and user group on the system radius server, the following fields are added.

```
ACOS(config)#system radius server
```

```
ACOS(config-radius-server)#derived-attribute usergroup {imei | imsi |
msisdn | custom1 | custom2 | custom3 | custom4 | custom5 | custom1}
regex NAME<length:1-127>
ACOS(config-radius-server)#derived-attribute userid {imei | imsi |
msisdn | custom1 | custom2 | custom3 | custom4 | custom5 | custom1}
regex NAME<length:1-127>
```

- To add the scope of the new custom derived-attribute to a limit policy, the following command is added to the **template limit-policy** command.

```
ACOS(config)#template limit-policy <number>
ACOS(config-limit-policy)#limit-scope radius attribute {usergroup |
userid}
```

- To add the firewall rule filter based on the domain derived through the radius attribute, the following command is added to the **traffic-control rule-set**.

```
ACOS(config)# traffic-control rule-set 1
ACOS(config-rule set:1)#rule limit
ACOS (config-rule set:1-rule:limit)#source class-list 3 type radius
derived-attribute userid
ACOS(config-rule set:1-rule:limit)#source class-list 3 type radius
derived-attribute usergroup
```

- To handle both IPv4 and IPv6 addresses for users and user groups in the rate-limiting traffic-control rule-set, the following option is added to the **ip-version** command:

```
ACOS(config)#traffic-control rule-set RL
ACOS(config-rule set:RL)#rule limit1
ACOS(config-rule set:RL-rule:limit1)#ip-version any
```

Show Commands

The following show commands have been enhanced for this feature:

- To display the generic and hierarchical rate-limiting entries, as well as the total number of rate-limiting entries or parent rate-limiting entries with the scope RADIUS usergroup and userid, use the **show fw rate-limit** command.
- To view the value of derived-attributes, use the **show system radius table** command.

- To filter based on a derived attribute and its value, use the **`show system radius table derived-attribute-name [usergroup | userid]`** command.
- To clear system RADIUS table information related to derived attributes, use the **`clear system radius table derived-attribute-name`** `{usergroup | userid} derived-attribute-value` *`value`* command.

Limitations

- The hierarchical rate-limiting policy only supports rate-limiting throughput and connections per second (CPS).
- The dynamic configuration of the derived attribute on the RADIUS server is only applied to the latest updated accounting messages. It does not affect the existing values of derived attributes per RADIUS session. ACOS gets the derived attribute after it receives the RADIUS start and interim update accounting messages. If parsing fails, rate limiting entries with new scope are not created based on the value of derived attribute.
- In the dual-PU chassis and scaleout setup, the rate-limiting per user ID is applied on local node only. Rate-limiting per user group is applied across the nodes.

See Also:

- Firewall Configuration Guide
- Command Line Interface Reference

Global Server Load Balancing

ACOS 6.0.5 introduces the following new features and enhancements for Global Server Load Balancing (GSLB).

The following topics are covered:

DNS Sticky Support for Active-RDT Metric

The GSLB policy has been enhanced to provide DNS sticky support with the Active Round-Trip Delay (aRDT) metric. The DNS sticky feature saves the previous service IP result for a certain subnet and continues to use that IP.

When DNS sticky is combined with aRDT, it provides the best sticky result based on aRDT and switches to DNS sticky when aRDT discovers a better result. This enhancement maximizes performance by dynamically selecting the best service IP depending on real-time network conditions.

CLI Configurations

To prefer DNS stickiness with aRDT at the GSLB policy-level, use the following command:

```
ACOS(config)# gslb policy gslbp5
ACOS(config-policy:gslbp5)# active-rdt prefer-dns-sticky difference <1-16383>
```

The specified value is compared to the difference in response time between the current and previous best service IPs. The DNS sticky updates to the current best IP if the value exceeds the defined difference. Else, it remains unchanged.

See Also:

- Global Server Load Balancing Guide
- Command Line Interface Reference

Site Failover Support for Individual GSLB Services

The Global Server Load Balancer (GSLB) provides the ability to monitor the health of individual services running on a server port. A real port or service port under GSLB service IP can contain multiple services per application, such as, HTTP or FTP. Service labels can be added per service and health checks can be configured to check the status of these individual services.

For example, if a particular service on a port like HTTP service is down, only the HTTP service will be marked down. If the same port has other active services, like FTP service, the active service will continue to function and receive traffic.

The same port with different protocols, such as, UDP or TCP cannot share the same service label. For example, port 80 tcp git and port 80 udp git cannot be configured.

This feature can be useful in case of a port hosting multiple services, where health monitoring of individual services is required to ensure service availability. It can also be used by the GSLB controller to failover DNS traffic across sites based on the health status of individual services and thus provide uninterrupted user experience.

CLI Configuration

To implement a health check to the individual service port in real server, use the following command:

```
ACOS(config)#slb server Name IP address
ACOS(config-real server)#port number {tcp | udp}
ACOS(config-real server)#port number {tcp | udp} <port-service-name>
ACOS(config-real server-node port)#health-check <health-monitor>
```

For example:

```
slb server rs1 10.10.20.100
  port 80 tcp
  port 80 tcp http
    health-check HM_UP
```

To implement a health check to the individual service port in the GSLB service-IP, use the following command:

```
ACOS(config)#gslb service-ip Name IP address
ACOS(config-service-ip:Name)#port number {tcp | udp}
ACOS(config-service-ip:Name-port:type)#port number {tcp | udp} <port-service-name>
ACOS(config-service-ip:Name-port:Name)#health-check <health-monitor>
```

For example:

```
gslb service-ip s1 10.20.20.50
  port 80 tcp
  port 80 tcp http
    health-check HM_UP
```

After applying the health-checks to the individual service ports, create a GSLB zone with matching individual service port and label in the `service` command. Map the DNS A records with the respective service name.

```
ACOS(config)#gslb zone Name
ACOS(config-zone:Name)#service port number <port-service-name>
ACOS(config-zone:Name-service:port-service)#dns-a-record {<real server |
gslb service-IP> |<port-service-name>}
```

For example:

```
gslb zone abc.com
  policy failover
  service 80 http
    dns-a-record rs1 http static
    dns-a-record s1 http static
```

The dns-a-record matches the server name, port number from gslb zone and then the service label name (service 80 http). The health check state is retrieved from the matching port.

Show Commands

- To verify the service port status, use the **`show gslb site`** command.
- To check the reason if a port service is down, use the **`show health monitor <monitor name>`** command.

Limitations

Configuring health checks for individual service ports has the following limitations:

- Does not support dynamic real servers and SLB server port range.
- Does not support GSLB protocol health check.
- The `show slb server` command does not show ports with service labels.

See Also

- Global Server Load Balancing Guide
- Command Line Interface Reference

Multi-Match Rule-Based DNS Resolution

A10 Global Server Load Balancing (GSLB) supports multi-match rule-based DNS Resolution that allows you to redirect incoming DNS client queries to a target zone

service (within the same zone) based on specific conditions, such as the domain name, the client's source IP, and the health status of GSLB service IP, GSLB site, or SLB server.

When a client DNS query matches all the conditions in a rule, it is redirected to the configured target service of the matched rule within the same zone. The policies and configurations of the new target service are then used to process the query. This capability helps organizations manage DNS queries more effectively and improves the availability and reliability of services across distributed environments.

The **service-matching-rules** command is introduced to implement rule-based DNS resolution. This command allows you to create multiple service-matching rules within a GSLB zone to match specific conditions and select the appropriate service.

CLI Configuration

- To configure service-matching rules in a GSLB zone, use the **service-matching-rules** command as shown below:

```
ACOS(config)# gslb service-matching-rules zone a10.com
ACOS(config-service-matching-rules:a10.com)# rule 1
ACOS(config-service-matching-rules:a10.co...)# domain-name equals
www.example.com
ACOS(config-service-matching-rules:a10.co...)# source-addr
192.168.6.0/24
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-site
a10-dc1 AllUp-or-PartUp
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-
service-ip a10-rs1 Up
ACOS(config-service-matching-rules:a10.co...)# health-state slb-server
a10-dc1-link-1b Down
ACOS(config-service-matching-rules:a10.co...)# service example-
service1
```

  In the above example configuration, service matching rule *1* is created within the GSLB zone *a10.com*. In this rule, the DNS queries are redirected to the *example-service1* service only when the following conditions are met:

  - The domain name matches *www.example.com*
  - The DNS query originates from the IP range *192.168.6.0/24*.

- The *a10-dc1* GSLB site is either fully operational or partially operational.
- The *a10-rs1* GSLB service IP is in Up state.
- The *a10-dc1-link-1b* SLB server is in Down state.

- To enable the hit count for rule matching within a GSLB zone, configure the **hitcount-enable** parameter:

```
ACOS(config)# gslb service-matching-rules zonea10.com
ACOS(config-service-matching-rules:a10.com...)# hitcount-enable
```

- To view the service matching rules configured in a specified zone:

```
ACOS(config)# show gslb zone <zone-name> service-matching-rules
```

- To view the service matching rules configured in all GSLB zones:

```
ACOS(config)# show gslb zone service-matching-rules
```

Limitations

- A maximum of 32 service matching rules can be configured for one GSLB zone.
- A maximum of four health-state statements can be defined in a single service matching rule.

See Also

- Global Server Load Balancing Guide
- Command Line Interface Reference

MIB

ACOS 6.0.5 introduces the following new features and enhancements for SNMP MIB:

The following topic is covered:

Enhanced SNMP Support for Multi-PU Platforms

This release extends Simple Network Management Protocol (SNMP) support for solutions involving Secure Sockets Layer (SSL) and Web-category that utilize multiple processing units (PUs).

The OIDs in the following SNMP MIB modules are officially tested for multi-PU platforms and are added to the public list:

- ACOS-PKI-CERT-STATS-MIB.txt
- ACOS-SLB-SSL-ACME-CERT-STATUS-MIB.txt
- ACOS-SLB-SSL-FORWARD-PROXY-MIB.txt
- ACOS-SLB-SSL-JA3-MIB.txt
- ACOS-SLB-SSL-JA4-MIB.txt
- ACOS-SLB-SSL-STATS-MIB.txt
- ACOS-WEB-CATEGORY-MIB.txt
- ACOS-WEBCATEGORY-STATISTICS-MIB.txt
- ACOS-WEBCATEGORY-LICENSE-MIB.txt

See Also:

- SNMP MIB Reference
- Command Line Interface Reference

Platforms

ACOS 6.0.5 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

AWS IAM Role Support

vThunder instances can now use AWS Identity and Access Management (IAM) roles to access resources needed for high availability (HA) failover.

When vThunder instances are configured in AWS HA mode with an IAM role, they automatically fetch temporary security credentials from the attached IAM role. These credentials are obtained dynamically during HA failover and written to the aws-cred file. The vThunder instances use these credentials to access AWS resources necessary to maintain HA.

An IAM role with the "AmazonEC2FullAccess" policy is required to configure vThunder instances in AWS HA.

See Also:

- Installing vThunder on AWS

ACOS Event Logs Timestamp Enhancement

ACOS event logs sent to the remote syslog servers now include the millisecond and year information in the timestamp. This additional information helps in accurate log analysis and operational efficiency for the DNS logging service, which operates over one million queries per second (1MQPS). The enhancement applies to both control plane and data plane logs.

The following commands are introduced:

- `enable-millisec` – To include milliseconds in the timestamp.
- `use-iso8601-timestamp` – To send the syslog messages with the standard header format that includes milliseconds and the year information in the timestamp of the logs. The timestamp is in the ISO 8601 format (yyyy-mm-ddThh:mm:ss+-ZONE), as per RFC 5424.

CLI Configuration

- To enable milliseconds in the timestamp, use the following command:

```
ACOS(config)# acos-events log-properties enable-millisec
```

- For standard header format which includes the year in the timestamp, use the following command. This is specific only to Syslog messages:

```
ACOS(config)# acos-events log-properties use-iso8601-timestamp
```

Log Sample

The following is a syslog sample that displays the year and milliseconds in the timestamp:

```
2024-07-29T14:11:14.761+0100 vThunder[ACOS] a10lb 486715314709463043:
UDP 15.15.15.10 56612 15.15.15.99 53 Type=Query QueryId=24300
Opcode=Query HeaderFlag=RD|AD QDCount=1 ANCount=0 NSCount=0 ARCount=1
dhost=www.a10.networks.com QueryType=A QueryClass=IN
```

See Also:

- Event Logging Guide
- Command Line Interface Reference

Enhanced Thunder 1060 Platforms

Thunder 1060S non-FTA platforms have been optimized to support CGN and CFW deployments (apart from ADC, SSLi, and TPS).

Additionally, these platforms provide flexible bandwidth tiers through modular licensing to scale your network capacity as needed.

See Also:

- A10 TH1060S Installation Reference Guide
- Platform Support Information

UDP Traffic on Port 4791

When RoCEv2 (Remote Direct Memory Access (RDMA) over Converged Ethernet version 2) protocol is enabled on the host configured with Mellanox Connect-X5/X6 SRIOV adapter, ACOS does not receive the UDP traffic on port 4791.

To ensure UDP packet transmission on port 4791, it is recommended to disable the RoCEv2 protocol on the host.

See Also:

- Installing vThunder on KVM
- Installing vThunder on VMware ESXi

Threat Protection System

ACOS 6.0.5 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to DDoS Mitigation Guide. Similarly, for TPS-related CLI commands, refer to DDoS Command Line Reference Guide.

Security Updates

The following security vulnerabilities are addressed in this release:

OpenSSL Vulnerability

- CVE-2024-2511: The vulnerability related to non-default TLS server configurations causing unbounded memory growth when processing TLS v1.3 sessions resulting in a Denial of Service.

A10 Vulnerability

- A10-2023-0018: The vulnerability compromised an authentication token that may be used to elevate user privileges, potentially providing access to unauthorized organization data.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.4

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.4 release:

The following topics are covered:

Application Access Management

ACOS 6.0.4 introduces the following new feature and enhancement for Application Access Management (AAM):

The following topic is covered:

Proxy Chaining Support

The SAML authentication forward proxy is enhanced to support the proxy chaining that provides a solution for “Cloud Access Proxy”. It controls traffic intended for the cloud services from bypassing the existing proxy. After successful SAML authentication, it creates the authentication session in the forward proxy environment, and then the traffic intended for the cloud services passes through the existing proxy. This feature works only in the forward proxy mode.

See Also:

- Application Access Management Guide

Application Delivery Controller

ACOS 6.0.4 introduces the following new features and enhancements for Application Delivery Controller (ADC):

The following topics are covered:

Enhanced DNS Application Firewall with TLD Filtering

The DNS Application Firewall (DAF) is enhanced to improve the security and optimize the traffic management of top-level domains (TLD).

DAF can now filter the DNS queries based on their TLDs. A TLD filtering policy can be configured to allow only DNS queries with legal TLDs. The DNS queries with illegal

TLDs are dropped. A class-list of type string-case-insensitive is used to define the legal TLDs.

The logging feature can also be enabled to capture dropped DNS queries without legal TLD or with illegal TLD. Logs can be stored remotely by default in the same format as the DNS query log. Local logging can be enabled based on user settings. The log contains the reasons for dropped queries.

CLI Configuration

To configure a case-insensitive string type class-list containing the legal TLDs:

```
ACOS(config)#class-list TLD-list string-case-insensitive
ACOS(config-class-list)#str com
```

To configure the SLB DNS template to enable TLD filtering and logging:

```
ACOS(config)#slb template dns d1
ACOS(config-dns)#tld-filter-white-list TLD-list
ACOS(config-dns)#tld-filter-log-enable
```

Log Examples

The following is a SYSLOG sample that displays a DNS query dropped due to TLD filtering:

```
486707686847545345#tcp 1.2.3.4 1 4.5.6.7 1 Type=query QueryId=1345
Opcode=QUERY HeaderFlag=RD QDCount=0 ANCount=0 NSCount=0 ARCount=0
dhost=server.example.com QueryType=A QueryClass=IN TLD Filter Drop
```

The following is a CEF log sample that displays a DNS query dropped due to TLD filtering:

```
486707686847545345#proto=tcp src=1.2.3.4 spt=1 dst=4.5.6.7 dpt=1
cs1=query cs1Label=Query cn1=1345 cn1Label=Query ID cs2=QUERY
cs2Label=Opcode cs3=RD cs3Label=Header Flag cn2=0 cn2Label=Question
Count cn3=0 cn3Label=Answer Record Count cn4=0 cn4Label=Authority Record
Count cn5=0 cn5Label=Additional Record Count dhost=server.example.com
cs4=A cs4Label=Query Type cs5=IN cs5Label=Query Class reason=TLD Filter
Drop
```

See Also:

- DDoS Mitigation Guide (For ADC)
- Command Line Interface Reference

Enhanced DNS Application Firewall with FQDN Label Length and Count Filtering

The DNS Application Firewall (DAF) is enhanced to filter DNS requests based on the Fully Qualified Domain Name (FQDN) label length and count. These filtering policies help mitigate DNS-based attacks, where attackers use FQDNs with excessively long or numerous labels to overwhelm the DNS server and disrupt service availability.

The **label-length-filter** and **label-count-filter** commands are introduced to implement these filtering policies. By configuring appropriate thresholds and actions, you can drop, or forward DNS requests based on the label length or count, thereby enhancing overall security and network performance. The dropped DNS requests can also be logged for further analysis and tuning of threshold settings.

CLI Configuration

- To enable the FQDN label length filter, configure the following commands under SLB DNS template:

```
ACOS(config)# slb template dns <template_name>
ACOS(config-dns)# label-length-filter
ACOS(config-dns-label-count-filter)# drop-log-enable
ACOS(config-dns-label-count-filter)# action { drop | ignore }
ACOS(config-dns-label-count-filter)# fqdn-label-length <1-63> suffix
<1-5>
```

  - To configure the action when the FQDN label length exceeds the configured threshold limit, use the **action { drop | ignore }** command.
  - To enable logging when the DNS request is dropped, use the **drop-log-enable** command.
  - To set the maximum length for an individual label in an FQDN, use the **fqdn-label-length** command.

NOTE: You can specify the **fqdn-label-length** parameter up to six times within one **label-length-filter** configuration, i.e., you can configure up to six different rules to check label lengths in a single FQDN label-length filter configuration.

- To specify the number of trailing labels to be ignored in an FQDN, use the **suffix** parameter.

- To enable the FQDN label count filter, configure the following commands under SLB DNS template:

```
ACOS(config)# slb template dns <template_name>
ACOS(config-dns)# label-count-filter
ACOS(config-dns-label-count-filter)# drop-log-enable
ACOS(config-dns-label-count-filter)# action { drop | ignore }
ACOS(config-dns-label-count-filter)# min-fqdn-label-count <1-31>
ACOS(config-dns-label-count-filter)# max-fqdn-label-count <1-7>
```

  - To configure the action when the FQDN label count exceeds the configured threshold limit, use the **action { drop | ignore }** command.
  - To enable logging when the DNS request is dropped, use the **drop-log-enable** command.
  - To set the maximum number of FQDN labels allowed per FQDN, use the **max-fqdn-label-count** command.
  - To set the minimum number of FQDN labels allowed per FQDN, use the **min-fqdn-label-count** command.

See Also:

- DDoS Mitigation Guide (For ADC)
- Command Line Interface Reference

DNS Cookie Record Filtering Support

The DNS Cache Cookie Policy is introduced and implemented while serving DNS requests containing cookie records. With this feature, ACOS filters cookie records present in DNS queries and responses.

Based on a client's DNS cookie policy, caching DNS responses having cookie records can lead to multiple issues. The DNS Cache Cookie policy can be configured to serve DNS queries with cookie records using either of the following options:

- from the cache without including cookie records
- forwarded to the backend server, ensuring that the cookie records are included in the response

The policy can be configured at the Global level and SLB DNS template, bound to the virtual port. By filtering records on cookies, ACOS ensures that the privacy and security of the cookie content is intact. The feature simplifies cookie management and also leads to enhanced performance.

This feature is applicable to UDP, DNS-UDP, DNS-TCP, and standard/nonstandard ports. It supports all DNS record types in ACOS.

CLI Configuration

To configure the cookie record filtering policy globally, use the following command:

```
ACOS(config)#slb common
ACOS(config-common)#dns-cookie-cache-policy {served-by-cache | served-by-backend}
```

To configure cookie record filtering policy within the SLB template, use the following command:

```
ACOS(config)#slb template dns <templatename>
ACOS(config-dns)#dns-cookie-cache-policy {served-by-cache | served-by-backend}
```

See Also:

- Application Delivery Controller Guide
- Commad Line Interface Reference
- RFC 7873

Supporting TYPE-based Resource Records in RPZ

ACOS DNS Firewall supports the parsing of **A**, **AAAA**, **CNAME**, **NS**, **SOA**, and **MX** Resource Records (RR) in an RPZ file. This implies that ACOS DNS Firewall can enforce policies to redirect and block queries based on the content of these specific RR types. To widen the range of RR types supported, ACOS DNS Firewall is enhanced to parse DNS records based on their TYPE IDs as well. This enhancement provides more flexibility to create RPZ policies using newer and less common RR types, thereby increasing ACOS DNS firewall's effectiveness in filtering and securing DNS traffic.

To enforce policies based on RR types you need to specify **TYPE**<*num*> in the RPZ file. For example, since the TYPE ID for **HTTPS** records is 65, to handle **HTTPS** records, you need to specify **TYPE65**.

NOTE: Since parsing **HTTPS** records is not supported, any **HTTPS** records in the RPZ file will be ignored. You must specify **TYPE65** to parse **HTTPS** records.

Consider the following two policies:

```
domain.org  IN TYPE65 .
domain.org  IN HTTPS  .
```

The first policy will be parsed and processed by ACOS, resulting in an **NXDOMAIN** response. However, the second policy will result in a parsing error, and all valid/invalid policies below it will be ignored.

See Also:

- DDoS Mitigation Guide (For ADC)

Weighted Least-Request Methods for Load Balancing

The load balancing functionality is enhanced with the addition of the server weighted and service port-weighted least-request methods to SLB service-group. These methods leverage both, the server/port weights respectively to prioritize servers/ports with higher weights and also consider the HTTP request count on each server or port.

This feature has the following key points:

- **Combines assigned weight and request count**: For selecting a server or service-port to distribute load, the method first checks the server weight/service-port weight respectively. Next, it checks the request count on the server or service-port as per the method used, and applies the formula request count/weight. As per the result in the formula, ACOS selects the server/service port that has the minimum value for distributing load.
- **Considers the combination of server/port weight compared to server/port template weight**:

  For the request count/weight formula, the following weight is considered in calculation:

  - If a server/port having a default weight configured, is bound to a template, with a weight also assigned to the server/port template, then the method considers the server/port template weight.
  - If the weight on a server/port is not the default weight, then, this weight is considered instead of the server/port template weight.

  Using the request count/weight formula, if there are multiple candidates with the same minimum value, then the selection first considers the processed bytes on the server/port. If there are still multiple candidates, then the method randomly chooses a server/port.
- **Provides Optimal Performance**: As the weight and request count criteria are both considered, load is distributed as per the capacity of servers/ports. This ensures that resources are used optimally and leads to improved performance.

CLI Configuration

To configure the weighted-least-request method for a server in a service-group, use the following command:

```
ACOS(config)#slb service-group <svg name> <tcp/udp>
ACOS(config-slb svc group)#method weighted-least-request
```

To configure the weighted-least-request method for a service port in a service-group, use the following command:

```
ACOS(config)#slb service-group <svg name> <tcp/udp>
ACOS(config-slb svc group)#method service-weighted-least-request
```

Limitation

This method only calculates the HTTP/HTTPS requests on virtual ports.

See Also:

- Command Line Interface Reference

ACME Certificate Chain Support

ACOS supports the automatic fetching of the ACME certificate chain (chain-cert) after successful ACME certificate enrollment, renewal, or removal. The ACME chain-cert uses ACME protocol to validate certificates against a chain of trusted authorities, ensuring the integrity of the connection between the client and server. This also ensures continuous security without manual intervention and compatibility across all the infrastructure's certificates.

The chain-cert information will be saved and logged as '<cert_name>_full_chain' in ACOS. Additionally, in an aVCS environment, the master and blade will synchronize the chain-cert information.

Show Commands

- To view the brief details of ACME chain-cert, use the **`show pki cert`** command.
- To view the complete details of ACME chain-cert, use the **`show pki cert <acme_cert_name>`** command.

See Also:

- Application Delivery Controller
- SSL Insight (SSLi) Configuration
- IP Security Configuration

Increased the SLB Resource Limits

In the SLB resources, ACOS has increased the maximum allowed GSLB service IP, port count, and health monitor. This enhancement addresses the requirements of large GSLB deployments, ensuring sufficient capacity for expanding infrastructure.

The following changes have been implemented:

- GSLB service IP count has been increased from 5k to 12K.
- GSLB service port count has been increased from 10k to 24K.
- Health monitor has been increased from 8K to 16K.

This change is only applicable on TH3350S and on vThunder devices with memory >=64 GB.

Show commands

The **show-slb resource-usage** command displays the increased number of service-IPs, service-ports, and health-monitor counters:

```
ACOS(config)# show slb resource-usage
Resource                          Current    Default    Minimum
Maximum
-------------------------------------------------------------------------
-------....
gslb-service-ip-count             12000      12000      512        12000
gslb-service-port-count           24000      24000      512        24000
health-monitor-count              16384      1023       512        16384
.....
```

See Also:

- Command Line Interface Reference

Firewall

ACOS 6.0.4 introduces the following new feature and enhancement for Firewall:

The following topics are covered:

Custom Logging Format for Firewall

The standard logging formats such as Syslog, CEF, and ASCII offer a robust logging framework. However, they often contain excessive data that may not always be relevant. This additional data increases the packet size, which results in higher logging expenses. To optimize log management, and improve efficiency and readability, the custom logging format is introduced for Firewall Session Open and Delete logs.

This compact format provides the flexibility to include only specific events (currently only session creation and deletion events are supported) and fields in the Firewall logs. You can also include event-specific details such as session start time, session duration, and more by using certain predefined keywords. This flexibility helps adjust and reduce the log size, thereby lowering logging costs.

The commands **format custom** and **custom message** are added to the Firewall logging template to configure a custom logging format for the Firewall.

CLI Configuration

To configure a custom log format, you need to enable the **format custom** command and then set the message string using the **custom message** command in the Firewall logging template.

```
ACOS(config)# fw template logging template_name
ACOS(config-logging)# format custom
ACOS(config-logging)# custom message {session-created | session-deleted}
custom_string
```

The **custom message** command allows you to set an arbitrary log message by specifying certain events and predefined keywords.

The following example demonstrates command usage:

```
ACOS(config)# fw template logging template_custom
ACOS(config-logging)# format custom
ACOS(config-logging)# custom message session-created FW_SESSION_
CREATED,$src-ip$,$src-port$,$proto-name$,$dst-ip$,$dst-port$,$sesn-start-
time$,$rule-set-name$,$rule-name$,$in-interface$,$out-interface$
```

```
ACOS(config-logging)# custom message session-deleted FW_SESSION_
DELETED,$src-ip$,$src-port$,$proto-name$,$dst-ip$,$dst-port$,$sesn-start-
time$,$sesn-dur$,$rule-set-name$,$rule-name$,$in-bytes$,$out-bytes$,$pkts-
tx$,$pkts-rx$
```

NOTE:

- The **format custom** command must be configured to enable custom logging. If the **custom message** command is configured without enabling this command, logs will be generated in the default CEF format.
- The keywords must be enclosed in dollar signs ($).

Corresponding custom logs generated:

```
FW_SESSION_
CREATED,10.0.0.6,1769,UDP,20.0.0.4,0,20240425223523,rs1,rule1,ve2,ve3
FW_SESSION_
DELETED,10.0.0.6,1768,UDP,20.0.0.4,0,20240425223543,14559,rs1,rule1,0,42,1
,0
```

See Also:

- Firewall Configuration Guide
- Command Line Interface Reference

Enhanced TCP Half-Close Idle Timeout Range

The configurable range for idle timeout value of TCP half-close firewall sessions has been extended from 60-120 seconds to 1-120 seconds, thereby allowing you to set timeout values below 60 seconds. Smaller timeout values improve resource utilization by enabling quicker termination of idle sessions. This enhancement is useful in environments having frequent session turnovers or short periods of inactivity.

CLI Configuration

The **fw session-aging** command allows you to set the half-close TCP session idle timeout value.

- To set the idle timeout value globally:

```
ACOS(config)# fw session-aging <template_name>
ACOS(config-session-aging)# tcp half-close-idle-timeout <1-120 seconds>
```

- To set the idle timeout value for a specific port:

```
ACOS(config)# fw session-aging <template_name>
ACOS(config-session-aging)# tcp port <port-num> half-close-idle-timeout <1-120 seconds>
```

See Also:

- Command Line Interface Reference

Global Server Load Balancing

ACOS 6.0.4 introduces the following new features and enhancements for Global Server Load Balancing (GSLB).

The following topics are covered:

Enhancement to GSLB Synchronization Mechanism

The GSLB Synchronization mechanism is enhanced to enable the synchronization of additional ACOS configuration objects, such as, real servers, service-groups, or virtual servers, from the GSLB master to all other members in the GSLB Controller group.

NOTE: All the member nodes in the GSLB group must run the same software release version. This feature only works if all the devices are in the shared partition.

The default GSLB synchronization only considered the configuration of GSLB-specific elements, such as, zones, sites, policies, and services. By enabling the

synchronization of other ACOS configuration, this feature helps maintain seamless GSLB operations and continuity of services during and after a failover.

The synchronization of additional ACOS configuration data also provides consistency across the members in the GSLB group. It ensures accuracy of DNS responses, optimal performance, effective load-balancing and efficient GSLB group management.

The enhanced GSLB synchronization feature brings the following functionalities:

- **Shared configuration**: All the controller nodes have the exact same data after synchronization. The additional configuration objects are thus considered as common or shared configurations.
- **Real-time Synchronization**: In case of any configuration change done on the master node, the same change is dynamically synchronized to all other members. The master node does not wait for a response from each member. A member logs a failure message if it fails to process the sync command.
- **Full Synchronization when a new GSLB node joins**: When a new GSLB node joins the existing GSLB Controller group, the master node pushes the entire default GSLB configuration objects and additional configured objects to the new node. The new node replaces its configuration with the pushed configuration. Errors occurring during the synchronization are ignored and the remaining configuration is applied on the member nodes.
- **Force Full Synchronization from GSLB Master to Members**: The GSLB master can forcibly perform the full synchronization of the entire configuration to the member nodes.

Additionally, the timeout option (1-60 minutes) is added to GSLB group synchronization to ensure that GSLB groups get sufficient time for full synchronization. The timeout feature ensures that member servers are up to date with the master.

CLI Configuration

The `gslb sync-objects` command is introduced to synchronize additional ACOS objects.

- To synchronize specified additional objects, use the following command on the GSLB master node:

```
ACOS(config)#gslb sync-objects <objects>
```

The following example demonstrates synchronizing the **slb.server** object:

```
ACOS(config)#gslb sync-objects slb.server
```

- To enable the synchronization globally, use the following command:

```
ACOS(config)#gslb sync-objects action enable
```

- To enable force synchronization of GSLB configuration from master to member nodes:

```
ACOS:Master(config-group:default)force-full-sync
```

- To specify the timeout for GSLB configuration synchronization, use the following command:

```
ACOS(config)#gslb group <groupname>
ACOS(config-group:default)#sync-timeout <1-60>
```

Limitations

- In case of a change of scope to GSLB dynamic synchronization, the changes are not applied to the existing configuration. The changes are only implemented to new configurations made after the changed scope.
- If a member fails to process the **gslb sync-objects** command, a failure rollback is not triggered in other nodes. Instead, the member logs a failure message.
- GSLB cluster does not detect out of synchronization cases between member nodes.
- The synchronization only considers common ACOS objects such as servers, service-groups, templates. It does not support the synchronization of device-specific configuration.

See Also:

- Global Server Load Balancing Guide
- Command Line Interface Reference

Support for Current Connection Metrics

ACOS has enhanced the load balancing functionality across sites in different data centres based on the current number of connections handled by each site. This feature has introduced the following capabilities:

- Implemented GSLB metric that aggregates the current connection count across all SLB devices within a site and uses this metric to select the site with the lowest aggregated current connections for serving DNS records.
- Enabled the sharing of a service IP (VIP) server across multiple SLB devices within the same site.

These capabilities are specifically designed for the organizations that run multiple data centers in a scaleout cluster, each hosting different services (sites) on load balancing devices to manage the traffic load.

When this feature is implemented, ACOS ensures that the load is distributed evenly across data centers by considering the number of active connections that each server is handling. It maximizes resource utilization and improves performance.

Supported Features

- The current connection metric is supported for all VIP servers bound under SLB devices in a site.
- The scaleout virtual IP servers must be restrictively used by only one site.
- A maximum of 16 SLB devices can share a service IP as a VIP server.
- The metric only considers the connection count of ports having active services. Connection count of virtual IP servers having services/ports with the DOWN status are not considered.

CLI Configuration

To enable current connection count for a policy (test_policy), use the following command:

```
ACOS(config)# gslb policy test_policy
ACOS(config-policy:test_policy)# dns server
ACOS(config-policy:test_policy)#connection-count-by-site enable
```

To enable current connection count within a policy (test_policy), use the following command in the **metric-order** command:

```
ACOS(config-policy:test_policy)# metric-order connection-count-by-site
```

The GSLB `test_policy` is configured, which enables an ACOS device to act as a DNS server for specific service IPs in the GSLB zone to which the policy is applied. The DNS records are filtered based on the aggregated current connections between different sites.

Show Commands

- The `Cur-Conn` counter in the following command is updated to display the port-wise aggregated current connection count. The 'S' attribute is added to indicate if the port is shared or not.

  ```
  ACOS(config)#show gslb service-port
  ```

- The `Current-Connections` counter is added to the following command to display the current connection count per SLB device that share the same virtual IP server having active services. It also displays the site-level aggregation count.

  ```
  ACOS(config)#show gslb site curr-conn
  ```

- The `Shared` attribute is added to the following command to show if the service IP is shared or not.

  ```
  ACOS(config)#show gslb service-ip
  ```

- The `show counters gslb dns` command is updated to display the counters for connection-count-by-site metric:

  ```
  ACOS(config)#show counters gslb dns
  ----------------------------
  Metric Connection Count by Site Hit                    4
  ```

- The `clear gslb samples` command is updated to clear the connection count for shared vip-service.

  ```
  ACOS#clear gslb samples
  ```

See Also:

- Global Server Load Balancing Guide
- Command Line interface Reference

Management Access and Security

ACOS 6.0.4 introduces the following new feature and enhancement for Management Access and Security (MAS):

NOTE: For configuration, refer *Management Access and Security (MAS) Guide* and for specific CLI commands, refer *Command Line Reference Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topic is covered:

Dynamic Authentication and Authorization using TACACS+ Group Extraction

ACOS can extract group memberships from the TACACS+ (Terminal Access Controller Access-Control System Plus) server at the time of user authentication and authorization. It grants the Thunder device access to the users based on these group memberships. The TACACS+ server defines group permissions, including various users across different user groups, each with specific roles, access types, and privilege levels.

When a user logs into the Thunder device using CLI or GUI, its access permissions are dynamically determined by the group assigned to them in the TACACS+ server. For example, if a user belongs to a read-only group in TACACS+ server, it can only be able to execute show commands and not the configuration commands.

CLI Configuration

To configure the Thunder device for dynamic authentication and authorization using TACACS+ group membership extraction:

```
ACOS(config)#authentication type tacplus local
ACOS(config)#authentication enable tacplus local
ACOS(config)#authentication login privilege-mode
ACOS(config)#authorization commands 15 method tacplus
ACOS(config)#tacacs-server host tacacs_server_ip secret encrypted
secret-key
ACOS(config)#interface management
ACOS(config-if:management)#ip address ip_address ip_subnet_mask
ACOS(config-if:management)#ip control-apps-use-mgmt-port
ACOS(config-if:management)#ip default-gateway default_gateway_address
```

Show Command

To verify if the access permissions are applied correctly based on the group memberships:

```
ACOS(config)#show admin session
```

See Also:

- Management Access and Security Guide

MIB

ACOS 6.0.4 introduces the following new features and enhancements for SNMP MIB:

The following topic is covered:

Enhanced SNMP Support for Multi-PU Platforms

ACOS provides enhanced Simple Network Management Protocol (SNMP) support for platforms with multiple processing units (PUs). A new CM subagent is introduced in ACOS. It provides the SNMP manager with data from individual PU or aggregated data from multiple PUs.

Multiple SNMP MIB tables are generated for stats data and oper data of a configuration management object. Each SNMP table contains a default index, **slotId**, for identifying blades in a multi-PU platform:

- slotId 0: Aggregation of all blades
- slotId 1: Data from PU1/Standalone platform
- slotId 2: Data from PU2

Limitation

The SNMP tables do not include an index for L3V partitions. To request data for an L3V partition, attach the partition name to the community string (e.g., public@p1) in the SNMP request. The response for the request will contain data specific to the requested L3V partition.

CLI Configuration

To enable the CM schema agent, use the following command:

```
ACOS(config)#snmp-server enable schema-agent
```

See Also:

- SNMP MIB Reference
- Command Line Interface Reference

Networking

ACOS 6.0.4 introduces the following new features and enhancements for the Network Configuration:

The following topics are covered:

Layer 3 Health Monitoring

ACOS provides layer 3 health monitoring support for virtual wire and virtual wire with SSLi (IP-less), which operates transparently in high-availability deployments. In

these deployments, two firewall devices manage the active and standby paths during failover scenarios. During a switch from active to standby, ACOS might continue to send packets for previously established sessions, causing traffic to route incorrectly, thereby disturbing network traffic.

To address these scenarios, Layer 3 health checks are introduced for VLAN monitoring. The ping, gratuitous ARP (GARP), and packet count heath check methods can be implemented on the target device. It allows ACOS to detect which VLAN is in active or standby mode. Moreover, the health check prevents ACOS from sending the packets to the ACOS standby devices, thus avoiding network disturbances. The health check works only on ACOS device.

The following L3 health check methods are introduced:

- **Ping Method**: In this method, ACOS sends an ICMP echo request to the target IP address from configured interface and checks for the response. If it does not receive a response to two consecutive echo requests, the VLAN status is marked as standby.
- **GARP Method**: In this method, the GARP packets monitor the target IP address or interface for a specified interval. If GARP packets are not received within the configured interval, the VLAN status is marked as standby.
- **Packet Count Method**: In this method, the packet rate monitors the target IP address or interface for a specified active threshold. If it falls below this threshold, the VLAN status is marked as standby.

The health check works only on ACOS device.

CLI Configuration

To configure the layer 3 health check methods, use the following command:

```
ACOS(config)# virtual-wire-health-check vlan 10 method {ping | garp |
packet-count}
```

Show Commands

- To view various layer 3 health check statistics, use the following show commands:
  - **show virtual-wire-health-check statistics**
  - **show virtual-wire-health-check vlan <id> statistics**

- To view the 'standby drop' counter for packets dropped due to VLAN in standby mode, use the **`show virtual-wire-global counters`** command.

Limitation

IPv6 addresses are unsupported and cannot be configured for the target device or interface.

See Also:

- Network Configuration Guide
- SSL Insight (SSLi) Configuration Guide
- Command Line Interface Reference

Next Generation Web Application Firewall

ACOS 6.0.4 introduces the following new features and enhancements for the Next Generation Web Application Firewall (NGWAF):

The following topics are covered:

Importing Next-Gen WAF Files Using Explicit Proxy Settings

The NGWAF file import process has been enhanced to utilize explicit HTTP proxy settings for downloading NGWAF files from the Fastly site. This feature is beneficial in environments with restricted direct internet access and where all communication is routed through an explicit proxy. It also helps to improve security, maintain compliance, and ensure operational efficiency in controlled networks.

CLI configuration

The **`proxy`** parameter is added to the **`import ng-waf-module`** and **`import ng-waf-custom-page`** commands to define HTTP proxy settings for downloading NGWAF files. This parameter allows you to specify proxy settings in the *`host:port`* format,

that supports usage of IPv4 address, IPv6 address, or hostname as the host.

- To import the latest NGWAF agent using proxy settings:

```
ACOS(config)# import ng-waf-module proxy <host:port> <remote_file_
path>
```

Example command using IPv4 address:

```
ACOS(config)# import ng-waf-module proxy 10.12.10.157:3128
https://dl.signalsciences.net/sigsci-agent/sigsci-agent_latest.tar.gz
```

- To import a custom HTML page for NGWAF using proxy settings:

```
ACOS(config)# import ng-waf-custom-page <html_page> proxy <host:port>
<remote_file>
```

Example command:

```
ACOS(config)# import ng-waf-custom-page mypage  proxy myproxy.com:443
 https://www.google.com
```

NOTE:

- An IPv6 address must be encased in a bracket, for example, *[a:b::1]:3128*.
- Only HTTP or HTTPS URLs can be specified for downloading files.

- The proxy parameter is also added to the following import sub-commands to support file downloads using explicit proxy settings:
  - **aflex**
  - **auth-saml-idp**
  - **bw-list**
  - **class-list**
  - **health-external**
  - **health-postfile**

See Also:

- Next-Gen WAF Configuration Guide
- Command Line Interface Reference Guide

Redirecting Requests Using Custom Agent Response Codes

Fastly has enhanced the custom response code functionality by adding codes 301 and 302 for request redirection. Using these codes, you can specify an absolute or relative URL within the Fastly site rules to redirect client requests. Additionally, you can also specify the **{{REQUESTID}}** placeholder along with the URL to pass the request ID to the redirected location.

The following enhancements have been introduced in ACOS Next-Gen WAF to support this functionality:

- Parsing the agent's response and sending the redirected response to the client.
- Adding a new **Redirected** counter to the **show ng-waf** *<vs> <vport>* command to indicate the number of requests redirected.
- Adding new fields and labels to the Syslog and CEF logs to indicate the redirected URL and the associated request ID.

Limitations

- The maximum length for a redirect URL cannot exceed 16384 characters.
- Request redirection does not function when the **ng-waf monitor-mode-enable** command is configured on the ACOS device because, in the monitor mode, Fastly site rules for blocking and redirecting requests are ignored.

See Also:

- Next-Gen WAF Configuration Guide

Enhanced Next-Gen WAF Logging

ACOS Next-Gen WAF (NGWAF) logging has been enhanced to include the following information in both Syslog and CEF formats:

- **Real Source IP Address**

  Currently, ACOS NGWAF logs the source IP address by extracting information from the IP header. However, when NGWAF is positioned behind a proxy, load balancer, or NAT device, the logged IP address may correspond to that of the intermediate device rather than the client's original address. To ensure accurate logging and tracking of the client's real source IP address, ACOS NGWAF now extracts details from the X-Forwarded-For (XFF) header and logs the real source IP address. This enhancement helps in troubleshooting issues and analyzing requests.

  New fields **`RealSource`** and **`Real Source`** are added to the Syslog and CEF formats, respectively, to display the actual source IP address of the client.

  NOTE: Since the XFF header is not formally standardized, some deviations in the IP address format may occur. Additionally, NGWAF does not validate the IP address format presented in this header; instead, it parses the content and logs it.

- **Session ID**

  The HTTP/HTTPS session ID associated with the event provides valuable contextual information about each session. Logging the session ID helps in troubleshooting issues and improving security analysis.

  New fields **`SessionID`** and **`Session ID`** are added to the Syslog and CEF formats, respectively, to display the session ID associated with the event.

Log Samples

The following log samples include the Real Source IP address and the Session ID:

Syslog format:

```
2024-02-20T18:01:25-05:00 1406_nonFTA a10logd: [WAF]&lt;3&gt; request
blocked by ng-waf for SIP 11.0.0.1 SPort 46892 RealSource 10.23.14.13 DIP
11.0.0.33 DPort 443 Attack SUSPECTED-BOT,site.tanmayee-test-002,BLOCKED
Hostname 11.0.0.33 URI /tanmayee-test-002 SessionID
65d4e8f51dfb008fc1a2893a
```

CEF format:

```
2024-02-20T18:05:37-05:00 1406_nonFTA  CEF:0|A10|SSLI|6.0.4-
d|909727124728840200|HTTP request is blocked by ng-waf|5|src=11.0.0.1
spt=40514 cs1=10.23.14.13 cs1Label=Real Source dst=11.0.0.33 dpt=443
cs2=SUSPECTED-BOT,site.tanmayee-test-002,BLOCKED cs2Label=Attack Type
cs3=11.0.0.33 cs3Label=Hostname cs4=/tanmayee-test-002 cs4Label=URI
cs5=65d4e9f11dfb008fc1a2893b cs5Label=Session ID
```

See Also:

- Next-Gen WAF Configuration Guide

Scaleout

ACOS 6.0.4 introduces the following new feature and enhancement for Scaleout:

The following topic is covered:

Handling RADIUS Messages with Scaleout Traffic Slices

ACOS supports RADIUS (Remote Authentication Dial-In User Service) message distribution with traffic slices to enhance traffic distribution and ensure consistency and reliability of accounting sessions.

The RADIUS message support is enhanced to:

- Enable traffic slice support for RADIUS messages across network nodes.
- Ensure scalability in mixed IPv4/IPv6 environments.
- Manage RADIUS messages in CGN/FW.
- Redirect RADIUS messages within the Scaleout clusters.
- Synchronize RADIUS SMP sessions across clusters.

When a RADIUS message is received on a node, ACOS identifies the traffic map associated with the IP address (IPv4 or IPv6) and checks the active status of the node using a class-list lookup. If the node is not the active node, the message is redirected to the active node for processing. On the active node, a Session Management

Protocol (SMP) entry is created based on the content of the RADIUS message, and the same SMP entry is synchronized to the standby node.

In multi-PU, the packets are processed on the appropriate PU based on the status of the client IP (odd/even) and the status (odd/even) of the RADIUS message's IP addresses (IPv4 and/or IPv6).

Limitation

If a RADIUS message has an IPv6 address prefix, the prefix-length must be consistent across all RADIUS messages. In addition, it should be equal to or greater than the “system ipv6-prefix-length” configuration to ensure the message is redirected to the correct node.

See Also:

- Scaleout Configuration Guide

SSL Insight

ACOS 6.0.4 introduces the following new feature and enhancement for SSL Insight (SSLi):

The following topic is covered:

Introduced JA4+ TLS Fingerprinting

ACOS introduced TLS fingerprinting with JA4+, also known as the 'JA4+ SSL Client Fingerprint' method, as a successor to the JA3 TLS fingerprinting. JA4+ analyzes the TLS Client Hello packet to build a fingerprint for the client based on various attributes within the packet.

This method utilizes fingerprinting techniques that are both human and machine-readable, aiding in prevention and detection of various attacks, such as:

- Malware, revere shell, or DDoS detection
- Threat actor scanning and grouping

- Session hijacking prevention

ACOS provides the following key features:

- **Insert and forward JA4+ fingerprinting** - When the connection is established the JA4+ fingerprint record is inserted in the HTTP request header and forwarded to the backend server.
- **Reject connections for malicious fingerprinting** - If the JA4+ TLS client fingerprint matches a known list of malicious fingerprints, the connection will be rejected.
- **Reject connections for IP-based fingerprinting** - If a specific IP address generates more than a certain number of different JA4+ fingerprints, the connection will be rejected.

CLI Configuration

The following commands are introduced in the SLB template client-SSL to implement JA4+ fingerprinting.

- To enable the JA4+ feature, use the following commands:

```
ACOS(config)#slb template client-ssl SSLI
ACOS(config-client ssl)#ja4-enable
```

- To insert the JA4 hash into the request as a HTTP header, use the following commands:

```
ACOS(config)#slb template client-ssl SSLI
ACOS(config-client ssl)#ja4-enable
ACOS(config-client ssl)#ja4-insert-http-header <string, length> {X-
JA4}
```

- To reject TLS connections by class-list, use the following commands:

```
ACOS(config)#slb template client-ssl SSLI
ACOS(config-client ssl)#ja4-enable
ACOS(config-client ssl)#ja4-reject-class-list reject_class
```

- To reject TLS connection based on the amount client address, use the following commands:

```
ACOS(config)#slb template client-ssl SSLI
ACOS(config-client ssl)#ja4-enable
ACOS(config-client ssl)#ja4-reject-max-number-per-host 2 ttl 30
```

Show Command

To view the current amount of JA4+ fingerprints of each address, use the `show slb ssl-ja4` command.

See Also:

- SSL Insight Configuration Guide
- Command Line Interface Reference

Platforms

ACOS 6.0.4 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

Introduced Thunder 1060 Platforms

Thunder 1060(S) and 1060-C has been introduced as the newly supported next generation entry level non-FTA platform. These platforms are designed to support ADC, SSLi, and TPS deployments.

Additionally, this platform provides flexible bandwidth tiers through modular licensing to scale your network capacity as needed. Both Modular Perpetual and Modular Subscription licensing models.

See Also:

- A10 TH1060S Installation Reference Guide
- Platform Support Information
- Global Licensing Manager

Enhanced Thunder 8665(S) Platform

Thunder 8665(S), a high-end 6th-generation FTA platform has been optimized for TPS deployments. It is a high-performance multiple processing unit (multi-PU) platform built for large-scale traffic distribution, and scalability in an L3 asymmetric deployment.

See Also:

- TH8665S Installation Reference Guide

Modular Licensing Support

Thunder 3350, 3350(S), and 7445 platforms, offer flexible bandwidth tiers through modular licensing to scale your network capacity as needed. Both modular perpetual and modular subscription licensing models are supported on these platforms.

See Also:

- A10 TH3350 Installation Reference Guide
- A10 TH7445 Installation Reference Guide
- Global Licensing Manager

Monitoring and Alert Management for Modular License

ACOS supports monitoring and alert management of the modular license (software-driven license) bandwidth usage for Thunder or vThunder devices. This feature provides SNMP messages and Syslog logging when the device's bandwidth usage exceeds the default set threshold. The `axSystemBandwidthThresholdAlert trap` is provided to support this feature.

When you enable a modular license on the device and upgrade the ACOS software image to 6.0.4, the device automatically sets the following threshold:

- Warning Threshold: When bandwidth usage reaches 75% and persists for 7 consecutive days, the SNMP and Syslog messages are triggered.
- Critical Threshold: When bandwidth usage reaches 95% and persists for two consecutive days, the SNMP and Syslog messages are triggered.

These threshold can be customized based on your business need. An emergency alert is generated when bandwidth usage hits 100%, which is regarded as an emergency threshold and its value cannot be modified.

CLI Configuration

- To modify the warning threshold percentage, use the following command:

```
ACOS(config)# system bandwidth warning-threshold <50-80>
```

- To modify the critical threshold percentage, use the following command:

```
ACOS(config)# system bandwidth critical-threshold <81-99>
```

Limitation

ACOS does not provide a detailed analysis of the traffic causing bandwidth spikes. The alerts messages only display the time of the threshold being exceeded and the percentage of bandwidth consumption.

See Also

- Event Logging Guide
- System Configuration and Administrator Guide
- Command Line Interface Reference
- Global Licensing Manager

Enhanced vThunder Failover in Azure High Availability

The failover process between vThunder instances in an Azure High Availability configuration has been enhanced. The fault-tolerance of the ACOS failover process is improved during IP address migration across vThunder instances.

See Also:

- Installing vThunder on Microsoft Azure

ACOS GUI Enhancement

ACOS GUI has improved the user experience by displaying the device name or hostname alongside the ACOS version in the top right corner of the page. Previously, the device name or hostname was only visible on the browser tab, which could become unreadable with multiple tabs open. This change helps users easily identify the Thunder device that they are managing.

For more information, see *ACOS Online Help*.

Support High Availability Across Different Availability Zones in vThunder AWS

ACOS supports the configuration of vThunder instances in High Availability (HA) mode across different availability zones (AZ) within the same VPC of an AWS region. This enhancement uses Virtual Router Redundancy Protocol (VRRP) to enable continuous availability of vThunder instances and minimize downtime during fail-over.

The following options are available for HA fail-over deployment across different availability zones:

- Elastic IP address
- Private (Alien) IP address

This enhancement supports only IPv4 addresses and allows a maximum of two vThunder instances with shared partition.

CLI Configuration

To configure HA-failover for vThunder instances across different Availability Zone (AZ) using Elastic IP address:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#multi-az-failover
ACOS(config-cloud-provider-aws-multi-az-f...)#vrid num
ACOS(config-cloud-provider-aws-multi-az-f...)#vip-interface-id name
ACOS(config-cloud-provider-aws-multi-az-f...)#vip num
ACOS(config-cloud-provider-aws-multi-az-f...)#private-ip IP_address
ACOS(config-cloud-provider-aws-multi-az-f...)#elastic-ip IP_address
```

To configure HA-failover for vThunder instances across different Availability Zone (AZ) using Private (Alien) IP address:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#multi-az-failover
ACOS(config-cloud-provider-aws-multi-az-f...)#vrid num
ACOS(config-cloud-provider-aws-multi-az-f...)#route-table-id name
ACOS(config-cloud-provider-aws-multi-az-f...)#vip-interface-id name
ACOS(config-cloud-provider-aws-multi-az-f...)#fip-interface-id name
ACOS(config-cloud-provider-aws-multi-az-f...)#vip-dest name
ACOS(config-cloud-provider-aws-multi-az-f...)#fip-dest name
```

Limitations

- Multiple partitions are not supported.
- HA fail-over using Elastic IP addresses may not support L4 (TCP) connection/session synchronization.
- HA fail-over using Private IP addresses may not support traffic originating from the public internet.
- Source NAT auto is not supported in SLB virtual server configuration.

See Also:

- Installing vThunder on AWS
- Command Line Interface Reference

Threat Protection System

ACOS 6.0.4 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to DDoS Mitigation Guide. Similarly, for TPS-related CLI commands, refer to DDoS Command Line Reference Guide.

Security Updates

The following security vulnerabilities are addressed in this release:

OpenSSL Vulnerabilities

- CVE-2023-3446 and CVE-2023-3817: A vulnerability with applications using DH_ check(), DH_check_ex(), or EVP_PKEY_param_check() functions to check a DH key or DH parameters that experienced long delays during the process.
- CVE-2023-5678: The vulnerability related to slow generation or checking of long X9.42 DH keys, causing a low-severity denial-of-service risk.
- CVE-2024-0727: OpenSSL vulnerability in processing the PKCS12 files may allow for potential Denial of Service attacks via NULL pointer dereference.
- CVE-2022-38023: Netlogon RPC Elevation of Privilege Vulnerability in Samba 3.0.37 may allow attackers to exploit weak RC4-HMAC encryption.

A10 Vulnerabilities

- A10-2023-0008: The vulnerability in the A10 ACOS CLI that allows unauthorized users to gain "root" access to the underlying operating system. Any authenticated user can run the health-monitor scripts potentially exploiting the external health function, which presents a serious security concern.
- A10-2023-0015: A vulnerability that allows recovery of an encryption key in ACOS that could decrypt firmware upgrades/backups, compromising system security.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.3-P2

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.3-P2 release:

The following topics are covered:

Application Access Management

ACOS 6.0.3 introduces the following new feature and enhancement for Application Access Management (AAM):

The following topic is covered:

ECDSA Digital Signatures for JWT-Based Explicit Proxy

ACOS supports the ES256 cryptographic technique for verifying JSON Web Tokens (JWTs) within a JWT-based explicit proxy to enhance the security.

ES256, or Elliptic Curve Digital Signature Algorithm (ECDSA) using P-256 and SHA-256, is based on elliptic curve cryptography that offers strong security with smaller key sizes compared to the RSA-based algorithms. This ensures efficient and robust authentication and data integrity validation.

CLI Configuration

To utilize the ES256 (ECDSA-based) JWT file, you must first import it using the

import command. Subsequently, you need to configure a JWT authorization template to employ the file for verifying the signatures of incoming JWTs:

```
ACOS(config)# import auth-jwks jwk_file scp://john@192.168.92.54:/jwk_
file
ACOS(config)# aam jwt-authorization test
ACOS(config-jwt-authz:test)# verification-jwks jwk_file
```

NOTE: After a system downgrade, if the ACOS version does not support ECDSA-based JWK, any existing ES256-based key will continue to remain in the system. However, it will no longer be utilized by the **aam jwt-authorization** command.

See Also:

- 'JWT (JSON Web Token) Authorization (AAM with JWT)' section in the *Application Access Management Guide*.

Firewall

ACOS 6.0.3-P2 introduces the following new feature and enhancement for Firewall:

The following topic is covered:

Disabling CEF Labels in the Syslog

Firewall logging uses the CEF format, which results in the size of each CEF log being larger as compared to the Syslog format. To optimize log management, and enhance efficiency and readability, the **fw logging cef-label** command is introduced. This command allows you to enable or disable including CEF label definitions in the Syslog, thereby resulting in a smaller log size.

This command is enabled by default, meaning all CEF labels are included by default. However, when it is disabled, all CEF labels are suppressed in the Syslog.

CLI Configuration

To suppress all CEF labels in the Syslog, configure the following command:

```
ACOS(config)# fw logging cef-label disable
```

See Also:

- 'Disabling CEF Labels in the Syslog' section in the *Firewall Configuration Guide*.
- 'fw logging' command in the *Command Line Interface Reference*.

Application Delivery Controller

ACOS 6.0.3-P2 introduces the following new features and enhancements for Application Delivery Controller (ADC):

The following topics are covered:

DNS Queries Per Second Logging

ACOS introduces support for logging the DNS Queries Per Second (QPS) by calculating the DNS QPS value per virtual port (vport) in the SLB DNS template. This feature allows to configure high and low QPS value thresholds and enable event logging and SNMP traps. When the QPS value exceeds configured high threshold, drops below the configured low threshold, or returns to a normal level, the system generates event logs and SNMP traps based on the current QPS value.

This enhancement supports only DNS over UDP (dns-udp), DNS over TCP (dns-tcp), and DNS over HTTP/HTTPS (doh) virtual ports. It applies to all SNMP versions.

Event Logs

The following three event logs are added for this feature:

Event Log	Description
Below low threshold	The QPS value drops below the configured low threshold value.
Back to normal level	The QPS value returns to normal value from high or low threshold value.
Above high threshold	The QPS value exceeds the configured high threshold value.

SNMP OID

The following four SNMP OIDs are added:

Event Type	Description	SNMP OID
Normal to high event	Transition from normal QPS level to high QPS level.	1.3.6.1.4.1.22610.2.4.3.12.2.6.13
High to normal event	Transition from high QPS level to normal QPS level.	1.3.6.1.4.1.22610.2.4.3.12.2.6.14
Normal to low event	Transition from normal QPS level to low QPS level.	1.3.6.1.4.1.22610.2.4.3.12.2.6.15
Low to normal event	Transition from low QPS level to normal QPS level.	1.3.6.1.4.1.22610.2.4.3.12.2.6.16

CLI configuration

- To configure QPS high and low threshold values, use the following commands:

```
ACOS(config)# slb template dns template_name
ACOS(config-dns)# query-rate-monitoring threshold-log high num low num
```

  With this configuration, the system starts calculating the current QPS value. The high threshold value is must be greater than the low threshold value.

- To enable event logging only for DNS QPS monitoring, use the following commands:

```
ACOS(config)# slb template dns template_name
ACOS(config-dns)# query-rate-monitoring threshold-log high num low num
enable
```

With this configuration, the system enables the generation of the event-logs whenever QPS value crosses the configured high and low threshold.

- To enable SNMP trap only for DNS QPS monitoring, use the following commands:

```
ACOS(config)# slb template dns template_name
ACOS(config-dns)# query-rate-monitoring threshold-log high num low num
ACOS(config-dns)# exit
ACOS(config)# snmp-server enable traps slb vip-port-qps
```

With **slb vip-port-qps** option enabled, the SNMP traps are triggered during threshold events only if the virtual port is associated with a DNS template and the high/low values for QPS monitoring in that template are configured.

- To enable event logging with SNMP trap for DNS QPS monitoring, use the following commands:

```
ACOS(config)# slb template dns template_name
ACOS(config-dns)# query-rate-monitoring threshold-log high num low num
enable
ACOS(config-dns)# exit
ACOS(config)# snmp-server enable traps slb vip-port-qps
```

Limitation

Low-latency mode is not supported.

See Also:

- 'DNS Queries per Second Logging' section in the *Application Delivery Controller Guide*.
- 'slb template DNS' and 'snmp-server enable traps' commands in the *Command Line Interface Reference*.

Real-Time Monitoring of DNS QPS and Cache Hit Rate

With this release, ACOS has introduced the capability to display the rate of current DNS Queries (QPS) and DNS cache hits when required. For this display, the DNS cache must be enabled. This feature provides flexibility and offers an instant and granular view on the DNS cache hits and DNS query rate (QPS).

CLI Configuration

To view the DNS QPS and DNS cache hit rate, use the following show command:

```
ACOS(config)#show dns rate
```

The following sample indicates the response of the `show dns rate` command:

```
Query rate(QPS) : 50 per second
Cache hit       : 41 per second
Cache hit ratio : 82% (cache hit/Query)
```

Limitations

- While retrieving the current DNS query rate (QPS) and DNS cache hit rate, the CLI momentarily pauses for one second. This brief pause halts the processing of CLI commands to gather real-time and accurate data on DNS QPS and DNS cache hit rate.
- The feature does not support L4 TCP port.

See Also:

- 'Display DNS Cache Hits and DNS Query Rate' section in the *Application Delivery Controller Guide*.
- 'show dns rate' command in the *Command Line Interface Reference*.

New counters for DNS RCODE and TSIG Error Codes

ACOS provides enhanced visibility and monitoring capabilities for DNS and Transaction Signature (TSIG) errors encountered during TSIG-enabled operations. The following new counters are added to monitor the occurrences of Response Codes (RCODEs) and TSIG-related error conditions within DNS transactions:

- DNS RCODE (RFC 2136): NOTZONE
- TSIG Error Codes (RFC 8945): BADSIG, BADKEY, BADTIME, BADTRUNC

This feature is supported for SLB virtual ports DNS over UDP (dns-udp) and DNS over TCP (dns-tcp) when the SLB DNS template is bound to these virtual ports.

Show command

To view the new counters for DNS RCODEs and TSIG error codes, use the following show command:

```
ACOS(config)# show slb virtual-server <VIP_name> <port-num> <port-type>
application-statistics extended
...
...
===Extended Statistics===
...
...
Rcode FORMERR Received:                          0
Rcode SERVERERR Received:                        0
Rcode NXDOMAIN Received:                         0
Rcode NOTIMPL Received:                          0
Rcode REFUSE Received:                           0
Rcode YXDOMAIN Received:                         0
Rcode YXRRSET Received:                          0
Rcode NXRRSET Received:                          0
Rcode NOTAUTH Received:                          0
Rcode NOTZONE Received:                          0
Rcode DSOTYPEN Received:                         0
Rcode OTHER VALUE Received:                      0
TSIG Rcode BADSIG Received:                      0
TSIG Rcode BADKEY Received:                      0
TSIG Rcode BADTIME Received:                     0
TSIG Rcode BADTRUNC Received:                    0
EDNS Query Type NSID:                            0
EDNS Query Type DAU:                             0
```

See Also:

- 'show slb virtual-server' command in the *Command Line Interface Reference*.

Enhanced Health Monitoring with Extended Up-Retry Value

In this enhancement, the maximum up-retry value for the health monitor feature is increased from 10 to 63. The up-retry value determines the number of attempts the ACOS makes to check the health status of a service before marking it as available.

The enhancement provides flexibility to set a higher timer value for services. Moreover, it is useful in cases where a server experiences intermittent downtime, causing client requests to get blackholed. When the time interval is increased, ACOS ensures that the client requests are properly served by extending the duration before marking a server as 'Up'.

CLI Configuration

To configure the maximum up-retry value, use the following commands:

```
ACOS(config)#health monitor hm
ACOS(config-health:monitor)#up-retry 63
```

The system will retry health checks up to 63 times before marking the monitored service as available if it responds successfully.

See Also:

- 'Health Monitoring' section in the *Application Delivery Controller Guide*.
- 'health monitor' command in the *Command Line Interface Reference*.

Scaleout

ACOS 6.0.3-P2 introduces the following new feature and enhancement for Scaleout:

The following topic is covered:

Multiple Traffic Slices Support

Traffic slice mapping is the process of distributing network traffic into separate segments (or slices) based on specific criteria such as application type, user group, or

network policy. Scaleout functionality has been enhanced by adding the following capabilities:

- Smaller NAT pools can now be supported for a subset of subscribers identified by binding a service-group-template config. Previously each NAT pool required to minimally be a /24 subnet. This applies only to NAT-related traffic.
- Added support for a configurable user-group count. A different user-group count can be configured for shared and L3V partitions. This helps with more granular subscriber NAT management. This applies to both NAT and FW traffic in the cluster.
- Introduced dedicated tracking templates for IPv4 and IPv6 for precise traffic map adjustments. This allows for a given node to continue handling traffic for one protocol family (IPv4 or IPv6) while switching to a different node for the other in case of protocol specific path failures in the network. This applies to both NAT and FW traffic in the cluster.
- Improved route-map matching options for IPv4 and IPv6 Scaleout states based on corresponding tracking template states. This applies to both NAT and FW traffic in the cluster.

CLI Configurations

- To match the ipv4/ipv6 specific state based on the relevant tracking template, the ipv4/ipv6 options are added under the `match scaleout` command:

```
ACOS(config)# match scaleout cluster-id [ipv4 | ipv6] {up | down}
```

- To configure IPv4 and IPv6 specific tracking template to be used by Scaleout, the following command is added under the `tracking template` command:

```
ACOS(config)# tracking-template [multi-template <name> | template
<name> [ipv4 | ipv6]]
```

Show Commands

The `show scaleout` output is further enhanced to:

- Display the Scaleout member nodes for IPv4 or IPv6 and the status of both IPv4 and IPv6 Scaleout node.

The `show scaleout traffic-map` output is further enhanced to:

- Display the default IPv4 Traffic Map and all service-config template Traffic Maps along with the default IPv6 Traffic Map.
- Display the traffic map for IPv4 traffic.
- Display the traffic map for IPv6 traffic.
- Specify the traffic map for the specified service-config template.

Limitations

- The Exit-Cluster will only be supported for the default template in the shared partition.
- The IPv4/IPv6 option cannot be changed dynamically. The tracking template must be removed and readded with the required option.
- Inter-partition references to Scaleout configurations such as tracking templates, user groups, and so on are not supported - all L3Vs are separate.
- When the user-group count at per partition or within a traffic slice is changed, you must clear all sessions or reload/reboot the device.
- On the multi-PU platform, the minimum user-group-count that can be configured is 2.
- When the LSN NAT Pools for Fixed NAT are configured in the shared partition or any L3V has an explicit ‘default-user-group-count’ configured, the user-group count in the shared partition cannot be modified.
- When the LSN NAT Pools for Fixed NAT are configured in the L3V partition, the user-group count in the L3V partition cannot be modified.

See Also:

- The following sections in the *Scaleout Configuration Guide*.
  - Service-Config Template
  - User Group
  - Configure Service-Config Template
  - Configure User Group

- Configure Policy-Based Failover - Overview
- Use Route Map to Withdraw or Redistribute Routes

- The following commands in the *Command Line Interface Reference*.
  - tracking-template
  - match scaleout
  - user-group-count

Platforms

ACOS 6.0.3-P2 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

Introduced Thunder 8665(S) Platform

Thunder 8665(S) has been introduced as the newly supported high-end 6th-generation FTA platform for CGN and GiFW deployments only. It is a high-performance Multiple Processing Unit (multi-PU) platform built for large-scale traffic distribution, load balancing, and scalability.

Additionally, the Thunder 8665S platform supports a second management port to enhance reliability. Each port can be configured separately and operates independently of the other. The first management port name is unchanged: 'management' or 'mgmt.' The second management port is named: 'management2' or 'mgmt2.'

The second management port supports the following capabilities:

- Configuring IPv4 and IPv6 addresses.
- Setting default route to different subnet and default gateway.
- Configuring IPv4 and IPv6 ACLs.

CLI Configuration

- To configure the IPv4 access and default gateway on the second management interface, use the following command:

```
ACOS(config)# interface management2
ACOS(config-if:management2)# ip address 192.168.10.2 /24
ACOS(config-if:management2)# ip default-gateway 192.168.10.1
```

- To configure the IPv6 access and default gateway on the second management interface, use the following command:

```
ACOS(config)# interface management2
ACOS(config-if:management2)# ipv6 address 2001:db8::2/32
ACOS(config-if:management2)# ipv6 default-gateway 2001:db8::1
```

Show Commands

The following show commands are enhanced to provide the details about the second management interface:

- **`show interfaces management2`**
- **`show interfaces brief`**
- **`show ip route`** and **`show ipv6 route`**

See Also:

- TH8665S Installation Reference Guide.
- 'Configuring Dual Management Interface' section in the *System Configuration and Administration Guide*.
- 'Platforms Support Information' in the *Release Notes*.
- 'interface' command in the *Command Line Interface Reference*.

Compatibility Enhancement in Bare Metal Platform

The compatibility of NIC and QAT models has been extended for Bare Metal platform.

Vendor/Model	NIC
Super Micro X13 servers	• Mellanox ConnectX-6 Lx 25/10G • Mellenox Connect-X 6 Dx 100GbE

NOTE: Tested with Super Micro server Model - SYS-621C-TN12R.

Compatibility Enhancement in vThunder VMware ESXi 8.0

The compatibility of NIC and Quick Assist Technology (QAT) models has been extended for vThunder ADC and Gi-FW managed by VMware ESXi 8.0.

Vendor	NIC	QAT
Super Micro X13 servers	• Mellanox ConnectX-6 Lx 25/10G • Mellanox ConnectX-6 Dx 100GbE • Intel E810 10/25/100 GbE • Intel X710 10/25/40 GbE	Intel 8970 Chipset or later

Dell Next Gen Thunder Multi-Tenant Virtual Platform (MVP) Manager Enhancements

The following enhancements are available in the Dell Next Gen Thunder Multi-Tenant Virtual Platform (MVP) Manager:

- Support Intel Quick Assist Technology (on-chip QAT) Hardware 2.0.
- MVP-Cockpit enhancements,
  - Web console connection accepted both on port-9090 and port-443.
  - “Import VM” option is renamed to “Create VM”.

See Also:

- 'Virtual Machines' section in the *Dell Next Gen Thunder Multi-tenant Virtual Platform (MVP) Manager*.

Security Updates

The following security A10 vulnerabilities are addressed in the ACOS 6.0.3-P2 release:

- A10-2024-0001: A vulnerability related to a system using a weak ssh-rsa algorithm (HostKeyAlgorithms).
- A10-2023-0014: A vulnerability that allows unauthorized users to overwrite files with root privileges, leading to system compromise.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.3-P1

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.3-P1 release:

The following topics are covered:

Application Delivery Controller

ACOS 6.0.3-P1 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC-specific configuration steps, refer *Application Delivery and Server Load Balancing Guide*. Similarly, for ADC-specific CLI commands, refer *Command Line Reference Guide*.

The following topics are covered:

DNS Filtering using Web Categories

ACOS has leveraged Webroot's website classification data to implement a flexible and scalable DNS filtering technique. ACOS DNS filtering is introduced to protect against potential security risks, comply with regulations, enforce corporate policies and implement parental controls by blocking access to malicious websites.

DNS filtering prevents users from accessing specific websites or online content by blocking requests to specific domains based on predefined criteria.

ACOS DNS filtering (using web categories), can be configured using the SLB DNS template **category-lookup** command to check the requested domain against Webroot's web categories and determine the action to be taken based on the configuration. If the requested domain falls into an allowed category, the DNS request is allowed to proceed. However, if the request falls into a blocked category, it is either dropped or redirected.

NOTE: You need to download and install the Webroot's web classification database on the system. The Webroot license must be installed and enabled before utilizing the database.

CLI Configuration

- To implement DNS filtering using web categories, you need to create web category lists and configure the actions to be taken when the DNS request matches a category from the list. Configure the **category-lookup** command under the SLB DNS template to set the actions **permit**, **drop**, or **respond** for the web lists.

```
ACOS(config)# slb template dnsdns_temp
ACOS(config-dns)# category-lookup <web-category-list> [ permit | drop | respond ]
```

NOTE:

  - The **category-lookup** command applies to all types of DNS, including Recursive Resolver.
  - You can configure up to eight category lists under the same DNS template.

- To enable online lookup, configure the **category-lookup-online-lookup** command under the SLB DNS template. By default, the system first checks the locally downloaded web classification database for domain matching.

```
ACOS(config)# slb template dnsdns_temp
ACOS(config-dns)# category-lookup-online-lookup
```

- To bypass a specific domain during DNS filtering, create a DNS type class list and

configure the **category-lookup-online-lookup** command under the SLB DNS template:

```
ACOS(config)# slb template dns dns_temp
ACOS(config-dns)# category-lookup-bypass <dns-type-list>
```

NOTE: DNS filtering (using Webroot categories) can also be configured using aFleX. However, the DNS template configuration takes precedence over aFleX, meaning ACOS checks and executes the DNS template configurations before aFleX. Consequently, if the template configuration executes the **respond** or **drop** action, the request is not processed further i.e., aFleX processing is bypassed. However, if the template configuration permits the request, ACOS proceeds with the aFleX configuration.

Show Commands

- To view the counters specific to a web category in the category list, execute the following show command:

```
ACOS(config)# show counters web-category category-listweb-category-list
```

- To view DNS queries' statistics based on web categories, execute the following show command:

```
ACOS(config)# show slb virtual-server vip53dns-udp application-statistics
```

Enhanced DNS Cache Functionality

The DNS cache functionality is enhanced to operate with class-lists when the global cache is enabled. ACOS now checks the class-list configurations for specific policies or limits mapped to the LID/GLID and then applies them to the incoming traffic.

This enhancement introduces the following capabilities, previously available for DNS Caching only when the global cache was disabled:

- Allows DNS cache bypass based on domain names and/or source IPv4/IPv6 address
- Enables connection rate limit based on limit identifiers (LID/GLID)

- Provides TTL (Time-to-Live) entry management capabilities.

This functionality helps to mitigate potentially high query rate attacks by restricting the volume of queries forwarded to DNS servers and to prevent reflection/amplification attacks by restricting the number of identical queries allowed per class-list.

Supported Features

- Shared and Private L3V partitions
- All types of DNS servers including Recursive Resolver
- DNS-UDP and DNS-TCP type virtual server ports
- DNS, FILE, IPv4, and IPv6 type class-lists.

CLI Configuration

To configure DNS caching with global DNS cache, a new command **global-dns-cache** is introduced in the SLB global configuration. This command allows you to configure various DNS caching parameters, such as connection rate limits, enabling or disabling DNS cache, and specifying over-limit actions for specific LID/GLID identifiers:

```
ACOS(config)# slb common
ACOS(config-common)# global-dns-cache
ACOS(config-common-global-dns-cache)# class-list cl_dns_cache
ACOS(config-common-global-dns-cache-class…)# lid 1
ACOS(config-common-global-dns-cache-class…)# conn-rate-limit 10000 per
10
ACOS(config-common-global-dns-cache-class…)# dns cache-enable
ACOS(config-common-global-dns-cache-class…)# over-limit-action drop
lockout 10
ACOS(config-common-global-dns-cache-class…)# user-tag dns_cache_bypass
```

For more information on the CLI commands, see *Command Line Reference Guide*.

Limitation

When the ACOS device is running recursive resolution, DNS responses from internet servers during resolution and/or populated Name Server and A/AAAA cache entries are not supported.

For more information on the global DNS cache configuration, see *Application Delivery and Server Load Balancing Guide*.

Enhanced Response to Server Selection Failure

ACOS has enhanced the response mechanism for server selection failures resulting from client requests during HTTP load-balancing. Now, when a configured server is down or unable to respond to a client's GET request, ACOS returns the HTTP 504 Gateway Timeout error. This enhancement improves the client experience by clearly indicating that the server is not reachable and cannot complete the request.

This feature supports the HTTP/1.1 and HTTP/2 protocols. It is applicable only to HTTP and HTTPS virtual ports.

CLI Configuration

The `when-server-selection-failed send-504` command is introduced in the HTTP or HTTPS virtual port configuration.

```
ACOS(config)#slb virtual-server vs
ACOS(config-slb vserver)#port 80 http
ACOS(config-slb vserver-vport)#service-group sg test
ACOS(config-slb vserver-vport)#when-server-selection-failed send-504
```

The new command is exclusive to the existing command `reset-on-server-selection-fail`.

For details on the configuration, see the *Application Delivery and Server Load Balancing Guide*.

Platforms

ACOS 6.0.3-P1 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

Support for Oracle Cloud Infrastructure

Starting with ACOS 6.0.3-P1, the following vThunder instances are supported for Oracle Cloud Infrastructure (OCI):

- High Availability (HA) mode within vThunders is deployed in OCI for a single availability zone.
- Creating templates using the Terraform tool, deploy OCI VMs (Compute Instances), and configuring ADC templates using the GUI configuration builder.
- All the legacy features such as Health monitors, SLB, SNMP, and so on of ADC that are supported on vThunders are also supported for OCI.
- TPS legacy features such as DDoS, ipfiltering, glid, zone-template, src-based policy, and capture config are supported for OCI VMs.
- VM.Standard3.Flex instance type
- Global Server Load Balancing (GSLB)
- HA mode across availability zone (availability domains in OCI parlance)

Security Updates

The following security vulnerability is addressed in the ACOS 6.0.3-P1 release:

- A10 Vulnerabilities:
  - A10-2023-0009: The vulnerability allows unauthorized users to exploit the A10 ACOS CLI health monitor functionality, potentially leading to unauthorized access and data exfiltration.
  - A10-2023-0010: The vulnerability in A10 ACOS CLI allows unauthorized access and potential exfiltration of files, including files restricted to superuser (root).
  - A10-2023-0020 and A10-2023-0021: The vulnerabilities involve Remote Code Execution and Local Privilege Escalation, potentially allowing high-privileged users to escalate their privileges to root when exploited.

- OpenSSL Vulnerability:
  - CVE-2023-5678: The vulnerability related to slow generation or checking of long X9.42 DH keys, causing a low-severity denial-of-service risk.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.3

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.3 release:

The following topics are covered:

Application Access Management

ACOS 6.0.3 introduces the following new feature and enhancement for Application Access Management (AAM):

NOTE: For AAM specific configuration steps, refer *Application Access Management Guide*.

The following topic is covered:

SAML Authentication with Kerberos Relay

Starting with ACOS 6.0.3, the SAML authentication with Kerberos relay feature provides the capability to integrate Microsoft Azure Active Directory (AD) with AAM SAML authentication and on-premises Exchange 2019 with Kerberos authentication.

The **username-attribute** option under the **aam authentication saml service-provider** command identifies and differentiates individual users within the database. It retrieves the username used in Kerberos relay and allows the access for both on-premises Exchange 2019 and Microsoft Azure Active Directory (AD) through Single Sign-on.

CLI Configuration

The **username-attribute**option is introduced in the the **aam authentication saml service-provider** command to identify and differentiate individual users within the database.

```
ACOS(config)#aam authentication saml service-provider <provider-name>
ACOS(config-SAML saml service-provider AD_SAML_SSO_SP)# username-attribute <username>
```

NOTE: The user account name must be the same in Azure AD and Exchange 2019 to support the Kerberos relay method.

For detailed commands and their implementation, see the *Command Line Interface Reference* and *Application Access Management Guide*.

Application Delivery Controller

ACOS 6.0.3 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC-specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for ADC-specific CLI commands, refer *Command Line Reference Guide*.

The following topics are covered:

Introduced ACL Support with Normal VIPs

ACOS supports the association of Access Control Lists (ACL) with normal VIPs. This feature helps when the maximum number of supported wildcard VIPs is not enough. To overcome the limitation, the destination IP in ACL can be transferred to the VIP, and the VIP acts as a non-wildcard VIP bound to an ACL. The source IP defined in the associated ACL continues to determine if the traffic matches the specified virtual port, while the IP address defined for the VIP determines the traffic destination.

This enhancement has the following features:

- You can configure multiple normal VIPs associated with ACLs while ensuring that the search performance does not degrade as the number of virtual servers increases. The maximum configurable number of VIPs depends on the platform and system memory size and is greater than the maximum configurable number of wildcard VIPs.
- You can continue to configure upto 200 or more wildcard VIPs associated with ACLs along with the normal VIP configuration. For details on the supported number of wildcard VIPs, see *Application Delivery Controller Guide*.
- If there are multiple VIPs with ACL configured with the same IP in the system, incoming traffic will match only one of the VIP and will be rejected by other VIPs.
- If traffic does not match any virtual port in a VIP with ACL, then ACOS tries to match the virtual port in other VIPs or if there are no matching VIPs, then in a wildcard VIP.
- It supports both IPv4 and IPv6.

NOTE: The ACL associated with the VIP should not contain any destination IP.

For details on the configuration, see the *Application Delivery and Server Load Balancing Guide*.

CLI Configuration

The following example is the configuration of a normal VIP with ACL:

```
ACOS(config)# slb virtual-server vserver2 10.190.7.10 acl name myacl2
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# service-group wbgroup2
ACOS(config-slb vserver-vport)# no-dest-nat
```

Limitations

- This feature is only supported for slow paths.
- Subnet VIPs cannot be associated with an ACL.
- The matching order for VIPs with ACL having the same IP address is not guaranteed. The matching does not follow the alphabetic order of ACL, the way it is done in wildcard VIPs.

Support for Parallel Queries in Recursive DNS

The DNS recursive resolution feature is now enhanced and supports parallel queries to multiple resolvers. Several queries are concurrently sent to multiple resolvers, and the first response received is used for the next round of resolution. This enhances the lookup process and leads to improved efficiency of recursive resolution. It also makes the lookup process more resilient to timeout issues.

You can specify the range of parallel queries between 1-15. This feature supports both, TCP and UDP protocols.

CLI Configuration

The following command is introduced in the **`slb template dns > recursive-dns-resolution`** command:

```
ACOS(config)#slb template dns test
ACOS(config-dns)#recursive-dns-resolution
ACOS(config-dns-recursive-dns-resolution)#parallel-queries <1-15>
```

Show Commands

The following counters are added to the **`show slb virtual-server v1 53 dns-tcp application-statistics`** command:

```
ACOS(config)#show slb virtual-server vip18 53 dns-tcp app
Recursive Resolution Late Responses:          0  -- response that comes
back without link to client resolver
```

```
Recursive Resolution Parallel Queries UDP:    0
Recursive Resolution Parallel Queries TCP:    0
```

For more information, see the *Application Delivery and Server Load Balancing Guide* and *Command Line Interface Reference Guide*.

Support SSL Session Secret Logging

ACOS supports logging SSL session secrets using an aFlex script. This log file can be exported and used to decrypt packet flows in Wireshark or other network forensic tools. The logged file adheres to the standardized format defined in the IETF Keylog File.

The key benefits of logging and exporting the SSL session secrets are as follows:

- Decrypt and inspect encrypted traffic.
- Identify and analyze security threats.
- Simplify security auditing and regulatory compliance.

Supported Features

- Key Exchange Methods: Rivest-Shamir-Adleman (RSA) and Diffie-Hellman (DH)
- SSL Modules: Intel QuickAssist Technology (QAT), Software TLS 1.3, and Nitrox V (N5) hardware acceleration
- aFlex Events: `CLIENTSSL_HANDSHAKE` and `SERVERSSL_HANDSHAKE`.

aFleX Commands and Events

The following aFlex command is introduced to integrate the SSL session secret logging:

- `SSL::sessionsecret` - This command returns the SSL session secret key for an SSL/TLS connection.

You can configure the aFlex command `SSL::sessionsecret` in the the `CLIENTSSL_HANDSHAKE` and `SERVERSSL_HANDSHAKE` aFlex events. Then bind the aFlex script to the SLB virtual port.

Log Sample

The secrets are logged in hex string format on the Syslog server: **`<label> <client`**

random> <secret>.

```
SERVER_HANDSHAKE_TRAFFIC_SECRET
19acc5019abe56ac3d531fa7f8ef54f57b9bcb3edc14bdadabe51a28d37d9ec4
3cad4c78ae9cad4f73f1b2be0c0b1ebba736107247111b0dc16b392077b233cf822c1ed3
54eb456d28feb2e71e3ea5db
EXPORTER_SECRET
19acc5019abe56ac3d531fa7f8ef54f57b9bcb3edc14bdadabe51a28d37d9ec4
c0fa0ecff7795b9ab9874f5e483abe9444b24de47d29d5cae1aa9be07e07547941715dbf
b93ca4bec178b493390787a1
SERVER_TRAFFIC_SECRET_0
19acc5019abe56ac3d531fa7f8ef54f57b9bcb3edc14bdadabe51a28d37d9ec4
03bfbc47a4c9f9bb22c919450fdcb4992f8f52d1de6bb3c16234f2c02cd9239ba5a54938
a62c6af880f35bb5459f6b1d
CLIENT_HANDSHAKE_TRAFFIC_SECRET
19acc5019abe56ac3d531fa7f8ef54f57b9bcb3edc14bdadabe51a28d37d9ec4
dd949b485c6347a280e48efe2f869133ae4bb85f7b7886ab287f6fb2a5fa6c7c001a0177
851cefa91785431f0e4da438
CLIENT_TRAFFIC_SECRET_0
19acc5019abe56ac3d531fa7f8ef54f57b9bcb3edc14bdadabe51a28d37d9ec4
8b29b981be9eda270297fbe036d461edacf56a3a35fd25b0f6b9df43444cc12ee777876c
6164420bce0a7c5323a5d5f2
```

Limitation

For TLS 1.3, only the first set of application secrets (`CLIENT_TRAFFIC_SECRET_0` and `SERVER_TRAFFIC_SECRET_0`) are logged. Any new secrets generated with TLS 1.3 KeyUpdate are not logged.

- For more information on the aFlex commands, see *aFleX Scripting Language Reference*.
- For more information on the feature, see *SSL Insight Configuration Guide*.

Carrier Grade NAT

ACOS 6.0.3 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

NOTE: For CGN-specific configuration steps, refer *IPv4-to-IPv6 Transition Solutions Guide* and for CGN-specific CLI commands, refer *Command Line Reference Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topics are covered:

Enhanced CGNv6 Domain-list DNS Resolution

When a new TCP connection attempt is received from a Network Address Translation (NAT) client that matches the LSN-Rule-List, the CGNv6 DNS resolution process does not initiate a retry immediately. Instead, it waits for a pre-configured time interval of 10 minutes (known as query interval) before initiating a retry again. This prolonged query interval may result in a disruption of service.

The CGNv6 Domain-list DNS resolution process has been enhanced so that you can configure the query interval and fail-interval for the CGNv6 domain lists at the domain level as well as the global system level. Additionally, you can also disable AAAA query records in the CGNv6 domain-list query, so that only A query records are sent for resolution. These enhancements improve the DNS resolution time and help mitigate service outages.

CLI Configuration

- To configure the query interval and fail-interval at the domain level:

```
ACOS(config)# domain-list <mylist>
ACOS(config-domain-list:mylist)# <domain-name> interval <minutes>
fail-interval <seconds>
```

- To configure the query interval at the global level:

```
ACOS(config)# cgnv6 global domain-list interval <minutes>
```

- To configure the fail-interval at the global level:

```
ACOS(config)# cgnv6 global domain-list fail-interval <seconds>
```

- To disable the AAAA query record for each domain in the CGNv6 domain list:

```
ACOS(config)# cgnv6 global domain-list aaaa-query disable
```

NOTE:

- Global configurations set using the **cgnv6 global domain-list** command are only effective for domains configured with default parameters. This implies that if you explicitly set the query interval and fail-interval at the domain level (using the **domain-list** command), the global configuration will not take effect.
- Ensure that the query interval and fail-interval are configured only once for a specific domain in one domain list. Configuring these parameters in multiple domain lists may result in undefined behavior.

Support to Configure NetFlow Data

ACOS supports fixed and custom templates with different Information Elements (IEs) to export logging information to the collectors. The custom templates do not support the standard NetFlow End Reasons as defined in RFC 5102. Hence, the Netflow collectors have issues using the NetFlow data from ACOS devices.

The `rfc-flow-end-reason` information element is added to the custom templates for compliance with RFC 5102 standards. It provides the flow end reason with the reason codes compliant with RFC 5102. You can continue to use the A10-specific flow-end-reason IE if you want to get a more granular flow end reason as tracked by the A10 device.

NOTE:

- The information element is supported only in the NetFlow version 10.
- The information element is only part of custom templates.

SSL Insight

ACOS 6.0.3 introduces the following new features and enhancements for SSL Insight (SSLi):

NOTE: For SSLi configuration steps, see *SSL Insight Configuration Guide*. Similarly, for SSLi-specific CLI commands, see *Command Line Reference Guide*.

The following topics are covered:

SSLi Deployment Support on One Virtual Port Only

ACOS supports deploying SSLi functionalities on a single virtual port instead of the conventional deployment that involves two VIPs or virtual ports. You can also simultaneously configure SSLi and explicit proxy on the same virtual port in this deployment.

SSLi on a single virtual port deployment allows you to:

- Simplify the configuration and reduce interface utilization.
- Intercept and inspect HTTPS traffic while performing explicit proxy functions.
- Apply aFlex scripts to insert HTTP headers into HTTPS requests.
- Implement URL filtering policies with full URL inspection.

Supported Features

- All basic SSLi functionalities that are available in the client-SSL template.
- SSLi in L2 and L3 modes for both static and dynamic ports.
- Explicit Proxy, transparent Proxy with proxy chaining.
- Software TLS1.3, QAT, and old N5 SSL modules.

Limitation

- ACOS utilizes only the client-SSL configuration to process and forward the traffic. The server-SSL configuration is ignored (except **`forward-proxy-enable`**).
- If you use aFlex for HTTP header insertion, the aFlex commands `SSL::enable serverside` and `SSL::template serverside "ss1"` cannot be used together in the same virtual port (single port deployment).

- The new N5 SSL module is not supported.

For detailed deployment and configuration information, see *SSL Insight Configuration Guide*.

New Categories Introduced in Web Category

The Web category bypass feature of the SSLi solution has been enhanced to accommodate the new online content/URL categories defined by the BrightCloud Web Classification Service. This enhancement provides additional control over what types of websites and content are allowed or blocked within your network.

Web Category refers to a set of features that includes URL Classification and Asynchronous Lookup. Classifying URLs provides this information that is used to filter unwanted content, adding an additional layer of security. The information can also determine which URLs should bypass SSLi decryption to comply with privacy laws.

The following categories are added:

Cat ID	Category Name	Category Grouping
85	Self-Harm	Sensitive
86	DNS Over HTTPS	Security
87	Low-THC Cannabis Products	Sensitive
88	Generative AI	Productivity

CLI Configuration

The new web categories are available in category-list-name sub-command of the following existing commands:

- **`Web Category`**
- **`Forward-policy destination matching`**
- **`Forward-proxy bypass rule`**
- **`Forward-proxy exception bypass.`**

```
ACOS(config)# web-category
ACOS(config-web-category)#category-list test
ACOS(config-web-category-category-list)#dns-over-https
ACOS(config-web-category-category-list)#generative-ai
ACOS(config-web-category-category-list)#low-thc-cannabis-products
ACOS(config-web-category-category-list)#self-harm
```

Show Commands

The statistics of the new web categories are available in category-list sub-command of the following show command:

- **show counters web-category**

To view all the web category commands and show commands, see *Command Line Interface Reference*.

Network Configuration

ACOS 6.0.3 introduces the following new feature and enhancement for the Network Configuration:

NOTE: For configuration, refer *Network Configuration Guide* and for specific CLI commands, refer *Command Line Reference Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topic is covered:

Support to Establish BFD Connection with VRRP-A Floating Address

BGP sessions can be established between a router and VRRP-A (active/standby) using the VRRP-A floating IP address as a source address. With this release, ACOS extends support to BGP with Bidirectional Forwarding Detection (BFD) using the VRRP-A floating IPv4 or IPv6 address.

Limitation

When VRRP-A switchover occurs, the new active device reinitiates the BGP and BFD sessions with the router using the VRRP-A floating IPv4 or IPv6 address. The BGP and BFD sessions will flap during the failover.

Platforms

ACOS 6.0.3 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

Disk Encryption

ACOS 6.0.3 provides full feature compatibility support for disk encryption, which was introduced in ACOS 5.2.1-P9 release. This feature is available only on Thunder 3745 and Thunder 3350 devices, when the disk encryption license is applied.

For more information on the feature implementation and configuration, see the Disk Encryption Support section in ACOS 5.2.1-P9 *New Features and Enhancements*.

SSLi QAT Support for Dell MVP

In the ACOS 6.0.3 release, for Dell Multi-tenant Virtual Platform (MVP) on-chip SSLi QAT is not supported.

Support for ADC Thunder on ESXi 8.0

Starting with ACOS 6.0.3, vThunder is supported on ESXI 8.0 for ADC.

- Reference platform: Dell R760

Support for Azure Standard VM Sizes

Starting with ACOS 6.0.3, the following Azure standard VM series and sizes are supported:

- Standard_D8s_v3
- Standard_D16s_v3
- Standard_D16_v5

Support for Intel E810-XXV NIC on ESXi 8.0

Starting with ACOS 6.0.3, the intel E810-XXV is supported on ESXI 8.0 with the following driver and firmware.

NIC Card	Model Number	Driver	Firmware
Intel	E810-XXV for SFP	1.8.5	4.2

Support for Multi-Control CPU in cThunder

Starting with ACOS 6.0.3, the multi-control CPU feature is supported in cThunder. The ACOS_CTH_NUM_OF_CTRL_CPUS environment variable is introduced to configure multi-control CPU in cThunder.

Environment variable: **ACOS_CTH_NUM_OF_CTRL_CPUS =** `<no_of_control_cpu>`

NOTE: It supports only the numeric value.

Support for VMware Paravirtual SCSI Controller

A10 Networks recommends using the 'VMware Paravirtual' SCSI controller for virtual machine running with ACOS 6.0.3 and later. The 'VMware Paravirtual' SCSI controller is not supported in versions prior to ACOS 6.0.3. In those prior versions, only the 'LSI Logic Parallel' is supported for virtual machine hardware.

NOTE: If the 'VMware Paravirtual' SCSI controller is attached to the VM on which ACOS 6.0.3 is running, downgrading to prior version is not possible.

System Configuration and Administration

ACOS 6.0.3 introduces the following new features and enhancements for System Configuration and Administration:

NOTE: For more information and details, refer *System Configuration and Administration Guide*.

The following topics are covered:

Configuration Synchronization Support for All Partitions

ACOS supports manual synchronization of configurations for all partitions utilizing the configure sync command. This feature is typically used in a VRRP-A environment to synchronize configurations from one device to another. It also allows each partition to independently synchronize its own settings, thereby providing a seamless synchronization process for each partition.

In the earlier releases, configuration synchronization could only be performed from the shared partition. To improve reliability and convenience, the configuration

synchronization feature has been extended to support synchronizing L3V and Service partition configurations also.

CLI Configuration

- To synchronize the running configurations from an L3V or Service partition:

```
ACOS<partion_name>(config)# configure sync running auto-authentication
<destination IP>
```

- To synchronize all configurations (running and startup) from an L3V or Service Partition:

```
ACOS<partion_name>(config)# configure sync all auto-authentication
<destination IP>
```

Limitations

- Only running and startup configurations are synchronized; while the device-specific configurations, such as interface configurations, are not synchronized.
- On multi-PU platforms, the partitions on PU2 do not get synchronized.

Enhancement to System Monitor Template

In the ACOS 6.0.3 release, the system monitor template can now be configured to clear the sessions for specific L3V partitions. Earlier, the template would clear the sessions for the shared partition only.

NOTE: By default, the clear sessions action takes effect only in the shared partition.

CLI Configuration

The following options are added to the `clear sessions` command.

```
ACOS(config)#system mon-template monitor num
ACOS(config-monitor)#action clear sessions {all | sequence num} {all-
partitions | partition name}
```

Here is a sample configuration that indicates the command application to clear sessions for a specific partition and for all partitions.

```
ACOS(config)#system mon-template monitor 1
ACOS(config-monitor)#action clear sessions sequence 1 partition test
ACOS(config-monitor)#monitor link-down eth 3 sequence 1

ACOS(config)#system mon-template monitor 2
ACOS(config-monitor)#action clear sessions all all-partitions
ACOS(config-monitor)#monitor link-down eth 3 sequence 1
```

Sharing Tokens with Multiple Hosts

While requesting access to the resources, ACOS authenticates a client using the client's source IP address, username, and password and sends a token back to the client. The admin session uses the client's token and source IP address to authorize access to the resources. Until now, this token could only be used by the client who requested access to the resources. If another client attempted to use this token, access to the resources was denied.

With this release, a new option, `axapi-token-sharing` is introduced under the `web-services` command to enable token sharing with multiple hosts. Enabling this feature reduces the number of authentication requests and improves the overall execution time.

NOTE: If `axapi-token-sharing` is enabled and multiple sessions are created, the outside hosts can access ACOS with the token from any session.

CLI Configuration

- To enable the sharing of aXAPI token within multiple hosts:

```
ACOS(config)# web-service axapi-token-sharing
```

- To disable sharing the aXAPI token within multiple hosts:

```
ACOS(config)# no web-service axapi-token-sharing
```

Limitations

- Sharing the token with multiple hosts poses a security threat.
- You can view the list of all hosts that share the token only in the logs. The `show admin session` command does not include the information.

Management Access and Security

ACOS 6.0.3 introduces the following new feature and enhancement for Management Access and Security (MAS):

NOTE: For configuration, refer *Management Access and Security (MAS) Guide* and for specific CLI commands, refer *Command Line Reference Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topic is covered:

Increased Timeout for Authentication Request

The timeout parameter under RADIUS external authentication has been enhanced. The maximum value has been increased from 15 seconds to 30 seconds. This enables an ACOS device to wait for an additional 15 seconds in replying to an authentication request before resending the request.

Threat Protection System

ACOS 6.0.3 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to *DDoS Mitigation Guide*. Similarly, for TPS-related CLI commands, refer to *DDoS Command Line Reference Guide*.

Security Updates

The following security vulnerability is addressed in the ACOS 6.0.3 release:

- OpenSSL Vulnerabilities
  - CVE-2023-3817: A vulnerability with applications using DH_check(), DH_check_ex (), or EVP_PKEY_param_check() functions to check a DH key or DH parameters and experiencing long delays during the process.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.2-P1

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.2-P1 release:

The following topics are covered:

Platforms

ACOS 6.0.2-P1 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

vThunder Supports RHEL 8.x KVM with Intel E810

With this release, vThunder supports RHEL KVM with E810. The following firmware, driver, and Dynamic Device Personalization (DDP) version are required with RHEL 8.x:

NIC Card	Model Number	ICEN Driver	Dynamic Device Personalization (DDP)	Firmware
Intel Card	E810	1.12.7	1.3.35	4.3

SSL Insight

ACOS 6.0.2-P1 introduces the following new feature and enhancement for SSL Insight (SSLi):

NOTE: For SSLi configuration steps, see *SSL Insight Configuration Guide*. Similarly, for SSLi-specific CLI commands, see *Command Line Reference Guide*.

The following topic is covered:

Virtual Wire Enhancement for Failover

ACOS supports the detection and tracking of active VLAN pairs in the virtual wire environment. This ensures uninterrupted traffic flow, even when VLAN configurations change during failover events or in topologies where forward and reverse traffic rely on different VLANs. This enhancement applies to both inbound and outbound SSLi use cases.

In virtual-wire SSLi (IP-less) deployments, packet brokers are used to route traffic to security devices as service chains using network and tool ports. Network ports handle traffic routing to the network, while tool ports direct service traffic to security devices.

When there are multiple upstream and downstream ports, such as multiple switches or firewall devices in a cluster, they act in an active-standby capacity for failover scenarios. The packet brokers serve as the 'bump-in-the-wire' between switches and firewalls. The packet broker utilizes VLAN tagging through Q-in-Q technology to track packet origins and destinations.

In this type of topology, it is important for ACOS to be aware of the VLAN pairs in the network and to keep track of the active VLAN pair during failover events. The virtual wire VLAN pairs can be implemented to facilitate ACOS in tracking the active VLAN pairs for virtual wire sessions. ACOS detects and updates the active VLAN pair in the network, forwarding the traffic to the active server.

For more details on the topology and implementation, see *Network Configuration Guide* and *SSL Insight Configuration Guide*.

CLI Configuration

To configure the virtual wire VLAN pairs feature, the following commands are introduced:

- Define the **virtual wire VLAN pair 1** to map with the active VLAN **2001** and **2003**.

```
ACOS(config)# virtual-wire-vlan-pair 1
ACOS(config-virtual-wire-vlan-pair:1)# vlan 2001 vlan 2003
```

- Define the **virtual wire VLAN pair 2** to map with the passive VLAN **2002** and **2004**.

```
ACOS(config)# virtual-wire-vlan-pair 2
ACOS(config-virtual-wire-vlan-pair:2)# vlan 2002 vlan 2004
```

- Configure the **virtual wire VLAN pair set 1**. Map the previously defined active and passive virtual wire VLAN pairs **1** and **2** .

```
ACOS(config)# virtual-wire-vlan-pair-set 1
ACOS(config-virtual-wire-vlan-pair-set:1)# virtual-wire-vlan-pair 1
ACOS(config-virtual-wire-vlan-pair-set:1)# virtual-wire-vlan-pair 2
```

Show Commands

The following show commands can be used for monitoring the virtual wire VLAN feature:

- **`show virtual-wire-global vlan-set-active-member`**
- **`show virtual-wire-global counter`**

Limitations

- This feature is supported only for slow paths.

  For example, the VLAN tagging with Q-in-Q technology and SSL inspection are often used in ‘slow paths,’ where the traffic needs to be inspected, processed, and managed more thoroughly.

- Making changes to **`virtual-wire-vlan-pair`** or **`virtual-wire-vlan-pair-set`** configurations in production may cause some virtual wire sessions to use the incorrect active VLAN.

Threat Protection System

ACOS 6.0.2-P1 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to *DDoS Mitigation Guide*. Similarly, for TPS-related CLI commands, refer to *DDoS Command Line Reference Guide*.

Enhancements in ACOS 6.0.2

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.2 release:

The following topics are covered:

Application Delivery Controller

ACOS 6.0.2 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC-specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for ADC-specific CLI commands, refer *Command Line Reference Guide*.

The following topics are covered:

Forward Proxy Enhancement

ACOS' forward proxy solution provides various rules, match conditions, and actions that allow you to control which client traffic is forwarded to servers or bypassed. This solution has been enhanced with fine-grained access control or Advanced Match Mode feature, allowing greater granularity and flexibility of forward proxy rules. The advanced match mode feature allows ACOS to filter HTTP requests based on multiple match conditions and take appropriate action.

This level of control is beneficial in scenarios where different types of HTTP content (request or response) require different treatments and analyze attempted policy violations.

The enhanced forward-proxy solution enables you to:

- Enable the advanced match mode in the 'forward-proxy' policy.
- Implement multiple advanced match conditions in the 'destination' rule to drop or bypass the traffic. These conditions can be combined with class-list matching rules.
- Setup additional actions such as sending a response page or message to notify the client that the access will be monitored. Similarly, setup a time range when the requests will be forwarded or dropped.
- Disable REQMOD and/or RESPMOD ICAP templates bound to the virtual port when the HTTP request matches the 'destination' advance match rule. See ICAP Pre-filtering Support.
- Applicable only to HTTP and HTTPS virtual ports.

CLI Configuration

Two new commands **`enable-adv-match`** and **`destination adv-match`** are introduced in the 'forward-proxy' module of the SLB template policy.

To configure the advance match mode in the forward-policy template, use the following commands:

```
ACOS(config)# slb template policy TEST
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# enable-adv-match
```

```
ACOS(config-policy-forward-policy)# source 1
ACOS(config-policy-forward-policy-source)# destination adv-match 799
ACOS(config-policy-forward-policy-source-...)# {action | disable-reqmod-icap | disable-respmod-icap | dual-stack-action | match options}
```

NOTE: All forward policy rules must contain an **action** or a **dual-stack-action**.

For detailed commands and their implementation, see *Command Line Interface Reference*.

Limitations

- The forward policy rule cannot filter HTTP responses.
- Binding or switching the advance match mode forward-policy template on a virtual port enables **proxy-layer v2** implicitly.

DNSSEC Validation Support in DNS Recursive Resolver

ACOS has implemented DNS Security Extensions (DNSSEC) support for authenticating and validating DNS data. The feature is used to authenticate genuine DNS response received or deny responses that cannot be trusted. ACOS already supported DNS recursive resolution. With this release, the DNS recursive resolver is enhanced as follows:

- Serves DNSSEC records if the 'DO' (DNSSEC OK) flag is present in client's query.
- Performs DNSSEC validation on responses before sending the responses to clients. This feature is disabled by default.

CLI Configuration

The following command is introduced in the **slb template dns**:

```
ACOS(config)#slb template dns test
ACOS(config-dns)#recursive-dns-resolution
ACOS(config-dns-recursive-dns-resolution)#dnssec-validation {enabled | disabled}
```

Show Commands

The following show command displays the statistics for DNSSEC validation of recursive resolution per virtual port:

```
ACOS(config)#show slb virtual-server vs 101 dns-udp application-
statistics | include DNSSEC
```

Limitations

The DNSSEC validation feature of the recursive resolver has the following limitations:

- It supports certain cryptographic algorithms and digest types. For the algorithms that are not supported, ACOS removes the DNSSEC records and unsets the 'DO' flag in the client response.
- It supports data size of upto 8000 bytes for DNS Record Set (RRset) validation.
- It uses DS records of the root zone as trust anchor. It does not support the configuration of the trust anchor.

For more information, see the *Application Delivery and Server Load Balancing Guide*.

Carrier Grade NAT

ACOS 6.0.2 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

The following topics are covered:

Anomaly Filtering Based on IPv6 Extension Headers

The IPv6 Extension Headers (EHs) contain supplementary information. Based on this information, routers and other network devices process and forward IPv6 packets. However, these EHs can be misused by attackers and therefore prove to be a security threat. Attackers can manipulate the options from Hop-by-Hop, Destination, and

Routing extension headers and cause IP spoofing attacks. Remote attackers can also abuse these extension headers to craft special IPv6 packets that trigger DDoS attacks.

The **ip anomaly-drop ipv6-ext-header** command is introduced to handle the security threat presented by the IPv6 Extension Headers. This command enables the detection and filtering of malformed IPv6 packets based on the extension header types.

Limitations

- This command can be enabled globally at the system level. It cannot be enabled at the partition level.
- Hardware FPGA does not accelerate the detection and filtering of IPv6 Extension Header based anomalies.
- This feature does not support logging.

CLI Configuration

The **ip anomaly-drop ipv6-ext-header** command enables filtering for the following:

- To detect and filter malformed IPv6 packets:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header malformed
```

An IPv6 packet is considered as malformed if the extension header order is not followed or the number of occurrences of the extension header is different than expected.

- To filter packets that contain the Hop-By-Hop/Destination EH:

For Hop-By-Hop Header:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header hop-by-hop option-type [ <0-255> [ to <0-255> ]]
```

For Destination Header:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header dest option-type [ <0-255> [ to <0-255> ]]
```

By configuring this command, you can drop a packet with a particular Option Type or a range of Option Types.

NOTE: Option Type 1 is often used for padding. Therefore, this field is set implicitly in most IPv6 packets. If you configure the **option-type** as 1, most of the IPv6 packets, including the non-malicious packets, will be dropped.

- To filter packets that contain the Routing EH:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header routing option-type [
<0-255> [ to <0-255> ] ]
```

By configuring this command, you can drop a packet with a particular Routing Type or a range of Routing Types.

- To filter packets that contain the Authentication EH:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header auth
```

- To filter packets that contain the ESP EH:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header esp
```

- To filter packets that contain the Fragmentation EH:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header frag
```

- To filter packets that contain the Mobility EH:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header mobility
```

- To filter packets that contain unknown extension header types:

```
ACOS(config)# ip anomaly-drop ipv6-ext-header eh-type <0-255> [ to <0-
255> ]
```

By configuring this command, you can drop a packet with a particular extension header type or a range of header types.

- To view packet filtering statistics based on IPv6 extension headers:

```
ACOS(config)# show ip anomaly-drop statistics
```

CGN Port Overloading Support with New NAT Pool Structure

ACOS supports Port Overloading, which enables one NAT mapping resource to be used by multiple flows destined for different destinations. This enhances NAT port

usage for many NAT IPs sharing the same concurrent connections. However, Port Overloading is only compatible with Port Batching v1 despite the NAT pool having variable types to configure. Port Overloading with Port Batching v1 is only supported when the `cgnv6 enable-port-batch-v1` command is enabled. Port Batching v1 fails in traffic processing performance and memory usage.

With this release, for better traffic processing and memory usage, ACOS supports the following:

- Port Overloading with the new NAT pool structure and Port Batching v2.
- Port Overloading configuration without configuring the `cgnv6 enable-port-batch-v1`.

CLI Configuration

- To configure a simple NAT pool with Port Overloading:

```
ACOS(config)# cgnv6 lsn port-overloading unique destination-address
ACOS(config)# cgnv6 lsn port-overloading udp
ACOS(config-port-overloading-udp)# port 2000 to 10000
ACOS(config)# cgnv6 nat pool pool1 198.51.2.1 198.51.2.10 netmask /24
```

- To configure a Port Batching v2 of NAT pool with Port Overloading:

```
ACOS(config)# cgnv6 lsn port-overloading unique destination-address
ACOS(config)# cgnv6 lsn port-overloading udp
ACOS(config-port-overloading-udp)# port 2000 to 10000
ACOS(config)# cgnv6 nat pool pool1 198.61.2.1 198.61.2.10 netmask /24
port-batch-v2-size 64 usable-nat-ports 1024 2000
```

Show Commands

The following counters are added to the `show cgnv6 lsn statistics` command:

- `Port Overloading NAT Port TCP Created`
- `Port Overloading NAT Port UDP Created`
- `Port Overloading NAT Port TCP Freed`
- `Port Overloading NAT Port UDP Freed`
- `Port Overloading Attempt Failed`

Limitation

A NAT port used for full-cone sessions cannot be used for Port Overloading.

Hardware Offloading of CGN and Firewall Sessions

In general, all CGN and Firewall sessions are processed and forwarded using software. This may cause a spike in CPU usage in case of heavy network traffic. In such scenarios, you can offload some CGN and Firewall sessions to the hardware. Hardware offloading frees up the CPU cycles, thereby enhancing the overall throughput, efficiency, and latency of the Thunder device.

Hardware offloading (also known as hardware acceleration or hardware forwarding) is only supported on FPGA devices having Ternary Content-Addressable Memory (TCAM). Such devices provide the capability to forward sessions in the hardware by programming the flows in the available TCAM.

Hardware Offloading Features in ACOS

- Supported only on TH7655 (Lite), TH6435, and TH14045 devices.
- Only the following sessions can be offloaded to the hardware:

  CGN LSN (NAT44) and NAT64

  Fixed NAT

  Firewall (only TCP and UDP traffic)
- Up to 128K IPv4 sessions or 64K IPv6 sessions can be offloaded to the hardware.
- Only established sessions can be offloaded to hardware.
- Only active sessions can be forwarded; standby sessions cannot be forwarded.

CLI Configuration

- To enable hardware offloading of CGN and Firewall sessions, use the following command:

```
ACOS(config)# system hardware-accelerate session-forwarding
```

- To check if a particular session is forwarded using hardware, use the enhanced **show sessions** command. The flags in the show command output indicate that the session is offloaded to the hardware.

- To view the information on the hardware entries being programmed into the TCAM, use the **`show hardware-accelerate statistics`** command.
- To view the hardware offloading statistics for the CGN and Firewall sessions, use the following show commands:
  - For LSN (NAT44) - **`show counters cgnv6 lsn hw-accelerate`**
  - For NAT64 - **`show counters cgnv6 nat64 hw-accelerate`**
  - For Fixed-NAT - **`show counters cgnv6 fixed-nat hw-accelerate`**
  - For Firewall - **`show counters fw hw-accelerate`**

Limitations

The following are the limitations of hardware offloading:

- Hardware offloading is not supported for any features that involve inspection of the payload. Therefore, the following features are not supported:
  - ALG sessions (for CGN and Firewall)
  - Tunneled traffic (for example, DS-lite)
  - DNS64 sessions
  - SCTP, GTP traffic
  - Rate-limiting
  - Application classification
  - Stateful and Generic Firewall sessions
  - Firewall local connections
- Since sessions can be offloaded only after they are established, the first few packets are always forwarded to the software.
- Hardware offloaded sessions do not support Round-Robin as a load-balancing method across trunk members.
- Fat flows are not supported.

Network Configuration

ACOS 6.0.2 introduces the following new features and enhancements for the Network Configuration:

NOTE: For configuration and CLI commands, refer *Network Configuration Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topics are covered:

Micro-BFD for Trunk Ports

Bidirectional Forwarding Detection (BFD) provides fast failure detection for control protocols. ACOS supports Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) interfaces also known as Trunks. This is achieved by executing an independent Asynchronous mode BFD session on every LAG member link called per-LAG-member-link BFD sessions “micro-BFD sessions”.

This feature supports the following:

- Verification of member link continuity in the absence of LACP.
- Verification of each member link to be able to forward L3 packets.
- Shorter detection time as compared to LACP.
- Static and LACP trunks.

NOTE:

- BFD should be enabled globally.
- The standard UDP destination port for Micro-BFD is 6784.
- Only one type of micro-BFD session, either an IPv4 or IPv6, exists per member link.

CLI Configuration

- To establish a micro-BFD session on the trunk ports for IPv4:

```
ACOS(config)#interface trunk 2
ACOS(config-if:trunk:2)#bfd per-member-port
ACOS(config-if:trunk:2-per-member-port)#ipv4 local-address 10.10.10.1
ACOS(config-if:trunk:2-per-member-port)#ipv4 neighbor-address
10.10.10.2
```

- To establish a micro-BFD session on the trunk ports for IPv6:

```
ACOS(config)#interface trunk 3
ACOS(config-if:trunk:3)#bfd per-member-port
ACOS(config-if:trunk:3-per-member-port)#ipv6 local-address 2001:1::1
ACOS(config-if:trunk:3-per-member-port)#ipv6 neighbor-address
2001:1::2
```

Show Commands

- To view the trunk type, Static or Link Aggregation Control Protocol (LACP), a new option Trunk Type is introduced in the output of the following show command:

```
show trunk
```

- To view if the BFD sessions are Micro-BFD, the interface (trunk member port) name will be added next to the ACOS interface (Our Address) in the output of the following show command:

```
show bfd neighbors
```

Limitation

The following are the limitations of Micro-BFD:

- You can only configure one type of Micro-BFD session per trunk – either IPv4 or IPv6.
- BFD echo and echo-demand are not supported for the Micro-BFD sessions.
- When a Firewall rule is configured, you must either disable the Unicast Reverse Path Forwarding (URPF) check or configure the micro-BFD source address on an interface. Otherwise, the BFD session state will not be UP.

Scaling in BGP, RIB, and FIB for 128G+ vThunder Platforms

The IPv4 and IPv6 BGP, RIB, and FIB route capacity has been upgraded for platforms with 128G and higher memory. The route limits are 1 million for IPv4 routes and 500K for IPv6 routes. These limits are set at the system level, which implies that the limits apply across the shared and all L3V partitions. For more information, see the datasheets.

Limitation

A minimum of two Control CPUs are required to support the new routing limits.

Platforms

ACOS 6.0.2 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

Various Product Support on Multi-PU Platform

Thunder 7650/7655S is a high-performance Multiple Processing Unit (multi-PU) platform built for large-scale traffic distribution, load balancing, and scalability. The multi-PU architecture has two active PUs: PU1 (Primary) and PU2 (Blade). The traffic for the same object is distributed to the PUs running the specific object. Both PUs can process the traffic, store the data and files, and compute statistics. This information can be accessed by logging in to the individual PU.

In the earlier releases, ADC product implementation was supported on multi-PU platforms. This release additionally supports the following ACOS products or components on a multi-PU platform.

- Application Access Management (AAM)
- Global Server Load Balancing (GSLB)
- IPsec Virtual Private Network (IPsec)
- Next Generation Web Application Firewall (NGWAF)
- SSL Insight (SSLi)
- Threat Intelligence Firewall

For detailed information on the implementation and configuration, see the respective *Configuration Guide* and *Command Line Interface Reference Guide*.

Security Enhancement in SSH Client

ACOS device utilizes SSH client to establish a secured connection between client and server. In this release, the ACOS device supports the encryption-based on Elliptic Curve Digital Signature Algorithm (ECDSA) to enhance security and align with FIPS compliance. ECDSA provides a modern and efficient approach to cryptography. It offers strong security with shorter key lengths and provides improved performance. Additionally, the SSH client now lists SSH keys and allows you to choose the required key type.

The process of generating ECDSA keys involves using the 'ssh-keygen' tool, which is similar to RSA key generation. The tool allows you to create an authentication key pair using the ECDSA algorithm with SHA-256, SHA-382, or SHA-521 digest-type. Once generated, these keys can be regenerated, loaded, and imported to the ACOS device.

For more information, see *System Configuration and Administration Guide*.

Support for Q-in-Q Traffic on Non-FPGA Devices

With this release, ACOS supports processing Q-in-Q traffic on selected non-FPGA devices. Q-in-Q was already supported on FPGA devices.

With this release, Q-in-Q support is extended to Thunder 3350 series (TH3350-E, TH3350, and TH3350S). To enable this feature, configure the **enable-all-ports** option in the **system q-in-q** command and the appropriate Tag Protocol Identifier for the inner and outer VLANs.

CLI Configuration

```
ACOS(config)#system q-in-q [enable-all-ports | inner-tpid | outer-tpid]
```

Limitations

- Once activated, Q-in-Q is enabled across all supported ports on a Thunder device.
- Only X710 ports (ports 9 to 20) on the Thunder 3350 platform support Q-in-Q. When the **enable-all-ports** option is configured:
  - Ports 9 to 20 accept both Q-in-Q and VLAN/normal traffic.
  - Ports 1 to 8 accept only VLAN/normal traffic (no Q-in-Q traffic).
- As Q-in-Q support is handled by NIC cards, there are no drop counters to show if a TPID mismatch takes place.
- This feature is only supported on the data plane.

For more information, see the *Network Configuration Guide*.

Thunder ADC Support on Google Cloud Platform

With this release, A10 Thunder ADC is a fully operational, software-based Application Delivery Controller (ADC) solution that can run on the Google Cloud Platform (GCP).

GCP is a suite of secure, reliable, and highly scalable cloud computing services offered by Google. You can deploy Thunder ADC as a virtual instance within GCP thereby offering advanced traffic management capabilities along with a robust load-balancing solution.

For more information, see *Installing Thunder ADC on GCP Guide*.

KVM Hypervisor Support

The below combination is supported for vThunder starting ACOS 6.0.2.

Hypervisor	OS Version	Supported NICs	Solution	Reference Platform
KVM	RHEL 9	Mellanox ConnectX-6 LX 25/10G , ConnectX 6 DX 100GbE	MVP CGN (Multi tenant virtual platform)	Dell R760
KVM	RHEL 8	ConnectX 6 DX 100GbE	CGN	Dell R760

Hardware Platform Support

Thunder 5960 has been introduced as the newly-supported hardware platform in the ACOS 6.0.2 release. For more information on the complete list of supported hardware Platforms, refer *Hardware Platforms Support* in *Release Notes*.

SSL Insight

ACOS 6.0.2 introduces the following new features and enhancements for SSL Insight (SSLi):

NOTE: For SSLi configuration steps, see *SSL Insight Configuration Guide*. Similarly, for SSLi-specific CLI commands, see *Command Line Reference Guide*.

The following topics are covered:

ICAP Pre-filtering Support

ACOS provides Internet Content Adaptation Protocol (ICAP) services for HTTP and HTTPS sessions. ACOS can act as an ICAP client and interact with ICAP servers to

perform content adaptation tasks for HTTP and HTTPS traffic that passes through ACOS. This feature is often implemented in conjunction with a forward-proxy such as SSLi to intercept and inspect traffic as a man-in-the-middle.

To provide granular control on what traffic should be bypassed and intercepted by ICAP server, a new action is introduced that allows you to enable or disable ICAP templates (REQMOD or RESPMOD) based on the HTTP request or response conditions. ACOS filters the HTTP requests that match these conditions using the 'forward-policy' module and disables the REQMOD and/or RESPMOD ICAP templates that is bound to the virtual port.

CLI Configuration

To configure the ICAP pre-filtering options in the forward-policy template, use the following commands:

```
ACOS(config)# slb template policy TEST
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# enable-adv-match
ACOS(config-policy-forward-policy)# source 1
ACOS(config-policy-forward-policy-source)# destination adv-match 799
ACOS(config-policy-forward-policy-source-...)# disable-reqmod-icap
ACOS(config-policy-forward-policy-source-...)# disable-respmod-icap
```

Limitation

- You cannot configure a rule to disable only the ICAP templates.

For more information, see Forward Proxy Enhancement.

GUI Logging Support for Inbound SSLi with Virtual Wire

ACOS supports a virtual wire (vwire) or bump-in-the-wire deployment mode, commonly used in SSLi solutions. In this mode, the Thunder device acts as a transparent proxy on the network. It intercepts and inspects SSL/TLS encrypted traffic using an IP-less configuration.

With this release, ACOS web GUI will capture the logs for the inbound SSLi with virtual wire for better visibility. It will allow you to effectively manage and monitor SSL/TLS traffic in a virtual wire environment. The logging feature leverages a client-

SSL template and a server-SSL template in conjunction with the forward-policy feature.

When the SSLi and ACOS event logging are enabled on the configured client-SSL template, the inbound SSLi logs are displayed on the web GUI **Log >> SSLi** page.

Limitation

Logs are not generated for other types of inbound SSLi that do not use the client-ssl and server-ssl templates.

A10 Call Home Enhancement

The Call Home feature is now enabled by default. Call Home enables ACOS devices to send information securely on how A10 products are used to the A10 Product Research team. This information includes configuration and environmental data such as the ACOS device, its form factor, deployment location (such as on-premise, public cloud, and so on), number of interfaces, L3V partitions, VLANs, and more. Additionally, it collects information on the ACOS licenses activated on the device. All the information collected is used to improve the quality of the product.

The Call Home data is collected from the ACOS device every 24 hours at midnight. You can manually offset the Call Home time by 1 to 60 minutes.

All information collected by A10 is processed in accordance with A10 Networks' Data Processing Addendum. However, if any PII is received, it will be processed in accordance with A10 Networks' Data Processing Addendum. All information received through the Call Home feature is anonymized and used purely to enhance our products and improve quality.

NOTE: For detailed information about Call Home, refer *System Administration and Configuration Guide*.

For Call Home to work, the following conditions must be met:

- **Internet Connection** — The ACOS device must be able to reach the internet for Call Home to send diagnostic data to the A10 centralized collector. This feature does not work with proxy server configuration.

NOTE: Call Home uses the management interface to send data to the A10 centralized collector.

- **Port** — The Call Home data from your ACOS device is sent over TLS protocol using port 443 by default. It is important to note that, in order to send data from your ACOS device to the A10 Product Research team, you must whitelist the following:
  - Call Home Endpoint: callhome.a10networks.com
  - Static IP address: 129.153.110.25

NOTE: Call Home is enabled by default from ACOS 5.2.1-P8 and 6.0.2 versions onwards. You can choose to manually disable the Call Home feature on your ACOS device.

CLI Configuration

To disable Call Home, enter the following commands and save your configurations:

```
ACOS(config)# call-home profile
ACOS(config-profile)# deregister
```

The `deregister` command disables the Call Home service and stops the ACOS device from sending data to A10.

To reenable Call Home on the ACOS device, ensure that the device has internet connectivity from the management plane. Then, enter the following commands and save the configurations.

```
ACOS(config)# call-home profile
ACOS(config-profile)# register
```

The `register` command enables the Call Home service. Once enabled, the Call Home data is collected from the ACOS device every 24 hours at midnight. You can manually offset the Call Home time by 1 to 60 minutes.

```
ACOS(config-profile)# time <1-60> mins
```

For example, if you configure the offset time as 5 mins, the data will be exported at 12:05 AM.

Threat Protection System

ACOS 6.0.2 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to *DDoS Mitigation Guide*. Similarly, for TPS-related CLI commands, refer to *DDoS Command Line Reference Guide*.

Security Updates

The following security vulnerabilities are addressed in the ACOS 6.0.2 release:

- OpenSSL Vulnerabilities
  - CVE-2023-0465: A vulnerability with applications using non-default options when verifying certificates may affect the ACOS data plane.
- Moment.js Vulnerability
  - CVE-2022-24785: A vulnerability with path traversal impacting npm (server) users.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.1

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.1 release:

The following topics are covered:

Application Access Management

ACOS 6.0.1 introduces the following new features and enhancements for Application Access Management (AAM):

NOTE: For AAM specific configuration steps, refer *Application Access Management Guide*.

The following topics are covered:

KDC Support for Linux and Windows

In the ACOS 6.0.1 release, ACOS extends AAM Kerberos Domain Controller (KDC) authentication support to the Linux environment. This is a notable change from prior releases, where ACOS only supported AAM KDC authentication in the Windows environment.

NOTE: The KDC validation and password change are supported only in the Windows environment.

Security Support for AAM Authentication Logon

The **AAM Authentication Logon Form-Based** page uses a set of web pages that contain data forms. ACOS sends the Logon page in response to a request to secure services.

ACOS provides additional security features to mitigate clickjacking attacks on the **AAM Authentication Logon Form-Based** page using the X-Frame Options (XFO) feature. Clickjacking (or click hijacking) is an interface-based cyberattack that involves tricking the user into clicking on actionable content on a hidden website element (iframe layer).

To enhance security for the **AAM authentication Logon Form-Based** page, configure the following HTTP security features or policies:

- **Content-Security-Policy (CSP) response header (frame ancestors):** This allows an administrator to specify whether a page should be rendered in the <frame> or <iframe>.
- **Strict-Transport-Security (HSTS) response header:** This allows an administrator to set the timeout value for the page and specifies whether the page (or sub-domains) should only be viewed through HTTPS until the timeout expires.

CLI Configuration

- To configure CSP, use the following commands:

```
ACOS(config)#aam authentication logon form-based <profile-name>
```

```
ACOS(config-form-based auth logon:<profile-name>)#csp-support
<none|self|specificURI>
```

- To deny the browser from rendering or embedding a page inside a <FRAME> or <IFRAME> tag, use the following command:

  ```
  ACOS(config-form-based auth logon:<profile-name>)#csp-support none
  ```

- To allow the current page to be displayed in a frame on another page, but only within the current domain, use the following command:

  ```
  ACOS(config-form-based auth logon:<profile-name>)#csp-support self
  ```

- To allow the current page to be displayed in a frame but only in a specific URI, use the following command:

  ```
  ACOS(config-form-based auth logon:<profile-name>)#csp-support
  specificURI https://a.example.com
  ```

- To configure the HSTS policy on authentication logon form-based, use the following commands:

```
ACOS(config)#aam authentication logon form-based <profile-name>
ACOS(config-form-based auth logon:<profile-name>)#hsts-support timeout
<seconds>
```

- To configure the HSTS policy on authentication logon http-authenticate, use the following commands:

```
ACOS(config)#aam authentication logon http-authenticate <profile-name>
ACOS(config-http-authenticate auth logon:<profile-name>)#hsts-support
timeout <seconds>
```

To view the information about CSP and HSTS policies, use the following show commands:

```
show aam authentication logon form-based
show aam authentication logon http-authenticate
```

Known Limitations

- The Clickjacking feature is supported only when the HTTP/2 protocol support is enabled.

NOTE: To insert the new supported HTTP headers (X-Frame-Options, Content-Security-Policy, and Strict-Transport-Security) the client traffic must be HTTP/2.

- AAM does not support the service partition.

For more information, see the *Command Line Interface Reference Guide* and *Application Access Management Guide*.

Application Delivery Controller

ACOS 6.0.1 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for ADC specific CLI commands, refer *Command Line Reference Guide*.

The following topics are covered:

Least Request Load-Balancing Method Enhancement

ACOS provides the least-request load balancing method to select the server and port that has the least unanswered HTTP requests. This method is enhanced with the following features:

- Change to the default behavior:

  In the earlier releases, the least-request method used the following formula to compare the requests on two servers and accordingly selected the server: *request_count/weight*

  In the current release, the least-request uses the *request_count/weight=1* formula. This indicates that the weight configured on the real server is not considered for server selection. It is instead based on the request count. Here, request_count indicates the HTTP/HTTPS requests sent to the server but not responded to, and weight indicates the weight value configured on the real server.

- Addition of Pseudo Round Robin (PRR) algorithm to the least-request load balancing method:

  The pseudo-round-robin method performs two levels of comparison to select the service group:

  - As the first level, it selects the service group by comparing the values of two servers using the request_count/weight=1 formula.
  - If the compared value for two servers is equal, the pseudo-round-robin acts as the second level and chooses the server that has not been selected for the longest time, based on its timestamp.

CLI Configuration

To enable this option in the slb service-group method, use the following command:

```
ACOS)config)#slb service-group <svg name> <tcp/udp>
ACOS(config-slb svc group)#method service-least-request-pseudo-round-robin
ACOS(config-slb svc group)#
```

Show Commands

After configuring the **service-least-request-pseudo-round-robin** method, the following show command displays the configuration and distribution method for the specific service group:

```
ACOS)config)#show slb service-group [name] config
```

Extended IPv6 AVP Support for RADIUS Load Balancing

ACOS supports source IP hash load-balancing for RADIUS traffic by extracting the Attribute Value Pairs (AVP). In the previous releases, only the IPv4 AVP 8 (Framed-IP-Address) and AVP 4 (NAS-IP) were supported on the RADIUS UDP. This feature is now extended to fully support the IPv6 AVP 97 (Framed-IPv6-Prefix) and 168 (Framed-IPv6-Address). Additionally, the IPv6 subnet masking (in bytes) can be configured to mask specific octets of the source IPv6 address and conduct hash load balancing.

The AVP number is a RADIUS attribute, which is derived from the originating IP address from the RADIUS packet. This IP address is then used for server selection. Furthermore, the IP offset can be configured to mask specific octets of the source IP and conduct hash load balancing. This implementation is achieved using the RADIUS UDP template, which is bound to the RADIUS virtual ports.

CLI Configuration

A new hash-based RADIUS load balancing method **`ipv6 avp`** is introduced in the SLB UDP template.

```
ACOS(config)#slb template udp radius s1
ACOS(config-l4 udp)# radius-lb-method hash ipv6 avp {168/97}
```

A new hash-based algorithm **`ipv6-subnet`** is introduced globally in the SLB common configuration.

```
ACOS(config)# slb common
ACOS(config-common)# lb-method-hash src-ip-only ipv6-subnet <0-15>
```

aFleX Support

aFleX supports the IPv6-related AVPs such as Framed-IPv6-Address and Framed-IPv6-Prefix.

Dynamic Service Enhancement for Forward Proxy Feature

The SLB dynamic service feature is enhanced with the capability to configure specific DNS servers based on the destination domain. This functionality is enabled by configuring the DNS servers for the specified Aho Corasick (AC) class-list.

ACOS can be used as a forward proxy to secure Internet access from internal clients. It uses the SLB dynamic service template and provides DNS resolution while forwarding traffic to the Internet. In the dynamic service template, you can define one or more DNS servers to resolve host names to IP addresses. This enhancement provides more granular conditions in addition to the existing rules within the SLB dynamic service feature.

The request is forwarded to the DNS server based on the following conditions:

1. If the class-list and the corresponding DNS server are configured in the dynamic-service template, ACOS selects the DNS server based on the domain name of the request. If the domain name matches one of the class-lists, the corresponding DNS server is selected. If the domain name matches multiple class-lists, the class-list is selected based on the priority set.
2. If the class-list and the corresponding DNS server are not configured, ACOS checks the configuration of the default DNS server in the dynamic service template. If the default server is configured, ACOS selects the default server to resolve IP address.
3. If both the class-list and the default DNS servers are not configured, ACOS checks the configuration of the Global DNS server in the **`ip dns <primary/secondary>`** command.

Supported Features

The enhanced dynamic service template for forward proxy supports the following conditions:

- Only the AC type class-list.
- A maximum of 64 class-lists, each containing a maximum of two DNS servers.
- The HTTP/1.1 and HTTP/2 protocols.
- The old and new proxy.

CLI Configuration

In the SLB template dynamic-service, first create an AC class-list:

```
ACOS(config)#slb template dynamic-service test2
ACOS(config-dynamic-service)#class-list super ac
```

Then, add DNS servers to the class-list and assign a priority to the class-list, as indicated in the following example:

```
ACOS(config)#slb template dynamic-service test2
ACOS(config-dynamic-service)#class-list super priority 20
ACOS(config-dynamic-service-class-list)#dns server 1.1.1.1
ACOS(config-dynamic-service-class-list)#dns server 2.2.2.2
```

Show Commands

After configuring the class-lists and the corresponding DNS servers in the **dynamic-service template**, the following show command displays which DNS servers are used for resolving specific destination domains:

```
ACOS(config)#show dns-cache
```

The following show command displays the configuration of a particular dynamic-service template:

```
ACOS(config)#show slb template dynamic-service test2
```

Increased Maximum Persistence Timeout Value

ACOS supports session persistence based on the source IP address. ACOS uses the configured source IP address to send all the traffic from a given client IP address to the same server until the server is up or the persistence timeout expires.

In this release, the range of the maximum persistence timeout value in the source IP persistence template is increased from 1-2000 minutes to 1-4321 minutes (about 72 hours). When the timeout value expires, the session is deleted, and the defined load balancing mechanism is used to select a new server.

This functionality is helpful when a consistent connection between a client and a server is required, and to track the client's interaction with the application.

CLI Configuration

The following command configures the maximum session timeout value in the SLB template persist source-IP.

```
ACOS(config)# slb template persist source-ip sip
ACOS(config-source ip persist)# timeout 4321
```

Defend against HTTP Request Smuggling

ACOS provides HTTP request compliance check capabilities to defend from HTTP/1 and HTTP/2 smuggling attacks. HTTP request smuggling exploits differences in how the front-end servers (proxies) and back-end servers execute requests from multiple senders.

ACOS 6.0.1 provides full feature compatibility support for defending against HTTP request smuggling attacks introduced in earlier releases. The following features are compatible with this release:

• Introduced in ACOS 5.2.1-P4, you can configure HTTP protocol compliance checks or conditions and enable the 'drop' action when the conditions are met.

• Introduced in ACOS 5.2.1-P5, you can configure HTTP header filter rules (header-name) to be detected and enable the 'drop' action when the header-name matches the filter rules.

For detailed information about the configurations, see the following sections:

- Defend against HTTP Request Smuggling
- HTTP Request Smuggling Enhancement

Enhancement to Compound Health Monitor Logs

Compound health monitors combine the results of multiple health checks into a single outcome to assess health of individual real servers, service ports, or service groups.

In previous ACOS releases, compound health monitor logs displayed only the UP or DOWN status of the servers with no context about the sub-health monitors that make up the compound health monitor.

With this release, the logging mechanism is enhanced to capture granular information on the various sub-compound health monitors, thereby improving troubleshooting and debugging.

The details on health monitor sub-compounds are logged in the following format:

[DateTime] [LogType] [ModuleName]:[<PartitionName>] Sub-Compound [SubCompoundName] on the server (IPaddress:PortNumber/[Method]) is [CompoundStatus] ([Reasons])

Limitations

This feature is not supported for data plane health monitors for database and kerberos.

Show Commands

```
ACOS#show log | in Sub-compound
Dec 13 2022 15:07:53 Info [HMON]:   CEF:0|A10|CFW|6.0.0-d|HMON
450395512181358593|sub-compound status changed|2|cs1=udp53 cs1Label=Sub-
compound name cs2=[2020::1:1]:53 cs2Label=on the server cs3=UDP
cs3Label=method cs4=up cs4Label=status cs5=UDP No Response
cs5Label=reason
Dec 13 2022 15:07:53 Info  [HMON]:   CEF:0|A10|CFW|6.0.0-d|HMON
450395512181358593|sub-compound status changed|2|cs1=udp53 cs1Label=Sub-
compound name cs2=20.1.1.1:53 cs2Label=on the server cs3=UDP
cs3Label=method cs4=up cs4Label=status cs5=UDP No Response
cs5Label=reason
```

Log Examples

The following is a sample SYSLOG that displays the details for HMON in a shared partition:

```
Oct 28 2022 15:55:26 Info [HMON]:Sub-compound udp53 on the server
([2001::101]:53/UDP) is up (UDP No Response)
Oct 28 2022 15:55:22 Info [HMON]:Sub-compound dns53 on the server
([2001::101]:53/DNS) is down (SNMP Receive OK)
Oct 28 2022 15:55:22 Info [HMON]:Sub-compound tcp25 on the server
([2001::101]:25/TCP) is up (TCP Verify Connection OK)
Oct 28 2022 15:55:22 Info [HMON]:Sub-compound http8080 on the server
([2001::101]:8080/HTTP) is up (HTTP Status Code OK)
```

The following is a sample CEF log in the L3V shared partition:

```
Dec 12 2022 18:38:32 Info  [HMON]:<p1>  CEF:0|A10|CFW|6.0.0-d|HMON
450395512181358593|sub-compound status changed|2|cs1=p1_tcp25
cs1Label=Sub-compound cs2=20.1.1.1:25 cs2Label=ip_str cs3=TCP
cs3Label=method cs4=down cs4Label=status cs5=TCP Timeout cs5Label=reason
Dec 12 2022 18:38:32 Info  [HMON]:<p1>  CEF:0|A10|CFW|6.0.0-d|HMON
450395512181358593|sub-compound status changed|2|cs1=p1_http8080
cs1Label=Sub-compound cs2=20.1.1.1:8080 cs2Label=ip_str cs3=HTTP
cs3Label=method cs4=down cs4Label=status cs5=HTTP Timeout
cs5Label=reason
Dec 12 2022 18:38:32 Info  [HMON]:<p1>  CEF:0|A10|CFW|6.0.0-d|HMON
450395512181358593|sub-compound status changed|2|cs1=p1_tcp80
cs1Label=Sub-compound cs2=20.1.1.1:80 cs2Label=ip_str cs3=TCP
cs3Label=method cs4=down cs4Label=status cs5=TCP Timeout cs5Label=reason
```

Firewall

ACOS 6.0.1 introduces the following new feature and enhancement for Firewall:

NOTE: For Firewall specific configuration steps, refer *Firewall Configuration Guide*.

The following topic is covered:

Creating Full Sessions in DSR Mode

The ACOS device creates a TCP session after completing the standard 3-way TCP handshake. However, if the device is deployed in Direct Server Return (DSR) mode, the standard TCP three-way handshake cannot be completed and therefore fully established sessions cannot be created.

The **`fw dsr-mode-support`** command is introduced to allow session creation when the device is deployed in the DSR mode. When this command is configured, a fully established session is created on receiving a single IPv4 or IPv6 TCP packet even if the standard three-way handshake is incomplete. The session is created on receiving any TCP packet except RST and FIN.

NOTE: If the **fw allow-non-syn-session-create** command is also enabled, a full session is created even on receiving a SYN TCP packet.

CLI Configuration

The **fw dsr-mode-support** command allows sessions to be created in the DSR mode based on whether the incoming TCP packets are IPv4 or IPv6.

- To create sessions for IPv4 TCP packets:

```
ACOS(config)# fw dsr-mode-support ipv4
```

- To create sessions for IPv6 TCP packets:

```
ACOS(config)# fw dsr-mode-support ipv6
```

- To create sessions for any (IPv4 or IPv6) TCP packets:

```
ACOS(config)# fw dsr-mode-support all
```

Limitations

Following are the limitations of the **fw dsr-mode-support** command:

- Supports session creation for TCP traffic only.
- Does not support ALG session creation.

IPsec Virtual Private Network

ACOS 6.0.1 introduces the following new features and enhancements for IPsec Virtual Private Network (VPN):

NOTE: For IPsec specific configuration steps, refer *IP Security Configuration Guide*.

The following topic is covered:

Signature Authentication in Internet Key Exchange Version 2 (IKEv2)

Internet Key Exchange Version 2 (IKEv2) supports Rivest-Shamir-Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) authentication methods. The RSA authentication method uses SHA1 for generating signature payloads, while the ECDSA authentication method supports three elliptic groups, with a fixed hash algorithm attached to each group.

With this release, ACOS supports signature authentication in IKEv2. It facilitates the use of stronger hash algorithms for generating authentication payloads during an IKEv2 negotiation. You can use different hash algorithms – SHA256, SHA384, and SHA512 for generating signature (authentication) payloads.

The `vpn signature-authentication` command must be configured to enable signature authentication. By default, it is disabled.

A new keyword "hash" is introduced to specify the hash algorithm used with the auth-method configuration.

CLI Configuration

- To enable signature authentication, use the following command:

```
ACOS(config)# vpn signature-authentication
```

- To add hash algorithm option for ECDSA, use the following command:

```
ACOS(config-ike-gateway:a1)#auth-method ecdsa-signature hash
```

- To add hash algorithm option for RSA, use the following command:

```
ACOS(config-ike-gateway:a1)#auth-method rsa-signature hash
```

Show Commands

- To view the configuration status of signature authentication, use the following command:

```
show vpn
```

- To view the hash algorithm used to sign authentication payloads, use the following command:

```
show vpn ike-sa <gateway-name>
```

Limitations

- Signature Authentication in IKEv2 works for site-to-site configuration only.
- The signature schemes corresponding to RSA (Section A.1 of RFC 7427) and ECDSA (Section A.3 of RFC 7427) are supported.
- When signature authentication is enabled, the IKE acceleration support on the QuickAssist Technology (QAT) devices has some limitations. The sign and verify functions for the ECDSA certificates are supported via the software paths.

Network Configuration

ACOS 6.0.1 introduces the following new features and enhancements for the Network Configuration:

NOTE: For configuration and CLI commands, refer *Network Configuration Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topics are covered:

BGP Large Communities

In this release, ACOS supports the BGP Large Communities attribute based on RFC 8092 and RFC 8195. The BGP Large Community attribute is an addition to the existing support of BGP Standard and Extended Communities attributes.

This feature provides a powerful tool for large network operators who wish to configure routing policies more efficiently to improve the performance and security of a network. It also offers the capability to tag routes and modify the BGP routing policy on routers. This allows the BGP router to receive large communities from one of its peers and decide whether to take specific action on these routes through route-map or announce these routes to the neighbors.

The BGP large community attribute is based on four-octet Autonomous System Numbers (ASNs). It is encoded as a set of 12-octet values and is represented in the XX:YY:ZZ format. Each value is divided into three parts with 4-octet each; global administrator field (ASN) and two 4-octet operator-defined fields ('Local Data Part 1' and 'Local Data Part 2').

This feature offers the following functionalities:

- Define the BGP Large Community List and BGP Large Community Attributes.
- Set and match the BGP Large Community List in the route map.
- Configure and apply the BGP Large Communities to the BGP neighbor or network.

CLI Configuration

- To define the BGP large community list and attributes, use the following commands:

```
ACOS(config)# ip large-community-list {expanded list-name | standard
list-name} {num <1-99> or <100-199>} deny | permit} community-number
<XX:YY:ZZ>
```

  Two types of BGP large community lists are supported for matching criteria, *standard* and *expanded*.

- To set and match the BGP Large Communities in the route map, use the following commands:

```
ACOS(config)# route-map map-name {deny | permit} sequence-num
ACOS(config-route-map)# match large-community list-id [exact-match]
ACOS(config-route-map)# set large-community {XX:YY:ZZ | additive} |
none}
ACOS(config-route-map)# set large-comm-list list-id {expanded |
standard} delete
```

  The route map matches the route with the large community-list values or other criteria and set additional large community values to the BGP peer.

- To add the BGP large communities on the specified network that is advertised to the neighbor, use the following commands:

```
ACOS(config)# router bgp {as-num}
```

```
ACOS(config-bgp:..)# network {ipaddr/mask-length | ipaddr [mask
networkmask]} large-community XX:YY:ZZ
ACOS(config-bgp:..)# neighbor neighbor-id send-community [all | both |
none | standard | extended | large]
ACOS(config-bgp:..)# address-family ipv6
ACOS(config-bgp:..ipv6)# network {ipaddr/mask-length | ipaddr [mask
network-mask]} large-community XX:YY:ZZ
ACOS(config-bgp:..ipv6)# neighbor neighbor-id send-community [all |
both | none | standard | extended | large]
```

The **network** command announces the route and the large community values from route-map to the BGP peers. Similarly, the **neighbor** command provides granular control of route announcements to individual BGP peers. The **send-community** options set the type of community (standard, extended, large community attributes) to send to a BGP peer. You must configure either **all** or the **large** option to send the BGP large communities.

Show Commands

To view the BGP large community, use the following show commands:

- **show bgp large-community <*X:Y:Z*>**
- **show bgp large-community-list <*list-name*>**
- **show ip bgp large-community <*X:Y:Z*>**
- **show ip bgp large-community-list <*list-name*>**
- **show route-map <*name*>**
- **show run ip large-community {expanded | expanded-num | standard | standard-num}**

Implicit Firewall Rules for Configured Routing Protocols

In the prior releases, ACOS supported implicit rules for the following protocols:

- VRRP-A
- Scaleout
- VCS

- DHCP
- TWAMP

With this release, ACOS installs internal firewall rules for routing protocols when the firewall feature is enabled. You do not need to add additional explicit rules for implicitly supported protocols. These internal rules have been extended to support the following protocols when they are configured:

- BGP (v4 and v6)
- OSPF (v2 and v3)
- BFD (v4 and v6)
- RIP
- RIPING

Limitations

The following are the limitations:

- Adding an explicit deny rule without specifically allowing traffic destined for the ACOS device will cause the dynamic routing protocols to stop functioning.
- The firewall rules for Non-Broadcast Multiple Access (NBMA) and virtual-link in Open Shortest Path First v2 (OSPFv2) and OSPFv3 are not auto-generated. You must add an explicit rule for it. For more information about OSPFv2/v3 virtual-link, see the *Command Line Interface Reference* guide.
- To enable Interior Border Gateway Protocol (IBGP) or multi-hop Exterior Border Gateway Protocol (EBGP), you must use the update-source commands. For more information about the update-source command, see the *Command Line Interface Reference* guide.
- If the Bidirectional Forwarding Detection (BFD) session is up and enabled without echo, it may cause the BFD session to experience brief flapping for several seconds. If needed, before enabling the BFD with the protocols, make sure to add BFD echo to prevent any flapping.

Next Generation Web Application Firewall

ACOS 6.0.1 introduces the following new features and enhancements for the Next Generation Web Application Firewall (NGWAF):

The following topics are covered:

Enhanced Dashboard Information

A10 Next-Gen WAF (NGWAF) agents deployed on the ACOS platforms communicate with the Fastly Cloud and send periodic updates. The Fastly Cloud dashboard displays the agent information, which includes the agent Name, Status, Version, Module, and so on. From this release, the Fastly Dashboard also displays the information of the A10 device (the Agent is connected to).

The following A10 devices are supported by NGWAF:

- Thunder devices (hardware) such as TH3350, TH1040F, and more.
- Thunder Multi-tenant Virtual Platform (Thunder MVP) deployed on Dell OEM.
- vThunder (Virtual Thunder) - In this case, the bandwidth license information is displayed.

For the complete list of MVP and Thunder platforms supported by NGWAF, see the *A10 Next Generation Web Application Firewall Configuration* guide.

NOTE: For these platforms, NGWAF is supported only for ACOS versions 6.0.0 TR, 6.0.0-P1, and 6.0.1 GA.

Explicit Proxy Server Usage

The default proxy-free connection to the Fastly Cloud is vulnerable to internet-borne threats. For better protection, you can configure an explicit proxy server and connect to the Fastly Cloud through it. The proxy server adds an extra layer of security to the connection, thereby protecting against malicious traffic.

CLI Configuration

The **use-https-proxy** command is introduced under **slb common** to enable connection to the Fastly Cloud through the specified explicit proxy server. This command allows you to specify an IPv4 or IPv6 proxy server.

- To connect through an IPv4 proxy server:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-https-proxy192.168.2.2 3128
```

- To connect through an IPv6 proxy server:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-https-proxy2022:192::33 3128
```

NOTE:

- Ensure that the configured explicit proxy server is reachable.
- NGWAF (if enabled) will restart automatically after configuring or deleting the explicit proxy server.

Licensing A10 Next-Gen WAF

Starting from ACOS 6.0.1, a valid license must be installed to use A10 Next-Gen WAF (NGWAF). The NGWAF license can be acquired from A10 Global License Manager (GLM).

For NGWAF license installation steps, refer to the A10 Next Generation Web Application Firewall Configuration guide.

Management Interface Usage

A10 Next-Gen WAF (NGWAF) connects to the Fastly Cloud through the data interface by default. For better traffic management, the **use-mgmt-port** command is introduced. When this command is enabled, the management interface is used to connect to the Fastly Cloud.

CLI Configuration

- To enable management interface usage for NGWAF:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-mgmt-port
```

- To disable management interface usage for NGWAF:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf use-mgmt-port
```

NOTE: This command is only available on the shared partition but is applied to all partitions

Overlay Networks

ACOS 6.0.1 introduces the following new feature and enhancement for Overlay Networks:

NOTE: For more information, refer *Configuring Overlay Networks Guide*.

The following topic is covered:

VXLAN Source Port Range Control

ACOS supports Virtual Extensible LAN (VXLAN) overlay tunnels where the layer 2 packets are tunneled over a Layer 3 network using UDP/IP over IP frames.

With this release, a configurable UDP source port range option has been provided for Virtual Extensible LAN (VXLAN) overlay tunnels. This option controls the VXLAN source port range either globally or on a per virtual tunnel endpoint (VTEP) basis. The source port range can be configured globally and per virtual tunnel endpoint (VTEP). The source port range can be set between 1 to 65535.

NOTE: The VXLAN source port range configuration is not supported on multi-PU platforms.

CLI Configuration

A new command **src-port-range** is introduced in the global overlay tunnel and VTEP configuration levels.

- For configuring the source port range globally, use the following command:

```
ACOS(config)# overlay-tunnel options src-port-range min-port <1-65535> max-port <1-65535>
```

- For configuring the source port range per VTEP, use the following command:

```
ACOS(config)# overlay-tunnel vtep 10
ACOS(config-overlay-tunnel:10)# src-port-range min-port <1-65535> max-port <1-65535>
```

Platforms

ACOS 6.0.1 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

vThunder Supports Ubuntu KVM with SR-IOV, PCI-PT, and Virtio Interfaces

With this release, vThunder supports Ubuntu KVM with SR-IOV, PCI-PT, and Virtio interfaces for ADC and SSLi only. The following are recommended and tested Kernel driver and firmware for 100G NICs:

NIC Card	Kernel Driver	Firmware
Intel E810	ICE 1.3.2	3.2
NVIDIA Mellanox ConnectX-5 Ex	5.8-2.0.3.0-LTS	16.35.2000-LTS
NVIDIA Mellanox ConnectX-6 Dx	5.8-2.0.3.0-LTS	22.36.1010-LTS

To enable the KVM SR-IOV support on Mellanox ConnectX-5 Ex and Mellanox ConnectX-6 Dx, see the NIVIDIA Mellanox documentation website.

NOTE:

- vThunder virtual machines in KVM supports SSLi for QAT card (C62x Chipset QuickAssist Technology).
- With Ubuntu KVM SR-IOV interfaces, it is recommended to enable the trust mode and disable spoof for all VFs. Use the below commands:
  - To set the trust mode on, use the `ip link set dev <interface_name> vf <vf_id> trust on` command on the host.
  - To set the spoof off, use the `ip link set dev <interface_name> vf <vf_id> spoof off` command on the host.

Internal Thunder Observability Agent Support

ACOS supports a new in-built plugin called Internal Thunder Observability Agent (iTOA). This plugin provides the capability to publish the vThunder-ADC logs, metrics,

or both to the cloud monitoring services.

The iTOA offers the following capabilities for vThunder-ADC:

- Manages the data collection, processing, aggregation, and publishing internally for configured L3V partitions using aXAPI or CLI commands.
- Enables and configures performance metrics monitoring to publish the 14 vThunder metrics on AWS CloudWatch, Azure Application Insights, and vRealize Operations Manager (vROps).
- Enables and configures the syslog monitoring to publish the vThunder Syslogs on AWS CloudWatch, Azure Log Analytics Workspace, and vRealize Log Insight (vRLI).
- Supports a maximum of 20 partitions per vThunder instance.
- Publishes metrics or logs every 1 minute.

CLI Configuration

The following commands enable the vThunder ADC logs and metrics monitoring on AWS.

To import AWS credentials and AWS configuration file:

```
ACOS(config)#admin adminuser
ACOS(config-admin:adminuser)#cloud-cred aws-cred import <file_transfer_
method>
ACOS(config-admin:adminuser)#cloud-cred aws-config import <file_
transfer_method>
```

To enable log monitoring:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#log
ACOS(config-cloud-provider-aws-log)#enable
ACOS(config-cloud-provider-aws-log)#log-group-name name
ACOS(config-cloud-provider-aws-log)#active-partitions name
```

To enable metrics monitoring:

```
ACOS(config)#cloud-services cloud-provider
ACOS(config-cloud-provider)#aws
ACOS(config-cloud-provider-aws)#metrics
ACOS(config-cloud-provider-aws-metrics)#enable
ACOS(config-cloud-provider-aws-metrics)#active-partitions name
ACOS(config-cloud-provider-aws-metrics)#namespace name
ACOS(config-cloud-provider-aws-metrics)#cps enable
ACOS(config-cloud-provider-aws-metrics)#cpu enable
ACOS(config-cloud-provider-aws-metrics)#disk enable
ACOS(config-cloud-provider-aws-metrics)#interfaces enable
ACOS(config-cloud-provider-aws-metrics)#memory enable
ACOS(config-cloud-provider-aws-metrics)#packet-drop enable
ACOS(config-cloud-provider-aws-metrics)#packet-rate enable
ACOS(config-cloud-provider-aws-metrics)#server-down-count enable
ACOS(config-cloud-provider-aws-metrics)#server-down-percentage enable
ACOS(config-cloud-provider-aws-metrics)#server-error enable
ACOS(config-cloud-provider-aws-metrics)#sessions enable
ACOS(config-cloud-provider-aws-metrics)#ssl-cert enable
ACOS(config-cloud-provider-aws-metrics)#throughput enable
ACOS(config-cloud-provider-aws-metrics)#tps enable
```

For more information on the CLI commands, see the *Command Line Interface Reference*.

For enabling the vThunder ADC logs and metrics on Azure and VMware, see the respective *vThunder Installation Guides*.

Limitation

The Internal Thunder Observability Agent (iTOA) and High Availability (HA) uses the same cloud credentials. The location and filename of the Cloud Credentials Import files and HA credentials files for AWS and Azure are the same. So, if the HA is already configured for AWS or Azure, the new **cloud-cred** import files override the existing HA credentials file. Similarly, if cloud credentials for iTOA is already configured, the new HA credentials file overrides the existing **cloud-cred** import file.

The following files have the same location for Cloud Credentials Import and HA:

- /a10data/.aws/config
- /a10data/.aws/credentials
- /a10data/.azure/credentials

Increased L4 Concurrent Sessions

The number of L4 concurrent sessions per processing unit (PU) has been increased based on the system memory size. This enhancement improves the system performance and enables concurrent processing of large-scale requests.

The software enhancements have been integrated into ACOS 5.2.1-P6-SP1 release onwards. The following Thunder models support the increased L4 concurrent sessions:

- Thunder 7655S - up to 768M (million)
- Thunder 6655S - up to 384M

This means that per PU can support 384M concurrent sessions if the memory per PU is 192 GB and above.

CLI Configuration

To set the total concurrent sessions, use the **system resource-usage l4-session-count** command.

```
TH7655S(config)# system resource-usage l4-session-count ?
<16777216-402653184> Total Sessions in the System
```

NOTE: A reboot is required to apply the setting.

Show Command

- To view the hardware information, use the **show hardware detail** command.

```
TH7655S#show hardware detail
Thunder Series Unified Application Service Gateway TH7655S
      Serial No   : TH76025020240018
      CPU         : Intel(R) Xeon(R) Gold 6258R CPU @ 2.70GHz
                    56 cores
```

```
                    7 stepping
      Storage     : Single 238G drive, Free storage is 89G
      Memory      : Total System Memory 191699 Mbytes, Free Memory
122074 Mbytes
      SSL Cards   : 9 device(s) present
                    9 QAT SSL device(s)

      L2/3 ASIC   : 3 device(s) present
      IPMI        : IPMI Present
      SP Engine   : Present

      Ports       : 16
      Flags       : CF
      SMBIOS      : Build  5.14
                     07/22/2020
      FPGA        : 4 instance(s) present
                    Date: 12/02/2021
      MCPLD Type  : 4
                    Date: 05/05/2020
```

- To view the sessions per PU, use the **`show session`** command.

```
TH7655S# show session
Processing-Unit 1
Traffic Type                          Total
-----------------------------------------------
Total Sessions                        0
TCP Established                       0
TCP Half Open                         0
Server TCP Established                0
Server TCP Half Open                  0
SCTP Established                      0
SCTP Half Open                        0
UDP                                   0
Non TCP/UDP IP sessions               0
Other                                 0
Reverse NAT TCP                       0
Reverse NAT UDP                       0
```

```
Curr Free Conn                          402562828   (384*1024*1024)
Conn Count                              0
Conn Freed                              0
TCP SYN Half Open                       0
Blacklist sessions                      0
Blacklist sessions Created              0
Blacklist sessions Freed                0
Conn SMP Alloc                          189
Conn SMP Free                           0
Conn SMP Aged                           0
Conn Type 0 Available                   801570816
Conn Type 1 Available                   402554826
Conn Type 2 Available                   200392704
Conn Type 3 Available                   100196352
Conn Type 4 Available                   50098176
Conn SMP Type 0 Available               801570816
Conn SMP Type 1 Available               400785408
Conn SMP Type 2 Available               200392704
Conn SMP Type 3 Available               100204354
Conn SMP Type 4 Available               50098176
Total Local Sessions                    0
```

- To view the maximum capacity per PU, refresh the command every second. (Press ^C to quit)

```
TH7655S# show session
Processing-Unit 1
Traffic Type                            Total
-----------------------------------------------
Total Sessions                          402542595
TCP Established                         0
TCP Half Open                           0
Server TCP Established                  0
Server TCP Half Open                    0
SCTP Established                        0
SCTP Half Open                          0
UDP                                     402542595
Non TCP/UDP IP sessions                 0
```

```
Other                                0
Reverse NAT TCP                      0
Reverse NAT UDP                      0
Curr Free Conn                       8075
Conn Count                           402542595
Conn Freed                           0
TCP SYN Half Open                    0
Blacklist sessions                   0
Blacklist sessions Created           0
Blacklist sessions Freed             0
Conn SMP Alloc                       116
Conn SMP Free                        0
Conn SMP Aged                        0
Conn Type 0 Available                0
Conn Type 1 Available                0
Conn Type 2 Available                0
Conn Type 3 Available                0
Conn Type 4 Available                0
Conn SMP Type 0 Available            0
Conn SMP Type 1 Available            0
Conn SMP Type 2 Available            0
Conn SMP Type 3 Available            8075
Conn SMP Type 4 Available            0
Total Local Sessions                 0
```

- To view the memory usage information, use the **`show memory`** command.

```
TH7655S# show memory
         Total(KB)      Used         Free        Usage
-------------------------------------------------------------
Memory:  191699152      68985250     122713902   35.90%
```

Scaleout

ACOS 6.0.1 introduces the following new feature and enhancement for Scaleout:

NOTE: For Scaleout specific configuration steps, refer *Scaleout Configuration Guide*.

The following topic is covered:

VCS Enhancement for Scaleout Stability

In the ACOS 6.0.1 release, the VCS disable and reload features are further enhanced to maintain Scaleout stability:

- VCS Reload - To reload the VCS and ensure the stability of the Scaleout cluster and uninterrupted traffic.

  The **db-safe** option allows Scaleout to ignore any node joining or leaving the cluster and any change in the traffic map during the reload process.

- VCS Disable - To disable the VCS configuration and database synchronization independently.

  The `vcs disable` command disables configuration synchronization and the `vcs database-distribution disable` command disables database synchronization.

CLI Configurations

- To disable the configuration synchronization, use the following command:

  ```
  vcs disable
  ```

- To disable the database synchronization, use the following command:

  ```
  vcs database-distribution disable
  ```

- To enable the db-safe mode for VCS reload feature, use the following command:

  ```
  ACOS(config)# vcs reload db-safe {start [timeout <seconds>] | complete
  force | device <device id>
  ```

  - `start` - To initiate the db-safe in VCS reload feature and keep the Scaleout cluster uninterrupted.
  - `start [timeout <seconds>]` - To configure the db-safe mode automatically based on the specified timeout value. The timeout value is 5-300 seconds (about 5 minutes).

- `complete force` - To complete the db-safe vcs reload within the specified timeout or after the timeout.
- `device <device-id>` - To reload a specific device when aVCS is enabled. The device ID can be between 1-16.

Show Commands

The `show vcs summary` output is further enhanced to:

- Display the enabled status information of the configuration synchronization and database synchronization.
- Display a message DB-SAFE-RELOAD-MODE displays in the VCS Database-distribution Enabled field when the db-safe vcs is reloading.

System Configuration and Administration

ACOS 6.0.1 introduces the following new feature and enhancement for System Configuration and Administration:

NOTE: For more information and details, refer *System Configuration and Administration Guide*.

The following topic is covered:

Import-Periodic Multi-PU Platform Support

When the `import-periodic` command is used on the multi-PU platform, Processing Unit 1 (PU1) and Processing Unit 2 (PU2) try to fetch files from the remote server. However, PU2 may encounter issues while fetching the files from the remote server if the management interface is not connected.

In this release, the imported files are automatically synced from PU1 to PU2, ensuring that PU2 can periodically and locally update the files. This also helps both PU1 and PU2 to import the same files.

The `import-periodic` command supports the following file types:

```
aflex                 aFleX Script Source File
auth-jwks             JSON web key
auth-portal           Portal file for http authentication
bw-list               Black white list files
ca-cert               SSL CA Cert File(enter bulk when import an archive
file)
class-list            Class list files
class-list-convert    Convert Class List File to A10 format
dnssec-dnskey         DNSSEC DNSKEY(KSK) file for child zone
dnssec-ds             DNSSEC DS file for child zone
geo-location          Geo-location CSV File
local-uri-file        Local URI files for http response
rpz                   Response Policy Zone File
ssl-cert              SSL Cert File(enter bulk when import an archive file)
ssl-cert-key          Bulk file
ssl-crl               SSL Crl File
ssl-key               SSL Key File(enter bulk when import an archive file)
thales-kmdata         import Thales Kmdata files
thales-secworld       import Thales security world files
tsig                  Transaction SIGnatures Key File
xml-schema            XML-Schema File
```

The following is an example of the `import-periodic` command of the scp file type:

```
import-periodic ssl-crl ssl-crl-file use-mgmt-port
scp://root:password@10.64.44.106/root/dataFile/crl.dat period 300
```

NOTE: When the import-periodic task is removed, the task will be deleted from PU2.

Security Updates

The following security vulnerabilities are addressed in the ACOS 6.0.1 release:

- OpenSSL Vulnerabilities
  - CVE-2023-0286: A Type confusion vulnerability related to processing of X.400 address.

- CVE-2023-0215: A public API helper function BIO_new_NDEF vulnerability related to streaming ASN.1 data via a BIO.
- CVE-2022-4304: A timing-based side-channel vulnerability in the OpenSSL RSA Decryption padding modes: PKCS#1 v1.5, RSA-OEAP, and RSASVE.

- Linux Kernel Vulnerabilities
  - CVE-2023-0394: A NULL pointer dereference vulnerability related to rawv6_push_pending_frames.
  - CVE-2022-3594: A function intr_callback vulnerability in the BPF component of the drivers/net/usb/r8152.c file.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.0-P2

This topic provides a brief overview of the new feature and enhancement added in the ACOS 6.0.0-P2 release:

The following topic is covered:

Threat Protection System

ACOS 6.0.0-P2 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to *DDoS Mitigation Guide*. Similarly, for TPS-related CLI commands, refer to *DDoS Command Line Reference Guide*.

Enhancements in ACOS 6.0.0-P1

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.0-P1 release:

The following topics are covered:

Platforms

ACOS 6.0.0-P1 introduces the following new features and enhancements for ACOS Platforms:

The following topic is covered:

Enhanced Password Policy Management

The ACOS system separates EXEC CLI sessions into two different access levels – “User EXEC” and “Privileged EXEC” for security purposes. The “Privileged EXEC” level is also known as “enable” level. It provides access to all the ACOS commands. Access to this level can be password protected so that only authorized users can configure or maintain the ACOS system.

In this release, ACOS provides additional security feature for administrators to enforce or validate the password complexity policy for the enable level users. When this feature is enabled, the password-policy complexity configured at the system level is enforced while setting the ‘enable-password’. The system validates the password entered based on the password complexity requirement. The password is rejected if it does not meet the specified requirement.

NOTE: If the password-policy complexity is not configured, the input in the enable-password is not checked for compliance.

Example If the password-policy complexity is set to Medium aging repeat-character-check, “a@LE6” as the enable-password will be rejected. This password is not long enough for “Medium complexity”. “A10@aaPAs” will also be rejected as it does not comply with the duplicate character check. “A10@aPAs” will be accepted.

For more information on System Password Policy Complexity, see the *Management Access and Security Guide* and the *System Configuration and Administration Guide*.

CLI Configuration

```
ACOS(config)# system enable-password follow-password-policy
```

Security Update

This release addresses CVE-2023-0286- A Type Confusion Vulnerability relating to X.400 address in OpenSSL.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 6.0.0

This topic provides a brief overview of the new features and enhancements added in the ACOS 6.0.0 release:

The following topics are covered:

Application Delivery Controller

ACOS 6.0.0 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for ADC specific CLI commands, refer *Command Line Reference Guide*.

The following topics are covered:

HTTP/3 Load Balancing

ACOS supports HTTP version 3 (HTTP/3) protocol for server load balancing. HTTP/3 uses QUIC, a UDP based transport protocol that provides a reliable connection for multiplexing several requests and a faster response time. The HTTP/3 configuration is supported for the following features:

- Content Compression
- URL/Host Switching
- Client IP/Port insertion
- URL redirect/redirect-rewrite
- Request Header insertion/erasure
- Request timeout
- Response Content replacement
- Response Header insertion/erasure
- RAM Caching
- HTTP/3 health monitoring
- QUIC-TLS offloading with backend HTTP/1.1, HTTP/2, or HTTP/3
- Decode HTTP

ACOS supports QUIC load balancing by leveraging several QUIC functionalities described in various RFCs, such as:

- 8999 - Version-Independent Properties of QUIC
- 9000 - QUIC: A UDP-based Multiplexed and Secure Transport
- 9001 - Using TLS to Secure QUIC

CLI Configuration

- To process HTTP/3 traffic, use the **http-over-quic** virtual server port.

```
ACOS(config)# slb virtual-server vip 10.10.10.10
ACOS(config-slb vserver)# port 443 http-over-quic
```

- To enable HTTP/3 health monitoring, use the **http-version3** method.

```
ACOS(config)# health monitor h3
ACOS(config-health:monitor)# server-ssl st
ACOS(config-health:monitor)# method https http-version3
```

- To control the QUIC connection parameters, use the **slb template quic** command.

```
ACOS(config)# slb template quic quic_http3
ACOS(config-quic)# connection-id-length <1-20 bytes>
ACOS(config-quic)# idle-timeout <1-3600 seconds>
ACOS(config-quic)# key-update-to-client
ACOS(config-quic)# key-update-to-server
ACOS(config-quic)# receive-buffer <30000-400000 bytes>
ACOS(config-quic)# server-retry
```

Show Commands

- To view the health monitor statistics, use the **show health** command.
- To view the HTTP/3 statistics, use the **show slb http3** command.
- To view the QUIC statistics, use the **show slb quic** command.
- To view the QUIC sessions, use the **show session quic** command.

aFleX Commands and Events

For 'http-over-quic' virtual port, the following aFleX commands and events are introduced:

QUIC Commands

- QUIC::CID - This command returns the current QUIC connection ID from client.
- QUIC::version - This command returns the current QUIC version being used from client.

QUIC Events

- QUIC_INITIAL - Execute the specific aFleX commands when the first initial packet is received from the client side.

- QUIC_CLIENT_ACCEPTED - Executes the specific aFleX commands after the SSL handshake is complete and the client connection is established with the ACOS device.
- QUIC_CLIENT_CLOSED – Executes the specific aFleX commands after the client side connection is closed.

Limitation

QUIC does not support early data in the server-SSL template. Hence, configuring this command may result a reboot when the traffic is flowing.

HTTP Brotli Compression

Brotli (RFC 7932) is a lossless compression technique that compresses data utilizing a combination of the LZ77 algorithm, Huffman coding, and 2nd order context modelling. Web servers and content delivery networks use Brotli to compress HTTP data, resulting in faster page load, and reducing the bandwidth consumption.

ADC supports Brotli compression and decompression whenever it is necessary. The following functionalities are included in this feature:

- Decodes/encodes the incoming HTTP traffic when the sliding window value of the compression is acceptable.
- Extends RAM Cache support for HTTP response caching when it is compressed in Brotli format.
- Supports the existing compression features in the HTTP template.
- Supports both the HTTP/2 and HTTP 1.1 protocols (if the 'method-order' is specified in the HTTP template).
- Supports aFlex commands.

CLI Configuration

- To enable the Brotli compression algorithm, use the following compression command in the HTTP Template.

```
ACOS(config)# slb template http http_brotli
ACOS(config-http)# compression enable
ACOS(config-http)# compression brotli-level 1
```

```
ACOS(config-http)# compression brotli-sliding-window 2
ACOS(config-http)# compression method-order "gzip brotli"
```

To view the Brotli compression ratio and statistics, use the following show commands:

- **show slb compression**
- **show slb http-proxy**
- **show slb virtual-server**

GUI Configuration

To enable the Brotli compression algorithm, go to **ADC > Templates > L7 Protocols > HTTP > Compression** section.

aFleX Commands

To enable the Brotli compression algorithm, use the following aFleX commands:

- COMPRESS::brotli level
- COMPRESS::brotli sliding-window
- COMPRESS::method-order

HTTP/2 SSL Offload without SNAT

ACOS supports HTTP/2 SSL offloading capability that does not require the source NAT participation. The 'http2-client-no-snat' feature can be utilized to dynamically adjust the max-concurrent-stream value when the source NAT is not configured on the virtual port, and the client-side is HTTP/2 when the server-side is HTTP 1.1.

In this case, the max-concurrent-streams will be set to '1' until the server supports HTTP2 and accepts other values.

CLI Configuration

```
ACOS(config)# slb template http test
ACOS(config-http)# http2-client-no-snat
```

GUI Configuration

To enable this feature, go to **ADC > Templates > L7 Protocols > HTTP > General**

Fields section.

Support HTTP/2 for Health Monitoring

In this feature, health-check is supported for HTTP/2 or HTTPS at real-port and service-group levels.

NOTE:

The following options under HTTP/2 and HTTPS are not supported:

- kerberos-auth
- text-regex
- disable-sslv2hello

CLI Configuration

- The following command is introduced under the http command in method:
  - **version2** - Configure this command to specify HTTP version 2
- The following command is introduced under the https command in method:
  - **http-version2** - Configure this command to specify HTTP version 2 for HTTPS.

    For choosing the cipher list for SSL handshake, the server-ssl template (server side SSL template for health monitor) must be applied to the health-monitor as mentioned in the following example:

```
ACOS (config)#health monitor https
ACOS (config-health:monitor)#server-ssl hm-server-ssl
ACOS (config-health:monitor)#method https http-version2
```

GUI Configuration

Go to **ADC > Health Monitors**. The **HTTP version 2** option is available under **Create Health Monitor** page while configuring a health monitor with method type **HTTP** or **HTTPS**.

DNS64 Functionality

DNS64 supports the communication between IPv6 environment and IPv4 server. This feature provides the address transfer and converts the request type if the server does not have the IPv6 interface to serve the client.

This feature is already available in the CGN **dns template**. A few commands are now extended in the **slb template dns**.

NOTE: This feature cannot be used with recursive resolution tags.

CLI Configuration

dns64 can be configured in the slb template dns:

```
ACOS(config)#slb template dns
ACOS(config-dns)#dns64 enable
```

NOTE: IPv4 service-group must be used with source-pool on the port.

The following commands are introduced in the **dns64**:

- `cache` - Uses a cached A-query response to provide AAAA query responses for the same hostname.
- `change-query` - Changes incoming AAAA DNS query to A query.
- `parallel-query` - Forwards the AAAA queries and generates the A query in parallel.
- `retry` - Specifies the maximum number of times the ACOS device retries an A query, if a response is not received from the DNS server. The default value is 3 and the configurable range is 0-15.
- `single-response-disable` - Disables the single response. When the single response is disabled, the ACOS device forwards both responses to the server, if both the responses are valid.
- `timeout` - Specifies the maximum number of seconds the ACOS device waits for an AAAA response before sending an A query. The default value is 1 second and the configurable range is 0-15.

Only dns-udp port is supported for the following options:

- `parallel-query`
- `retry`
- `timeout`

GUI Configuration

Go to **ADC > Templates > L7 Protocols > Create > DNS**. On the **Create DNS Template** page, select **Enable DNS64** to see the following options:

- **Use a cached A-query response to provide AAAA query responses for the same hostname** - Select this option to use a cached A-query response to provide AAAA query responses for the same hostname.
- **Always change incoming AAAA DNS query to A** - Select this option to change incoming AAAA DNS query to A query.
- **Forward AAAA query & generate A query in parallel** - Select this option to forward the AAAA queries and generate the A query in parallel.
- **Retry count** - Specify the maximum number of times the ACOS device retries an A query, if a response is not received from the DNS server. The default value is 3 and the configurable range is 0-15.
- **Disable Single Response which is used to avoid ambiguity** - Select this option to disable the single response. When the single response is disabled, the ACOS device forwards both responses to the server, if both the responses are valid.
- **Timeout to send additional Queries (second)** - Specifies the maximum number of seconds the ACOS device waits for an AAAA response before sending an A query. The default value is 1 second and the configurable range is 0-15.

Global DNS Cache Synchronization

Enabling DNS cache optimizes CPU utilization on the active ACOS device because most DNS requests get served directly through the cache. However, a failover event can cause the CPUs to spike on the standby ACOS device because the device has to resolve all destination hosts in bulk. This CPU spike becomes amplified if recursive DNS service is also enabled.

To alleviate this issue, the ACOS 6.0.0 release introduces DNS cache entry synchronization. Upon failover, the standby device stays ready to resolve DNS queries from cache.

NOTE: The synchronized messages that are lost cannot be recovered.

The CLI commands to configure global DNS cache synchronization are mentioned below:

CLI Configuration

To configure global DNS cache synchronization, the following commands are introduced under `slb common`:

- `dns-cache-sync` - This command enables high availability (HA) synchronization.

  For example,

  ```
  ACOS(config)#slb common
  ACOS(config-common)#dns-cache-sync
  ```

- `dns-cache-sync-entry-size` - This command configures DNS cache entries with smaller size to be synchronized to the standby device. The default value is 256 bytes and the configurable range is 1-4096.

  For example,

  ```
  ACOS(config)#slb common
  ACOS(config-common)#dns-cache-sync
  ACOS(config-common)#dns-cache-sync-entry-size 500
  ```

- `dns-cache-sync-ttl-threshold` - This command configures DNS cache entries with higher TTL value to be synchronized to the standby device. The default value is 0 seconds and the configurable range is 0-10000000.

  For example,

  ```
  ACOS(config)#slb common
  ACOS(config-common)#dns-cache-sync
  ACOS(config-common)#dns-cache-sync-ttl-threshold 300
  ```

DNS Firewall Support with DoH

When the DoH (DNS over HTTP/HTTPs) feature is configured on ACOS, the DNS traffic decapsulated from DoH is forwarded to a DNS service-group. With the support of the service-chaining feature, the DNS traffic can be forwarded to a DNS vport on the same partition for additional DNS features such as DNS firewall, GSLB and other DNS features. However, this requires the packet to be processed twice, once for DoH and once for the DNS vport.

To avoid the dual processing, the DNS firewall features in this release can be deployed on the DoH traffic without requiring any service-chaining.

To support DNS Firewall with DoH, bind a DNS template in the DoH template. The following DNS features are supported for a DNS template when it is bound in the DoH template:

- DNS query/response existing scrubbing features
- DNS query type/class filtering
- DNS response rate limiting
- DNS logging template
- DNS caching
- EDNS client subnet

Limitations

The following features in the DNS template are not supported when it is bound in a DoH template:

- Class-list (Class-list based rate limiting is supported at the HTTP vport level and not at the DNS packet level)
- GSLB (DNS vport feature)
- Query-id-switch
- Recursive DNS resolver
- DNSSEC service group
- Malformed-query forwarded to another service-group

- udp-retransmit (This command does not apply to DoH and is used where dns-tcp vport is bound to udp service-group. DoH UDP retransmits are config controlled in DoH template).

CLI Configuration

To enable DNS Firewall Support with DoH, the following commands are introduced:

- `ACOS(config-doh-forwarder)#bypass-doh` - When this command is configured, the HTTP request is forwarded to the service-group bound and then to the virtual port as is after the DNS template validates the DNS query. This way, DoH forwarding is bypassed for a valid DoH request.

NOTE:
This command is mutually exclusive to the service groups or other forwarding commands.

- `ACOS(config-doh)#template dns <DNS template name>` - This command applies a DNS template to the DoH template.

An example is mentioned below:

```
ACOS(config)#slb template doh DoH_Template
ACOS(config)#template dns dns_template
ACOS(config-doh)#forwarder
ACOS(config-doh-forwarder)#bypass-doh
```

GUI Configuration

Go to **ADC > Templates > L7 Protocols > Create > DNS**. On the **Create DNS Template** page, the following new option is added:

- **DNS Template** - Select the option to bind a DNS template to the DoH template. Select from the list of predefined DNS templates. This option enables the DNS Firewall support with DoH.

  NOTE: When a user has **read** permission and the **Lineage slb.template.dns** is set to **write**, only then the **DNS Template** field is visible to the user.

Enhanced DNS Logging Template

In the previous releases, ACOS supported the request log as dns-logging template. With this release, response log is also supported to log content from the DNS server response.

NOTE: Only remote log is supported for DNS logging. The remote log must use acos-events. For more details about the ACOS-events, see *Event Logging Guide*.

DNS Minimal Response Support for Recursive Lookup

With this release, ADC supports DNS minimal response for recursive lookup. When this option is configured, the 'Authority' and 'Additional' sections are removed from the query response before returning the output to the client.

Minimal response is bypassed in the following scenarios:

- Negative response (NXDOMAIN and NODATA)
- Delegation

NOTE:

- The sections will not be removed for EDNS(0) as they follow bind server behavior.
- The complete response is saved in cache. If the cache is shared, other users will be able to access the complete response unless they have minimal-response configured.

CLI Configuration

To enable 'Minimal Response', configure the following command:

```
ACOS(config)# slb template dns test
ACOS(config-dns)# recursive-dns-resolution
ACOS(config-dns-recursive-dns-resolution)# minimal-response
```

GUI Configuration

To enable the feature, go to **ADC > Templates > L7 Protocols > Create > DNS**. On the **Create DNS Template** page, select the **Recursive Dns Resolution** option to see the

Minimal Response checkbox.

EDNS(0) Client Subnet Support for ADC DNS

The existing DNS template is enhanced by introducing an option to insert Extension mechanism for DNS (EDNS(0)) Client Subnet in a query. This extension contains sufficient network information and allows a recursive DNS resolver to specify the network subnet for the host on whose behalf the DNS query is made. It also helps to speed up the delivery of data from the content delivery networks by allowing better use of the DNS-based load balancing.

NOTE:

- This feature is supported for 'DNS-UDP' and 'DNS-TCP' type virtual server ports.
- This feature is supported for DNS over HTTPs (DoH). An HTTP port with DOH can be bound to a DNS template.

DNS Recursive Lookup Order

ACOS supports specifying the lookup order for each query type in recursive DNS lookup when both IPv4 and IPv6 nat-pools are configured. ACOS performs lookup via the preferred IP protocol. In case of failure, the lookup is performed with the secondary IP protocol.

CLI Configuration

To configure the lookup order for each DNS query type, the following commands are introduced in the `recursive-dns-resolution`:

- `lookup-order` - Specify the lookup order for each DNS query type individually using the preferred IP protocol for resolver to perform lookup via IPv4 or IPv6. The following options are available:
  - `query-type` - Specify the query type from the following options:
    - `A` - Address record
    - `AAAA` - IPv6 Address record

- `CNAME` - Canonical name record
- `MX` - Mail exchange record
- `NS` - Name server record
- `SRV` - Service locator
- `PTR` - PTR resource record
- `SOA` - Start of authority record
- `TXT` - Text record
- `ANY` - All cached record
- `<1-65535>` - Other query type value

Specify one of the following options for the query types mentioned above:

- `ipv4-precede-ipv6` - Recursive lookup is performed via IPv4. In case of failure, IPv6 is used.
- `ipv6-precede-ipv4` - Recursive lookup is performed via IPv6. In case of failure, IPv4 is used.

GUI Configuration

Go to **ADC > Templates > L7 Protocols > Create > DNS**. On the **Create DNS Template** page, select the **Recursive Dns Resolution** to see the **Lookup Order** option. Click **Add** to specify the details:

- **Query Type** - Select the query type from the list.
- **Type Value** - This field is activated when 'NUMBER' is selected as 'Query Type'. The configurable range is 1 to 65535.
- **Order** - Select one of the following options:
  - **Ipv4 Precede Ipv6** - Recursive lookup is performed via IPv4. In case of failure, IPv6 is used.
  - **Ipv6 Precede Ipv4** - Recursive lookup is performed via IPv6. In case of failure, IPv4 is used.
- **Action** - Click the 'Save' icon to save the entry.

Enhanced Recursive DNS Resolution

New commands are added to Recursive DNS Resolution:

- To configure the maximum number of total trials that ACOS performs before quitting the recursive process.
- To configure the maximum number of retries at each level of the DNS resolution process.

CLI Configuration

As an enhancement to `recursive-dns-resolution`, the following commands are introduced:

- `max-trials` - This command configures the maximum number of total trials that ACOS performs, cumulative of all levels based on client DNS queries, before quitting the recursive process.
  The default value is 30 and the configurable range is 1-62.
- `retries-per-level` - This command configures the maximum number of retries at each level of the DNS resolution process.
  The default value is 6 and the configurable range is 1-6.

GUI Configuration

Go to **ADC > Templates > L7 Protocols > Create > DNS**. On the **Create DNS Template** page, select **Recursive Dns Resolution** to see the following options:

- **Retries Per Level** - This option configures the maximum number of retries at each level of the DNS resolution process.
  The default value is 6 and the configurable range is 1-6.
- **Max Trial** - This option configures the maximum number of total trials that ACOS performs, cumulative of all levels based on client DNS queries, before quitting the recursive process.
  The default value is 30 and the configurable range is 1-62.

Recursive DNS Gateway Health Monitoring

ACOS supports health monitoring for recursive DNS Gateways. This feature is useful when the recursive DNS resolver cannot serve queries due to system misconfiguration or an Internet outage. The recursive gateway's health status will also be considered when determining the state of the virtual port. This aids in the efficient management of load balancing resources.

By enabling the health monitoring, ACOS periodically performs recursive resolution based on system and template wide configuration.

- When the recursive DNS resolution is complete and the final answer is found, the gateway is considered UP.
- When the recursive DNS resolver does not receive the final answer (or no matched type record), or an error occurs during the process, the gateway is considered DOWN.

CLI Configuration

To configure this feature, enable **`recursive-dns-resolution`** first and then **`gateway-health-check`** commands under SLB template DNS. The following health monitoring options are available:

- *`interval`* - Number of seconds between health check attempts.
- *`retry`* - Maximum number of times the DNS query retries at each server level before determining the health check failed.
- *`retry-multi`* - Number of times the health check consecutively fails before determining the gateway is DOWN.
- *`timeout`* - Period (in seconds) that recursive resolver waits for a reply to a health check.
- *`up-retry`* - Number of times the health check consecutively passes the same before determining the gateway is UP.
- *`ns-cache-lookup`* - Lookup NS record cache during the health check process.
- *`query-name`* - Query name of the probe DNS queries.
- *`query-type`* - Query type of the probe DNS queries.

```
ACOS(config)# slb template dns temp
```

```
ACOS(config-dns)# recursive-dns-resolution
ACOS(config-dns-recursive-dns-resolution)#gateway-health-check
ACOS(config-dns-recursive-dns-resolution-...)# interval 4
ACOS(config-dns-recursive-dns-resolution-...)# up-retry 2
```

Support Negative Caching of DNS Responses

ACOS supports negative caching or caching the negative responses for a domain. A negative response indicates that the requested domain information is unavailable or that the server is unable to respond to the query. This feature enhances query responses while decreasing backend DNS traffic.

DNS caches the negative responses when the query contains:

- CNAME and SOA records
- NS and SOA records
- Empty response and SOA records

CLI Configuration

- To enable negative caching globally, the following command is introduced under SLB common:

```
ACOS(config)#slb common
ACOS(config-common)# dns-negative-cache enable
```

- To enable negative caching per virtual port, the following commands are introduced under SLB template DNS:

```
ACOS(config)# slb template dns dns_negative
ACOS(config-dns)# negative-dns-cache enable
ACOS(config-dns-negative-dns-cache:)# bypass-query-threshold <number>
ACOS(config-dns-negative-dns-cache:)# max-negative-cache-ttl <seconds>
```

Show Command

- To view the global negative cache entries, use the **show dns cache entry** show command.

- To view the per VIP negative cache entries, use the **show slb virtual-server** show command.

Display DNS Response Record in DNS Cache

ACOS supports display of DNS cache entry information, client statistics and cache statistics. With this release, the resource records in DNS cache entry can also be displayed.

CLI Configuration

The following commands are introduced in the **show dns cache entry** and **show dns cache global**:

- `brief` - Displays the DNS response resource records of the cache entry in brief. It displays only the answer section.
- `detail` - Displays the DNS response resource records of the cache entry in detail. It displays the answer section, authority section and additional section.

  The following sub-options are available in the options **brief** and **detail**:

  - `max-rdata-size` - Specify the maximum rdata size for each record. Specify one of the following options:
    - `<1 to 8192>` - Specify the maximum rdata size to be displayed for each record.
    - `all` - Displays full content of rdata for each record; maximum limit is 8192 characters.
  - `max-record-num` - Specify the number of maximum records to be displayed for each section of the cache entry. Specify one of the following options:
    - `<1-1024>` - Specify the number of records to be displayed for each section of cache entry.
    - `all` - Displays all the records for each section of cache entry; maximum limit is 1024 records.

GUI Configuration

Go to **ADC > Statistics > L7 > DNS > DNS Cache Entry**. The following options can be selected to view the statistics on this page:

- **Global** - The filter is applied to the DNS cache global entries.
- **Virtual Server** - This field is enabled only when the 'Global' field is disabled. Select the virtual server from the list.
- **DNS Virtual Port** - This field is enabled only after the 'Virtual Server' field is enabled. Then, select the virtual port from the list.
- **Content Mode** - Select one of the following options from the list:
  - **Brief** - Displays the DNS response resource records of the cache entry in brief. It displays only the answer section.
  - **Detail** - Displays the DNS response resource records of the cache entry in detail. It displays the answer section, authority section and additional section.

  The following options are enabled when **Content Mode** is specified:
  - **Max Record Number** - Select 'All' or specify a value between 1-1024.
  - **Max Record Data Size** - Select 'Full' or specify a value between 1-8192.
- **DNS Class** - Select one of the options from the list or specify a value between 1-65535.
- **DNS Type** - Select one of the options from the list or specify a value between 1-65535.
- **Domain Name** - Select from the list (**DNS Domain** or **FQDN Domain**) and specify the **Domain Name**.

Persistent Storage for Global DNS Cache

The DNS cache feature is extended to support persistent storage for saving the cached entries. As a result, the cached entries are loaded from the persistent storage and improves the CPU performance. Additionally, the maximum limit and TTL threshold values can be set for the persistent cached entries.

When recursive DNS server is used in a standalone setup, the DNS cache handles a high number of DNS requests. This can cause high CPU usage when the ACOS device restarts with an empty cache and need to reload the cached DNS entries.

CLI Configuration

To configure persistent storage for global DNS cache, the following commands are

introduced under `slb common`:

- `dns-persistent-cache-enable` - This option enables persistent storage for global DNS cache.

  For example,

```
ACOS(config)#slb common
ACOS(config-common)#dns-persistent-cache-enable
```

- `max-persistent-cache` - Maximum persistent cache entries can be limited using this option. The option can be configured only in a shared partition. The maximum value is the maximum supported DNS cache on the platform.

  For example,

```
ACOS(config)#slb common
ACOS(config-common)#dns-persistent-cache-enable
ACOS(config-common)#max-persistent-cache ?
<1-65536> Maximum persistent cache entry
```

- `dns-persistent-cache-ttl-threshold` - This option sets the TTL threshold value for persistent cache. The DNS cache entries with higher TTL value are saved as persistent cache. The value can be set from 0-10000000. The default value is 0.

  For example,

```
ACOS(config)#slb common
ACOS(config-common)#dns-persistent-cache-enable
ACOS(config-common)#dns-persistent-cache-ttl-threshold 200
```

- `dns-persistent-cache-hit-threshold` - This option saves the DNS cache entries with higher hit count. The value can be set from 0-10000000. The default value is 0.

  For example,

```
ACOS(config)#slb common
ACOS(config-common)#dns-persistent-cache-enable
ACOS(config-common)#dns-persistent-cache-hit-threshold 5
```

Examples of the show commands added for displaying persistent cache statistics and entries are mentioned below:

- Example 1:

```
ACOS#show dns persistent-cache ?
entry          Show DNS Persistent Cache Entry
statistics     Show DNS Persistent Cache Statistics
```

- Example 2:

```
ACOS#show dns persistent-cache entry
                             S = DNSSEC, T = Type, C = Class
                            Qlen = Query length, Rlen = Response length
Domain                                S     T    C    Qlen  Rlen  TTL
-----------------------------------+---+---+-----+-----+-------+------
-
 test.dnsrr.com                       0    2    1    32    90    300
 www.test.dnsrr.com                   0    1    1    36    98    300
 ns3.test.dnsrr.com                   0    1    1    36    26    300
Total: 3
```

- Example 3:

```
ACOS#show dns persistent-cache statistics
                       Total
-----------------------------------------------
Total persistent cache 3
Total saved            3
Total deleted          0
Database Busy          0
Database Error         0
```

A new command and the options that are added for deleting persistent cache statistics and entries are mentioned below:

```
ACOS#clear dns persistent-cache ?
entry          Clear DNS Persistent Cache Entry
statistics     Clear DNS Persistent Cache Statistics
```

RPZ Import Using DNS Zone Transfer with TSIG

The existing Response Policy Zone (RPZ) import feature is enhanced by introducing the standard full zone transfer (AXFR) protocol. Additionally, the Transaction Signature (TSIG) key is employed to add a layer of security during these transactions.

The TSIG key can be generated using DNS Security Extensions (DNSSEC) key generation tool (**dnssec-keygen**).

The **import tsig** command is also introduced to import the TSIG key files on the system.

NOTE: The TSIG public key and the private key must be present on the system while importing an RPZ file using the AXFR protocol.

CLI Configuration

The following commands are introduced:

- To import an RPZ file to the ACOS device using zone transfer with TSIG:

```
ACOS(config)# import rpz <rpz-filename> zone-transfer use-mgmt-port
axfr://[tsig-keyfile@]host/domain-name
```

Example:

```
ACOS(config)# import rpz test.rpz zone-transfer use-mgmt-port
axfr://Krpz.com.+157+20696.key@192.168.93.182/rpz.com
```

- To periodically import an RPZ file to the ACOS device using zone transfer with TSIG:

```
ACOS(config)# import-periodic rpz <rpz-filename> zone-transfer use-
mgmt-port axfr://[tsig-keyfile@]host/domain-name period <seconds>
```

- To import the TSIG key file:

```
ACOS(config)# import tsig <tsig_filename> use-mgmt-port scp://
[user@]host/<tsig_filename>
```

- To display the TSIG key files on the system:

```
ACOS(config)# show tsig
```

GUI Configuration

To import the RPZ file using zone transfer, navigate to **System > Settings > File Management > Import > RPZ > Remote** and enable **Zone Transfer**.

Explicit Proxy with Dual-Stack Forwarding

ACOS is enhanced to support IPv4 and IPv6 dual stack forwarding in explicit proxy mode, starting with the DNS resolution. This solution allows the explicit proxy VIP to serve as a gateway between IPv4 (or IPv6) clients and dual-stacked servers, giving preference to IPv6.

Prior to this feature, although the dual-stacked operation was already supported in ACOS through DNS dynamic service templates as well as separate SLB policy templates, it lacked dynamic address translation or interconnectivity, which could lead to service outages or delays in some cases. For instance, you could configure IPv4 and IPv6 DNS servers on the same dynamic service template, but an IPv4 explicit proxy VIP serving an IPv4 client could only reach out to remote servers over IPv4. Similarly, an IPv6 explicit proxy VIP serving an IPv6 client could only reach out to remote servers over IPv6.

With this feature, once you configure IPv4 and IPv6 DNS servers under the dynamic service template, it behaves as follows:

- An IPv6 DNS server is given preference over an IPv4 server to send DNS requests.
- AAAA (IPv6) and A (IPv4) record requests are sent to the DNS server as two separate requests unless a cached record exists.
- AAAA record replies are preferred over A records.
- Based on the DNS response, the appropriate source NAT pool i.e., either IPv6 NAT-pool or IPv4 NAT-pool is used.

This enables an explicit proxy virtual port to forward HTTP or HTTPS requests via IPv4 or IPv6 networks. Additionally, when this feature is configured, the SSLi certificate fetching module also allows connections with IPv4 addresses on the client side and IPv6 addresses on the server side and vice versa.

NOTE: This feature is not applicable to Transparent Proxy and Proxy chaining.

CLI Configuration

To enable this feature, you need to configure the **`dual-stack-action`** command under **`forward-policy`** in the SLB template policy and then bind the action to any destination rule of the forward policy.

The following example demonstrates the **dual-stack-action** command usage:

```
ACOS(config)# slb template policyDUAL_Stack_6n4
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# dual-stack-action FWD_6n4
ACOS(config-policy-forward-policy-dual-st...)# ipv4 To_Internet_v4 snat
EP_POOL_v4
ACOS(config-policy-forward-policy-dual-st...)# ipv6 To_Internet_v6 snat
EP_POOL_v6
ACOS(config-policy-forward-policy-dual-st...)# fallback To_Internet_v6
snat fall_back_v6
ACOS(config-policy-forward-policy-dual-st...)# log
ACOS(config-policy-forward-policy-dual-st...)# exit

ACOS(config-policy-forward-policy)# source ANY
ACOS(config-policy-forward-policy-source)# match-any
ACOS(config-policy-forward-policy-source)# destination any dual-stack-
action FWD_6n4
```

Preserve Client IP for Explicit Proxy Custom Ports

ACOS provides full non-standard port support without SNAT to preserve the original client IP address in the Explicit Proxy environment. This feature benefits in various scenarios such as statistics collection and analysis based on client IP address and many more.

A new 'port-translation-only' option is introduced in the SLB policy template under forward-policy actions:

- forward-to-internet
- forward-to-service-group
- forward-to-proxy

CLI Configuration

```
ACOS(config)# slb template policy p1
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# action aaa
ACOS(config-policy-forward-policy-action)# forward-to-internet http snat
port-translation-only
```

```
ACOS(config-policy-forward-policy-action)# forward-to-service-group http
snat port-translation-only
ACOS(config-policy-forward-policy-action)# forward-to-proxy http
support-cert-fetch snat port-translation-only
```

GUI Configuration

- To enable the Port Translation Only feature, go to **Security > Forward Proxy > Template > Policy > Create**.
- To view the source port translation statistics, go to **Security > Forward Proxy > Statistics > Policy Source Port Translation Only** tab.

Support Health Check with HA Proxy Header

This feature supports health check with HA (High Availability) proxy header. Using the HA proxy protocol, the connection information such as a client's address can be communicated safely across multiple layers of NAT or TCP proxies. At the beginning of each connection, the connection initiator places an easily parsable header.

Note:

- This feature supports proxy-header under health checks for the TCP, HTTP and HTTPS method types only.
- This feature is applicable only to the health checks that establish connection on L4 protocols.

Forward Proxy Event Logging Enhancement

The forward proxy event logging provides additional log data in the HTTP requests and responses when **`support-http2`** and **`forward policy`** templates are configured. This enhancement includes the following new elements:

- The HTTP request logs contain User Agent, Referrer, HTTP version, and Server Name Indication (SNI) information.
- The HTTP response logs contain the HTTP version information.

CEF Log Format Example

The following CEF log example shows the HTTP request:

```
Nov 21 12:15:44 vThunder  CEF:0|A10|CFW|6.0.0-d|FWD-PROXY
486709001107537921|Receive Forward Proxy HTTP request and
response|2|outcome=SUCCESS cs5=10.10.10.5 cs5Label=client IP cn6=45126
cn6Label=client port cs7=20.20.20.199 cs7Label=server IP cn8=8080
cn8Label=server port dhost=index2.html requestMethod=GET
request=https://index2.html/ cn4=104 cn4Label=bytes act=To Internet
cs1=HTTPS-policy cs1Label=policy name cs2=1 cs2Label=source rule name
cs9=in_ingress_vip cs9Label=virtual-server cn9=443 cn9Label=virtual-
server-port requestClientApplication=curl/7.61.1
requestContext=www.makemytrip.com app=HTTP/1.1 cs6=index2.html
cs6Label=sni
```

The following CEF log example shows the HTTP response:

```
Nov 21 12:15:44 vThunder  CEF:0|A10|CFW|6.0.0-d|FWD-PROXY
486709001107537921|Receive Forward Proxy HTTP request and
response|2|outcome=SUCCESS cs5=10.10.10.5 cs5Label=client IP cn6=45126
cn6Label=client port cs7=20.20.20.199 cs7Label=server IP cn8=8080
cn8Label=server port sourceTranslatedAddress=10.10.10.5
sourceTranslatedPort=45126 cn1=200 cn1Label=response code cn4=104
cn4Label=bytes act=From Internet cs1=HTTPS-policy cs1Label=policy name
cs2=1 cs2Label=source rule name cs9=in_ingress_vip cs9Label=virtual-
server cn9=443 cn9Label=virtual-server-port app=HTTP/1.1
```

Syslog Format Example

The following Syslog example shows the HTTP request:

```
Nov  9 11:27:39 vThunder a10lb: [ACOS]<6> partition-id<2> <ssli_in>
result=SUCCESS, client-ip=10.10.10.5, client-port=44822, server-
ip=20.20.20.199, server-port=8080, host=index2.html, request-method=GET,
request=https://index2.html/, bytes=104, action=To Internet,
policy=HTTPS-policy, source-rule=1, virtual-server=in_ingress_vip,
virtual-server-port=443, user-agent=curl/7.61.1,
referrer=www.makemytrip.com, http-version=HTTP/1.1, sni=index2.html
```

The following Syslog example shows the HTTP response:

```
Nov  9 11:27:39 vThunder a10lb: [ACOS]<6> partition-id<2> <ssli_in>
result=SUCCESS, client-ip=10.10.10.5, client-port=44822, server-
ip=20.20.20.199, server-port=8080, snat-ip=10.10.10.5, snat-port=44822,
response-code=200, bytes=104, action=From Internet, policy=HTTPS-policy,
source-rule=1, virtual-server=in_ingress_vip, virtual-server-port=443,
http-version=HTTP/1.1
```

Silent Termination of SSLi Sessions

When SSLi terminates idle sessions, it sends out RST and FIN packets in both directions, i.e., to the client and the server. This ensures that all sessions between clients, servers, and ACOS are always gracefully terminated. However, this behavior can be problematic in pure Layer-2 SSLi deployments with redundant paths, especially if upstream and downstream networking devices, such as firewalls, govern the active-standby paths.

In such deployments, the upstream firewall selects an active path, and sessions are established on the active SSLi appliance. When a failover occurs to the standby path, gratuitous ARPs are sent out, and sessions start re-establishing on the standby SSLi appliance. However, in due time, the previously active SSLi appliance sends RSTs and FINs to terminate stale sessions, but this disrupts the firewall's MAC address tables, resulting in network loops.

To address this behavior, ACOS now supports silently terminating stale SSLi sessions so that the passive SSLi appliance does not send out any RSTs or FINs.

This feature supports HTTP/1.1 and HTTP/2 connections.

CLI Configuration

A new option **ssli-silent-termination-enable** is introduced under SLB common configuration mode.

```
ACOS(config)#slb common
ACOS(config-common)#ssli-silent-termination-enable
```

GUI Configuration

A new option 'Enable SSLi Silent Termination' is introduced under **ADC > SLB > Global**.

Limitation

Enabling this feature may cause sessions to stall on either the client or the server side.

Layer 4 Proxy Protocol

ADC solution already supports the layer 7 proxy protocol feature that helps you identify the client's IP address when the load balancer uses TCP for back-end connections. With this release, ADC supports layer 4 proxy protocol.

This protocol supports two header formats:

- Version 1 - a human-readable (ASCII string) format
- Version 2 - a binary format

Limitations

- The proxy-header option will take effect only when the TCP template is bound on the TCP virtual port.
- Fast path and UDP are not supported.
- Following functionalities or configurations are not supported:
  - aflex with TCP payload replace
  - Fast-fix with client IP insert
  - FTP virtual port

CLI Configuration

To enable the proxy protocol option, use the **`proxy-header insert`**.

```
ACOS(config)# slb template tcp TP
ACOS(config-l4 tcp)# proxy-header insert {v1 | v2}
```

GUI Configuration

To enable the proxy protocol option, go to **ADC > Templates > L4 Protocols > TCP**.

SSL Data Plane Health Monitoring

ACOS supports SSL-based health monitoring on the data plane. This is implemented by binding the server SSL to the health monitor. The server SSL can consist of an SSL cipher and other SSL settings for successful SSL negotiation.

The health monitor could utilize SSL acceleration hardware and allow ACOS data plane processes to manage HTTPS connections directly. This improves the scalability and performance of health monitoring systems.

The following configurations are supported for this feature:

- Server SSL template configuration can include **`version`**, **`session-ticket-enable`**, and **`cipher`** settings.
- Health monitor method HTTPS configuration can include **`expect-cert-name`**, **`sni host`**, **`http-version2`**, **`cert`** and **`key`**, and **`http-version3`** settings and can be bound to a real port or service group.

Dual-Blade Chassis Enhancements

For the Dual-Blade chassis, the Linux traffic is currently redirected only to the Master server for processing. To enhance the Blade capabilities and balance the load between the two servers, the following features are implemented:

- Split the 64k ports equally between the Master and the Blade. This helps in identifying the traffic meant for the Blade.
- Provide flexibility to choose a specific port range and allocate the desired number of ports to the Linux Kernel, Health Monitor, ALG types, and Smart NATs.

CLI Configuration

The following commands are introduced at the global level:

- To enable port splitting for the chassis, use the **`system chassis-port-split`** command.

```
ACOS(config)# system chassis-port-split enable
```

NOTE: This command is supported only for the Thunder 7650 chassis platform with **chassis-application-type** as ADC.

- To allocate the desired number of ports for certain applications, use the **system port-count** command.

  This command can be configured with **system chassis-port-split** to split the allocated ports equally between the Master and the Blade.

```
ACOS(config)# system port-count
ACOS(config-port-count)# kernel 18000
ACOS(config-port-count)# hm 1024
ACOS(config-port-count)# alg 6000
```

NOTE: This command is supported for TCP and UDP traffic only.

GUI Configuration

To configure these options, navigate to **System> Settings > System Port**.

ADC GUI Support Thunder 7650 and 7655

ACOS provides GUI support for ADC in the Thunder 7650 and 7655 devices. In addition, a new 'Chassis Application Type' option is introduced for configuring the 'ADC' or 'CGNv6' as the application type. Using GUI, you can manage Virtual Servers, Virtual Services, Service Groups, Applications, Health Monitoring, and many more.

The following are not supported on Thunder 7650 and 7655:

- 'SSL Cert Pinning' under **ADC > SSL Management**
- 'SSLi Certs' and 'Cert Revocation' under **ADC > Statistics > L7 > SSL**.
- 'SSL Forward Proxy' and 'SSLi Errors' counters under **ADC > Statistics > L7 > SSL > SSL Stats**

For more information, see GUI *Online Help*.

Known Limitation

- The GSLB, AAM, and Log main menus are unavailable on the Chassis GUI.

- The 'VRRP-A Status' icon on the Home page (top right corner) is hidden by default when more than one VRID is present. Since the VRIDs are always in pairs in the chassis, the 'VRRP-A Status' icon is unavailable on the Chassis GUI.

Application Access Management

ACOS 6.0.0 introduces the following new features and enhancements for Application Access Management (AAM):

NOTE: For AAM specific configuration steps, refer *Application Access Management Guide*.

The following topics are covered:

SAML Authentication for Forward Proxy Client

Prior to ACOS 6.0.0, the Security Assertion Markup Language (SAML) authentication only supported the reverse proxy functions. ACOS serves as a service provider in the SAML flow, redirecting the client to the Identity Provider (IdP) server. In the forward proxy scenario, the client's traffic passes through the ACOS device where the user is unable to authenticate though it is redirected to IdP. This is because the IdP is on the cloud and client traffic cannot pass through ACOS to enter IdP before authentication.

In the forward proxy environment, ACOS supports the SAML authentication for the client to connect to a third-party Identity Provider (IdP) server (Microsoft Azure Active Directory") through ACOS to authenticate and to protect users' data and resources as part of Zero Trust Architecture. You must configure an ac class-list that includes the domains of IdP and bind the class-list to the `aaa-policy` rule to allow ACOS to forward the SAML authentication traffic to IdP. The new `domain-whitelist` command is added to bind class-list in `aaa rule`.

CLI Configuration

Configure the whitelist domain class-list and bind it to the AAM authentication template.

1. To configure the class-list, enter the following commands:

```
ACOS(config)# class-list whitelist1 ac
ACOS(config-class list)# contains domain1
ACOS(config-class list)# contains domain2
```

2. To bind the class list to `aaa rule` under `aaa-policy`, enter the following commands:

```
ACOS(config)# aam aaa policy1
ACOS(config -aaa policy:policy1)# aaa-rule 1
ACOS(config-aaa policy:policy1-aaa rule:1)# action allow
ACOS(config-aaa policy:policy1-aaa rule:1)# domain-whitelist
whitelist1
```

For example, configure the class-list with the Microsoft listed domains and then bind it to the domain-whitelist under aaa policy. The CLI configuration is:

```
ACOS(config)# class-list c1 ac
ACOS(config-class list)# contains login.windows.net
ACOS(config-class list)# contains secure.aadcdn.microsoftonline-p.com
ACOS(config-class list)# contains microsoftonline.com
ACOS(config-class list)# contains microsoftonline-p.com
ACOS(config-class list)# contains msauth.net
ACOS(config-class list)# contains msauthimages.net
ACOS(config-class list)# contains msecnd.net
ACOS(config-class list)# contains msftauth.net
ACOS(config-class list)# contains msftauthimages.net
ACOS(config-class list)# contains phonefactor.net
ACOS(config-class list)# contains enterpriseregistration.windows.net
ACOS(config-class list)# contains management.azure.com
ACOS(config-class list)# contains policykeyservice.dc.ad.msft.net
ACOS(config-class list)# contains ctldl.windowsupdate.com
ACOS(config)# aam aaa-policy policy1
ACOS(config-aaa policy:policy1)# aaa-rule 1
ACOS(config-aaa policy:policy1-aaa rule:1)# action allow
ACOS(config-aaa policy:policy1-aaa rule:1)# domain-whitelist c1
```

Show Command

To view AAM authentication statistics, use the following command:

```
show aam authentication statistics
```

The following new counters are added in the show aam authentication statistics command under the **`Engine statistics`** category.

- `Domain whitelist matched`
- `Domain whitelist unmatched`

If the host of request matches the whitelist, the domain whitelist matched counter will be increased by one. Else, domain whitelist unmatched will be increased by one.

For more information, see the Command Line Interface Reference Guide.

Limitations

- The SAML forward proxy works only on the new proxy and the class-list type must be ac. You must configure ACOS as the proxy server.
- ACOS will be forced to IP based mode under SAML forward proxy.

aFleX

ACOS 6.0.0 introduces the following new features and enhancements for aFleX.

NOTE: For more information, refer *aFleX Scripting Language Reference*.

The following topics are covered:

Enhanced aFleX IP Commands

With this release, two new aFleX IP commands are introduced in ACOS that provide BrightCloud's local database lookup capabilities of finding the reputation and category of an IP address. The information retrieved by these commands is the IP intelligence information that can be used to filter malicious traffic.

The new IP commands are as follows:

- IP::reputation - Get IP reputation value from the local database.
- IP::category - Get IP category from the local database.

Limitations

- The local database contains 'High Risk (1-20)' records but does not contain IPv6 records.
- The ACOS IP category list is not consistent with the IP category list in BrightCloud database.

New SSL Module Support for Existing Commands

From this release, the following aFleX commands are enhanced to support the new SSL (QAT, new N5, and Software TLS1.3) module:

- HTTP::collect
- HTTP::release
- Pool
- Node
- SSL::payload
- SSL::respond
- TCP::close
- SSLI::bypass
- SSLI::cache_cert
- SSLI::drop
- SSLI::inspect

Limitation

The SSLI aFleX commands are valid for the SERVERSSL_SERVERCERT event only.

aXAPI

ACOS 6.0.0 introduces the following new features and enhancements for aXAPI:

NOTE: For aXAPI specific configuration steps, refer aXAPIv3 Reference Document. Similarly, for ADC specific CLI commands, refer *Command Line Interface Reference.*

The following topic is covered:

ACT Software Download Migrated to GLM

With this release, ACOS supports the AppCentric Template (ACT) installation and upgrade through Global License Manager (GLM).

Limitations

- The install, uninstall, upgrade, and downgrade operations of multiple ACT apps in different browser tabs are not supported.
- Simultaneous install, uninstall, upgrade, and downgrade operations of different ACT apps in multiple tabs are not supported.
- This feature does not have backward compatibility. The uninstall, upgrade, and downgrade operations may not work for any new ACT APP running on the version before ACOS 6.0.0.

Carrier Grade NAT

ACOS 6.0.0 introduces the following new feature and enhancement for Carrier Grade NAT (CGN or CGNAT):

The following topic is covered:

NetFlow Logging Support over Dedicated Partition

In the prior releases, the NetFlow logging could be configured only for the sessions originating within a partition (shared or ADP) and could be sent only through the

interfaces belonging to the partition. In ACOS 6.0.0, the NetFlow logging capabilities have been enhanced to send NetFlow logs over a dedicated partition. You can also allow other partitions to send the logs through this dedicated partition. This feature helps to meet the requirements of lawful interception that runs on a separate network and uses an overlapping IP range with the subscriber for Netflow collectors.

To choose the partition for NetFlow logging, use the `netflow use-partition` command.

You cannot configure `netflow use-partition` on the current partition if NetFlow Monitor is already configured (and vice versa).

Firewall

ACOS 6.0.9 introduces the following new features and enhancements for Gi or SGi Firewall:

NOTE: For more information, refer *Firewall Configuration Guide*.

The following topics are covered:

Action to Set DSCP Value

The firewall rule-set action-group is enhanced by introducing the **`permit set-dscp`** action. This is a session-bases action that sets the Differentiated Services Code Point (DSCP) value in the IP (IPv4 and IPv6) header for all the session packets. The DSCP bits contain packet classification information that signal other devices (along the path), how to treat the traffic.

CLI Configuration

The following example configures the action-group with **`permit set-dscp`** action:

```
ACOS(config)# rule-set test
```

```
ACOS(config-rule set:test)# rule 1
ACOS(config-rule set:test-rule:1)# action-group
ACOS(config-rule set:test-rule:1-action-group)# permit set-dscp cs1
```

GUI Configuration

To configure the action to set the DSCP value, navigate to:

Security > **Firewall** > **Rulesets** > **Rule** > **Action Group** > **Set DSCP**

Limitations

- If a rule is configured with application protocol, this action is applied only after application classification.
- If the DSCP change is applied by CGN, SLB, SSLi or IPsec modules, this action will not take effect.
- If the DSCP configuration changes during the session life, the new DSCP value will be set for the new session only.

Multiple VRID

Earlier, only one Virtual Router Identifier (VRID) could be configured with the Firewall, which would create a session that could sync with only one VRRP group. To implement redundancy and load sharing, the firewall is now enhanced to support multiple VRIDs, so that the firewall sessions can be synced with different VRRP groups (based on the VRID). The Active VRID can have multiple standby VRIDs. However, the session is synchronized only with the primary standby VRID that takes over when the active VRID fails.

Known Limitations

- Applies only to firewall traffic.
- Applicable only for A10 platforms that support the firewall (including application firewall) and VRRP-A.

Rate Limit Policy for IPsec Traffic

The firewall rule-set action group supports the **`permit limit-policy`** (rate-limit policy) and **`permit ipsec`** actions, which were mutually exclusive. The action-group is

now enhanced so that the rate-limit policy can be applied to the traffic that matches the rule with `permit ipsec` action configured.

The rate-limits are applied to the outbound traffic before being encrypted by IPsec, and to the inbound IPsec traffic after it is decrypted.

NOTE: The rate-limit policy is not applicable for the encrypted IPsec packets.

GUI Configuration

To configure a limit policy template, navigate to:

Security > **Firewall** > **Configure** > **Template Limit Policy** > **+ New Limit Policy**

To bind the limit policy template to the rule, navigate to:

Security > **Firewall** > **Rulesets** > **Rule** > **Action Group** > **Permit Limit Policy**

Global Server Load Balancing

ACOS 6.0.0 introduces the following new feature and enhancement for Global Server Load Balancing (GSLB).

NOTE: For more information, refer *Global Server Load Balancing Guide*.

GSLB Policy Enhancement for DNS Zone

A10 Global Server Load Balancing (GSLB) balances the load on servers and ADCs across all global data centers by routing client requests to the closest or highest-performance data center. In the event of failure, client requests are forwarded to the available data centers. When GSLB is deployed in server mode, the ACOS device responds directly to queries for the specific service IP addresses in the GSLB zone while forwarding other queries to the authoritative DNS server.

A10 GSLB now provides zone lookup functionality to specify the DNS server as the zone owner. If the query matches the zone but the zone does not include the domain name requested, GSLB responds with NXDOMAIN to indicate that it is the authoritative server for this zone and that no further resolution is required.

CLI Configuration

To enable this feature, a new command **zone-owner-mode** is introduced in the GSLB policy.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns server any authoritative zone-owner-mode
```

GUI Configuration

To enable this feature, go to **GSLB > Policies**, expand **DNS Options** and check **Server Mode** to see the **Zone Owner Mode** check box.

FQDN Support for Multiple Load Balancing Devices

In this release, the global load balancing site configuration is extended to support the Fully Qualified Domain Name (FQDN) of the devices that perform load balancing for the sites. This feature supports IPv4 address, IPv6 address, or mixed resolutions.

When you have multiple devices (multi-cloud deployment) distributed across different data centers at varied locations, this capability directs the traffic towards each instance. It also provides the ability to perform health checks of the targets behind an FQDN.

CLI Configuration

To enable this feature, use the following command:

```
ACOS(config)# gslb site NY-site
ACOS(config-gslb site:NY-site)# slb-dev D1 hostname {resolve-to-ipv4 |
resolve-to-ipv6 | resolve-to-ipv4-and-ipv6}
```

To view the FQDN statistics, use the following commands:

- `ACOS(config)#show gslb slb-device`
- `ACOS(config)#show gslb site`

GUI Configuration

Go to **GSLB > Sites > SLB Devices > Create**. On the Create SLB Device page, the following options are added:

- Address Type / Hostname
- IP Address

- IPv6 Address
- Hostname
- Resolve to

Limitation

Each device hostname or FQDN allows only one static vip-server configuration.

GSLB Support for Certificate Authority Authorization Record Type

In this release, ACOS supports Certificate Authority Authorization (CAA) as one of the DNS record types for global load balancer zone, zone services, and policy. This feature determines which certification authorities (CAs) may issue SSL certificates for your domain and subdomains.

When this feature is configured, ACOS transmits a DNS reply with personalized CAA record type and corrects the RDATA when the client requests.

ACOS supports the following structure of a CAA record:

- **Issue Critical Flag**: An unassigned integer with a range from 0 to 255. All records have the default issuer critical value of 0, indicating they are not critical and value 255 is used for critical.
- **Property Tags**:
  - **NAME**: Specifies the custom-defined property tags as per your requirement. It can be lowercase alphanumeric and up to 255 characters in length.
- **RDATA**: A variable-length string of octets that describes the resource. The format of this information varies according to the TYPE and CLASS of the resource record. It is only the domain name or domain name along with other parameters. It can be up to 1000 characters.
- **TTL**: It is time-to-live for the CAA record in second. By default, the TTL of the zone is used.

CLI Configuration

- To enable the CAA option on GSLB Zone, use the following commands:

```
ACOS (config)#gslb zone a10-black.com
ACOS (config-zone:a10-black.com)#dns-caa-record <issuer_critical_flag_
num>
<issuer_property_tag_name>
<issuer_domain_name> {sampling-enable {all | hits} | ttl}}
```

- To enable the CAA option on GSLB Service, use the following commands:

```
ACOS (config)#gslb zone a10-black.com
ACOS (config-zone:a10-black.com)#service 80 test
ACOS (config-zone:a10-test.com-service:test)#dns-caa-record
<issuer_critical_flag_num>
<issuer_property_tag_name>
<issuer_domain_name> {sampling-enable {all | hits} | ttl}}
```

- To enable the CAA option on GSLB Policy or Server Mode, use the following commands:

```
ACOS (config)#gslb policy TEST
ACOS (config-policy:TEST)#dns server {caa}
```

- To view the CAA information or statistics, use the commands:
  - `ACOS (config)# show gslb zone`
  - `ACOS (config)# show gslb fqdn`
  - `ACOS (config)# show gslb service`
  - `ACOS (config)# show gslb service-group`

GUI Configuration

Go to **GSLB > FQDNs > Update > DNS Records > Create**. A new Record Type – **Zone CAA** is added, and the following fields are added in Zone CAA:

- Record Type
- Issuer Critical Flag
- Property Tags
- Domain Name or URL
- Enable baselining
- TTL

Global License Manager

ACOS 6.0.0 introduces the following new feature and enhancement for Global License Manager (GLM):

Migration of ACT software download to GLM

With this release, the ACOS authenticates the ACT software access request using Global License Manager (GLM) thus, ensuring better security.

NOTE: This feature does not have backward compatibility.

IPsec Virtual Private Network

ACOS 6.0.0 introduces the following new features and enhancements for IPsec Virtual Private Network (VPN):

NOTE: *For IPsec specific configuration steps, refer IP Security Configuration Guide.*

The following topics are covered:

IPSec Active - Backup Tunnel

ACOS supports policy-based VPN (site-to-site) and allows you to direct traffic based on firewall rules or policies. Additionally, ACOS supports IPsec session synchronization for stateful failover of active VPN sessions based on the configured priority and the Dead Peer Detection (DPD) method.

With this release, ACOS supports failover functionality when each site-to-site VPN connection has multiple tunnels and gateways deployed. ACOS allows configuring the ipsec-group to identify and group a set of tunnels to provide redundancy at the granularity of the IPsec tunnels. This functionality is supported only for policy-based IPsec tunnels.

You can configure the ipsec groups using the `ipsec-group` command. An ipsec-group consists of a group of tunnels with a priority number for each tunnel. The tunnel with the highest priority value is the active tunnel, and the other tunnel(s) serve as the backup tunnels for that group.

If the active tunnel is down, the traffic switches over to the backup tunnel with the next highest priority. The switchover between an active tunnel and a backup tunnel is done in the following ways:

- Automatic switchover through DPD configuration
- Manual switchover through priority configuration in the ipsec-group
- When the tunnel interface is disabled or re-enabled

The minimum DPD interval that can be configured is reduced from 10 seconds to 1 second.

CLI Configuration

The following example creates an IPsec tunnel named a1, adds to the group named group1, and sets the priority to 9.

```
ACOS(config)#vpn ipsec a1
ACOS(config-ipsec:a1)#lifetime 300
ACOS(config-ipsec:a1)#bind tunnel 1 12.12.12.1
ACOS(config-ipsec:a1)#ike-gateway a1
ACOS(config-ipsec:a1)#exit
ACOS(config)#vpn ipsec-group group1
ACOS(config-ipsec-group:group1)# ipsec a1 priority 9
```

Show Commands

- The following is the show command to view the group and group member details:

```
show vpn ipsec-group <group-name>
```

- The following is the show command to view all the groups in that partition:

```
show vpn ipsec-group
```

Clear Commands

- The following is the clear command to clear all the SAs associated with the group:

```
clear vpn ipsec-group <group-name>
```

- The following is the clear command to clear all the SAs of all the groups in all the partitions:

```
clear vpn ipsec-group all-partitions
```

Limitations

- IPSec Active or Backup Tunnel supports only the site-to-site configuration.
- An IPSec tunnel can be associated with several data sessions according to the configuration. With groups, a group member with the highest priority will be designated to pass the traffic. If this group member is disassociated from the group (using the no command), while the traffic is being passed, the traffic will continue to pass through the existing member on these data sessions. However, when new ones are created, they will select a new group member to pass the traffic.

CGN and IPsec in Same Partition

In this release, ACOS provides the capabilities to implement the following scenarios on one partition:

- The CGNAT and IPsec functionality is often deployed in the same location where the data center is located (server-side), and sometimes deployed at the client-side. This functionality is needed to meet the traffic delivery requirements that combine the CGN for network address translation and IPsec for encrypting and protecting the traffic.
- Based on the deployment scenario, it may be required to decapsulate the traffic first and then apply CGN or apply CGN first and then encapsulate the packets to send over the IPsec tunnel.

Limitations

The following are the limitations:

- Only VPN stateful mode works with CGN and Gi-FW.
- CGN and Gi-FW are not supported after IPsec encapsulation.
- IPsec decapsulation after CGN is not supported.
- The chassis devices such as TH7650 and TH14045 are not supported because the reverse packets are encapsulated by IPsec and cannot be distributed to the same processing unit with the forward packets.

Internet Key Exchange (IKE) Message Fragmentation

When IPsec uses digital certificates for authentication, IKE messages exceed the interface MTU size (1500 bytes) and fragment at the IP level. These fragmented IP packets cannot pass through some intermediate network devices, that prevent IKE from establishing an IPsec tunnel. Also, the jumbo frame MTU cannot be set if the IPsec peers are connected through the public networks.

With this release, ACOS supports the IKE message fragmentation solution (RFC 7383) to split the large IKE messages into a series of smaller messages. This solution allows IKE messages to pass through environments that might block IP fragments. You can use the `fragment-size` command to configure the fragment size between 576 and 1280 bytes.

CLI Configuration

To set the fragment size, use the following command:

```
ACOS(config)# vpn ike-gateway name
ACOS(config-ike-gateway:name)# fragment-size 578
```

Show Command

To view the fragment-specific counters, use the `show vpn ike-sa` show command.

Limitation

IKEv1 peers on Windows 7 and Windows 8 only fragment messages if they expect certificates.

Distributed Sequence Numbers for IPsec Scaleout

In this release, ACOS supports the sequence number distribution for the tunnel in the outbound direction in the Scaleout topology. This feature distributes the sequence number accurately on the nodes and manages the flow of outbound traffic (server-to-client) that reaches any nodes in the Scaleout topology.

The Anti-replay window that protects against replay attacks is enhanced to support the window sizes of 2048, 3072, 4096, and 8192. It is recommended to set a larger window size for high traffic.

GUI Configuration

To configure sequence number, go to **Security > IPsec VPN > VPN Tunnels > Create VPN Tunnel**. The following values are added to the Anti Replay Window Size field.

- 2048, 3072, 4096, and 8192.

Network Configuration

ACOS 6.0.0 introduces the following new features and enhancements for the Network Configuration:

NOTE: For configuration and CLI commands, refer *Network Configuration Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topics are covered:

BGP 4-Byte AS Number Formatting

In this release, the ACOS device provides two new options to format the BGP 4-byte Autonomous System Number (ASN).

In ACOS, an AS number notation is denoted as follows:

- asdot – In this notation, an AS number less than 65536 is denoted as 'asplain', that is as a decimal number, and an AS number equal to or greater than 65536 is denoted as 'asdot+', that is two 16-bit decimal numbers joined by a dot: <high order number>.<low order number>. For example, AS number 65537 is printed as 1.1 while AS number 65530 is printed as 65530. The asplain format is the default.
- asdot-plus – In this notation, an AS number is denoted as two 16-bit decimal numbers joined by a dot: <high order number>.<low order number>. An AS number less than or equal to 65536 is denoted as a low order number and the high order value is set to 0. For example, AS number 65537 is printed as 1.1 while AS number 65530 is printed as 0.65530.

CLI Configuration

The following command sets the formatting of the ASN in the BGP show commands:

```
bgp extended-asn-cap [asdot | asdot-plus]
```

The following show commands are updated to include the AS number in the output:

- `show ip bgp`
- `show ip bgp neighbor`
- `show ip bgp summary`
- `show ip bgp neighbor a.b.c.d received-routes`
- `show ip bgp neighbor a.b.c.d advertised-routes`

GUI Configuration

To configure a BGP Router, go to **Network > BGP**. The following options are added:

- Global – Used to edit a BGP
- Router – Used to create a BGP Router

Layer 2 Health Monitoring

ACOS provides the layer 2 health monitoring infrastructure support for Virtual wire, Layer 2, or Virtual Wire with SSLi (IP-less) deployments where monitoring other network devices is required for failover. In the case of firewall load balance by virtual wire or firewall service in SSLi deployment, this feature can detect if the defined internal path is up or down.

This functionality can also be utilized to connect the path status to the real server interface. When the internal path is blocked due to a firewall failure, ACOS can detect the change in the state and notify the interface real server on the path to reflect the condition. Once the real server's state has been updated, the application can select a working server to process the subsequent request.

CLI Configuration

The following CLI commands are introduced to configure layer 2 health monitoring infrastructure:

- To configure global level BFD feature, use the following command:

```
ACOS(config)# bfd enable
```

- To configure global level layer 2 health monitoring feature, use the following command:

```
ACOS(config)# l2-bfd {ether-type | rx-interval | tx-interval |
multiplier}
```

- To configure the individual health monitor/check object, use the following command:

```
ACOS(config)# system health-check monitor_name {l2-bfd | rx-interval |
tx-interval | multiplier}
```

- To configure the layer 2 health monitor path object, use the following command:

```
ACOS(config)# system path path-object {interface-pair {ethernet |
trunk} | use monitor_name | user-tag user_tag_name}
```

- To associate the layer 2 health check path with the interface real server, use the following command:

```
ACOS(config)# slb server S1 ethernet 3
ACOS(config-real server)# l2-health-check-path test_path
ACOS(config-real server)# port 80 tcp
```

Show Commands

The following CLI commands are introduced and updated to view the layer 2 health monitoring statistics:

- To view the statistics of system path status for layer 2 health monitoring, use the following show command:

```
ACOS(config)# show system path{summary | details}
```

- To view the statistics of bfd neighbors, use the following show command:

```
ACOS(config)# show bfd neighbors details
```

- To view the statistics of server state, synchronize with the system path object, use the following show command:

```
ACOS(config)# show slb server
```

GUI Configuration

- To configure/edit the global-level layer 2 health monitoring settings, go to **Network > BFD > Edit Network L2 BFD** page.
- To configure the individual health monitor/check object and layer 2 BFD settings, go to **System > Settings > Health Check > Create** page.
- To configure the layer 2 health monitor path object, go to **System > Settings > Layer 2 Path > Create** page.

MIB

ACOS 6.0.0 introduces the following new features and enhancements for MIB:

NOTE: For more information about supported MIB object details, refer *MIB Reference Guide*.

The following topics are covered:

SNMP EngineID Enhancement

The existing SNMPv3 EngineID feature is enhanced to display engineID with vcs-local-only status, by default. In the previous releases, all ACOS devices had the same engine ID and traps/alerts were sent from these devices with the same engineID. Due to which, the SNMP client was unable to differentiate them and perform the SNMPv3 security checking. With this enhancement, the SNMPv3 EngineID synchronization is disabled and a unique engineID gets configured for each ACOS device. The SNMP client can now differentiate based on the unique engine ID and perform the SNMPv3 security checking.

The **`show snmp-server engineID`** command is modified to display engine ID with its VCS status.

Limitations

Compatibility issues for existing customer may occur. In such case, change the schema file 'snmp-server.sch' on engineID field by removing ‘vcs-local-only’ status.

SNMP MIB Routing

With this release, the MIB objects for SNMP monitoring are enhanced for:

- OSPFv2 routing protocol to support RFC 1850
- BGP routing protocol to support RFC 4273
- IS-IS routing protocol to support RFC 4444

  Limitations:

  - The **`isisRouterTable`** router ID is disabled on IS-IS. Hence, this table is not supported.
  - The **`isisReachAddr`** table is unavailable on IS-IS. Hence, this table is not supported.

  As part of RFC 4444 support, a new SNMP trap has been added under IS-IS.

  CLI Configuration

  The following CLI command enables the isisLSPErrorDetected trap on IS-IS:

```
ACOS(config)# snmp-server enable traps routing isis
isisLSPErrorDetected
```

Limitation:

The new SNMP trap does not send any notification for the following MIB trap objects:

- **isisErrorOffset**
- **isisErrorTLVType**

SNMPv3 Authentication and Encryption Enhancement

The SNMPv3 authentication and encryption methods are enhanced to support better performance and improved security.

The authentication is performed using an authentication key to send the message. The authentication key is generated using either the MD5 or SHA authentication method and a specified password. The key size for SHA is typically 512, 384, 256, or 224 bits.

The encryption is performed using a privacy key, to encrypt the data of the sent message. The privacy key is generated using either the AES or DES encryption method and a specified password. The AES method uses a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

CLI Configuration

The following example shows the authentication type for the snmp-server command:

```
ACOS(config)# snmp-server SNMPv3 user exampleuser group examplegroup v3
auth sha-512
md5      Use HMAC MD5 algorithm for authentication
sha      Use HMAC SHA algorithm for authentication
sha-512  Use HMAC SHA-512 algorithm for authentication
sha-384  Use HMAC SHA-384 algorithm for authentication
sha-256  Use HMAC SHA-256 algorithm for authentication
sha-224  Use HMAC SHA-224 algorithm for authentication
```

The following example shows the encryption type for the snmp-server command:

```
ACOS(config)# snmp-server SNMPv3 user exampleuser group examplegroup v3
auth sha-512 authpassword priv aes-192 privpassword
des       DES encryption alogrithm
aes       AES encryption alogrithm
aes-192   AES-192 encryption alogrithm
aes-256   AES-256 encryption alogrithm
```

GUI Configuration

To enable this feature, go to **System > Monitoring,** under **SNMP** tab, select **SNMPv3 User**.

Platforms

ACOS 6.0.0 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

AC Trie Memory Pool Enhancement

ACOS has introduced a new memory block allocation mechanism for the Aho-Corasick (AC) class-list at the backend. This facilitates the AC class-list module to manage its memory block. As a result, the 'show memory' CLI command will not display the 'AC Trie Memory' information.

Hide Password Input and Obfuscate when Displayed

When the admin user password is entered with the keyboard-interactive method during CLI configuration, it is echoed to the screen. This functionality is now enhanced to hide the admin user password on the screen.

The existing CLI commands `admin`, `password` and `enable-password` have been extended to configure this functionality. When these commands are executed, a prompt appears on a new command line to input the password that does not echo to the screen. After providing the password and pressing the Enter key, another prompt appears on a new command line to confirm the entered password. When both the passwords are matched, the password is accepted. Only the admin user password and enable password can be entered as an obfuscated text and they cannot be left blank.

CLI Configuration

The following command inputs the admin user password for `admin` command:

```
ACOS(config)# admin adminuser1 password
Password:
Retype password:
Modify Admin User successful!
ACOS(config-admin:adminuser1)#
```

The following command inputs the admin user password for `password` sub-command:

```
ACOS(config)# admin adminuser1
ACOS(config)# password
Password:
Retype password:
ACOS(config-admin:adminuser1)#
```

The following command inputs the enable password for `enable-password` command:

```
ACOS(config)# enable-password
Password:
Retype password:
ACOS(config)#
```

NOTE: The password is obfuscated and therefore it is not displayed on the screen.

Limitations

- The obfuscated admin user password support is applicable only for `admin`, `password` and `enable-password` CLI commands.
- The admin user does not support `no password` command.

Strong Default Password Policy

With this release, the existing ACOS password policy is enhanced to enforce a user to create strong and unique passwords.

Default Password-Policy Complexity

A new password-policy complexity option **Default** is introduced under the **`system password-policy complexity`** command. This policy is enforced when you log in for the first time with a default admin password on a new vThunder device or after resetting the device using the **`system-reset`** command. The ACOS prompts you to change the default admin password based on the following criteria:

- The password should be at least nine characters in length.
- The password should contain at least one number, an uppercase letter (English), a lowercase letter (English), and a special character.
- The password should have at least one letter or number different from the previous password.
- The password should not contain its corresponding username with the same capitalization of letters.
- The password should not contain repeated characters of the same letter or number with the same capitalization of letters.
- The password should not contain the sequential row keyboard input of four letters or numbers with the same capitalization of letters.

After you execute the **`erase`**, **`reboot`**, **`reload`**, and **`upgrade`** commands, the system does not enforce you to change the admin password as per the default password-policy complexity. It is enforced ONLY after you execute the **`system-reset`** command.

CLI Configuration

The following CLI commands are used to set the default password policy complexity:

```
ACOS(config)# system password-policy complexity Default
ACOS(config)# system password-policy complexity Default username-check
enable
ACOS(config)# system password-policy complexity Default repeat-
character-check enable
ACOS(config)# system password-policy complexity Default forbid-
consecutive-character 4
```

To create a password using CLI mode, perform the following steps after you log in for the first-time on a new vThunder device or after resetting the device using the **system-reset** command:

1. Log into the CLI using SSH.
2. On the **login as:** prompt, enter the default admin username.
3. On the **Password:** prompt, enter the default admin password.
   A message is displayed to change the default password.
4. On the **Please enter your new password:** prompt, enter the new password as per the **Default** password-policy complexity criteria.
5. On the **Please re-enter your new password:** prompt, re-enter the new password for verification.

GUI Configuration

To create a password using GUI mode, perform the following steps after you log in for the first-time to a new vThunder device or after resetting the device using the **system-reset** command:

1. Open a supported Web browser.
2. In the URL field, enter the IP address of the vThunder device management interface.
   A login page is displayed.
3. Enter your admin username and the recently configured password.

NOTE: The default admin username and password are “admin”, “a10”.

4. Click **Login**.
   The Change the Default Password page is displayed.
5. Enter the new password as per the **Default** password-policy complexity criteria, re-enter the new password for verification, and click **OK**.

You can change the password-policy complexity later as per your requirement using the **system password-policy complexity** command in CLI mode.

For more information, see *Command Line Interface Reference Guide*.

Password Checks

Starting from ACOS 6.0.0, three new password checks have been introduced in all the password-policy complexity options to improve the password strength. These checks are enabled using the CLI mode. The checks are as follows:

- Allow or prevent a user to create a password that contains the username. The **username-check** is case-sensitive and is disabled by default.

```
system password-policy complexity [Strict | Medium | Default | Simple]
username-check [enable | disable]
```

- Allow or prevent a user to create a password that contains repeated characters of the same letter or number. The **repeat-character-check** is case-sensitive and is disabled by default.

```
system password-policy complexity [Strict | Medium | Default | Simple]
repeat-character-check [enable | disable]
```

- Allow or prevent a user to create a password that contains sequential row keyboard input of letters or numbers. The **forbid-consecutive-character** check allows sequential row keyboard input of special characters and letters or numbers not in the same keyboard row. The unallowed repeated length can be configured within the range of <3-5> characters. If the length value is set to either 3, 4, or 5, the check is enabled and if it is set to 0, the check is disabled. This check is case-sensitive and is disabled by default.

```
system password-policy complexity [Strict | Medium | Default | Simple]
forbid-consecutive-character num
```

CLI Configuration

The following CLI command enables the username check for medium complexity:

```
ACOS(config)# system password-policy complexity Medium username-check
enable
```

When this check is enabled, a password cannot contain the corresponding username with the same capitalization of letters. For example, 'pass!@admin1QW' password is invalid for 'admin' user whereas 'pass!@Admin1QW' is valid.

The following CLI command enables the repeat character check for simple complexity:

```
ACOS(config)# system password-policy complexity Simple repeat-character-
check enable
```

When this check is enabled, a password containing repeated characters of the same letter or number with the same capitalization of letters is prohibited. For example, password containing 'aa', 'AA', '11' is invalid whereas password containing 'aA', 'Aa' is valid.

The following CLI command enables the forbid consecutive character check for strict complexity with five consecutive characters:

```
ACOS(config)# system password-policy complexity Strict forbid-
consecutive-character 5
```

When this check is enabled, a password containing sequential row keyboard input of letters or numbers with the same capitalization of letters is prohibited. For example, a password containing 'asdfg' or 'gfdsa' is invalid whereas a password containing 'asdf', '1234', 'fdsa', 'ASdfg', '!@#$%', 'klzxc', 'iopas', '890qw' is valid.

The following CLI command disables the forbid consecutive character check for strict complexity:

```
ACOS(config)# system password-policy complexity Strict forbid-
consecutive-character 0
```

For more information, see *Management Access and Security Guide*.

Require Default Password to Change

When you log in for the first time to a new device or after resetting the system using the `system-reset` command, ACOS prompts you to change the default admin password.

For more information, see the *System Administration and Configuration Guide*.

Optimized QAT Performance

The performance of the Quick Assist Technology (QAT) accelerator is improved by offloading the SSL handshake hash and extended master secret (EMS) operations to QAT. Furthermore, the maximum concurrent session is increased for memory optimization with the new SSL.

Limitation

Only TLS 1.0/1.1/1.2 handshake hash will be offloaded.

PCAP Next Generation (PCAPNG) Support in axDebug

In the prior releases, the ACOS debugging (axDebug) utility supported capturing packets in the PCAP file format, which is widely understood by third-party diagnostic applications such as Wireshark (formerly Ethereal) or tcpdump.

With this release, ACOS supports capturing packets in the PCAP Next Generation (PCAPNG) file format to enhance debugging capabilities. Wireshark fully supports the PCAPNG file format, whereas libpcap has partial support for the PCAPNG file format.

For more information on PCAPNG, see https://datatracker.ietf.org/doc/html/draft-tuexen-opsawg-pcapng.

Each PCAPNG file has numerous data blocks containing various types of information. In this release, the following block types are supported:

- Section Header Block (SHB) – Includes a list of blocks such as interfaces and packets that are logically correlated.

- Interface Description Block (IDB) – Contains information describing an interface on which the packet data is captured.
- Enhanced Packet Block (EPB) – Stores the packets coming from the network.
- Decryption Secrets Block (DSB) – Stores session secrets (including pre-master secret key of SSL session) that enable decryption of packets within the capture file.

Under axDebug, a new option called **pcapng-config** is added for configuring the PCAPNG file format using CLI and GUI.

For more information, see the *Command Line Reference Guide*.

CLI Configuration

- To enable PCAPNG, use the following commands:

```
ACOS# axdebug
ACOS(axdebug)# pcapng-config
ACOS(axdebug-pcapng)# pcapng-enable
```

- To enable SSL key tracking, use the following commands:

```
ACOS# axdebug
ACOS(axdebug)# pcapng-config
ACOS(axdebug-pcapng)# pcapng-enable
ACOS(axdebug-pcapng)# ssl-key-enable
```

Show Commands

To view the packet capture information, refer to the following show commands:

- **show axdebug file**
- **show axdebug config-file**
- **show axdebug pcapng**
- **show axdebug status**

GUI Configuration

To enable or disable the PCAPNG and SSL Key tracking, go to **System** > **Diagnostics** > **PCAPNG Config**.

For more information, see *Online Help*.

Limitations

- The names of the packet capture files must be unique.
- When using the **ssl-key-enable** under **pcapng-config** command, the Wireshark version 3.6.5 (or prior versions) does not show the server certificate key. As a workaround, you must change the following settings in the capture file:
  - For HTTPv1/HTTPv2:

    Under Analyze Option: Decode As- +TCP port 443 and select HTTP
  - For HTTPv3:

    Under Analyze Option: Decode As - +UDP port 443 and select HTTP

CPU Packet Prioritization

With this release, the Thunder for Bare Metal and ESXi support the CPU packet prioritization feature. The feature uses the NVIDIA Mellanox ConnectX-6 and NVIDIA Mellanox ConnectX-5 cards hardware programmable flow rules to classify and prioritize control packets, such as BFD, BGPv4, BGPv6, OSPFv2, OSPFv3, RIP, RIPng, LACP, STP, VCS, Scaleout, and VRRP packets over the data packets.

To enable the control packet prioritization, run the following command:

```
ACOS(config)# system cpu-packet-prio-support enable
```

vCenter Support for vThunder on ESXi

With this release, you can install vThunder using vCenter ESXi 7.0 U3 or later. If you are using an older version of the ESXi hypervisor, use ACOS 4.1.4-P2 or prior version.

For more information, see the *Installing vThunder on VMware ESXi* guide.

System Configuration and Administration

ACOS 6.0.0 introduces the following new feature and enhancement for System Configuration and Administration:

NOTE: For more information and details, refer *System Configuration and Administration Guide*.

The following topic is covered:

Call Home

Call Home enables ACOS devices to send diagnostic information securely to the A10 Product Research end-point. This diagnostic information includes configuration and environmental data such as the ACOS device, its form factor, deployment location, number of interfaces, L3V partitions, VLANs, and more. It also collects information on the ACOS licenses activated on the device. All the information collected is used to improve the product quality.

Call Home is not enabled by default. You can manually enable Call Home on your ACOS devices. When enabled, the ACOS device pushes the collected diagnostic information to the A10 end-point daily at midnight . You can choose to manually offset the call home time by 0 to 23 minutes after midnight, if needed.

The following conditions must be met for A10 Call Home to work:

- **Internet Connection** — The ACOS device must be able to reach the internet for Call Home to send diagnostic data to the A10 end-point. This feature does not work with proxy server configuration.
- **Port 443** — The Call Home data from your ACOS device is sent over TLS protocol using port 443 by default.

CLI Configuration

- To enable Call Home, verify internet connectivity and configure the call-home profile on the ACOS device:

```
ACOS(config)# call-home profile
ACOS(config-profile)# register
```

The ‘register’ command enables the call-home service. Once enabled, the Call Home data is collected from the ACOS device every 24 hours at midnight. You can choose to manually offset the Call Home time by 0 to 23 minutes.

To offset the export time:

```
ACOS(config-profile)# time <0-23> mins
```

For example, if you configure the offset time as 5 mins, the data will be exported at 12:05 AM.

ACOS Events Log Server Hash Load Distribution Method

When there are multiple external log servers configured in a collector group, each log is forwarded to only one of the log servers. The log messages are default forwarded to the external log servers using the Round-Robin method. In this release, the hashing method is introduced in which the log messages are forwarded to the external log servers based on hashing to provide a consistent hashing framework where the related logs are sent to the same log server.

The server Distribution method uses a server name or IP tuple to distribute the log servers. By default, a log server name is used for distribution but can be configured to use the log server IP address. The ability to configure can be useful in different scenarios like when the log servers go down, they are replaced.

CLI Configurations

- Use the following command to configure the hashing method in the collector group for distributing the logs:

```
ACOS(config-collector-group:c1)#log-distribution hashing
```

- Use the following command to configure the hashing method as the Name of the log server in the collector group for distributing the logs:

```
ACOS(config-collector-group:c1)#server-distribution-hash name
```

- Use the following command to configure the hashing method as an IP tuple of the log server in the collector group for distributing the logs:

```
ACOS(config-collector-group:c1)#server-distribution-hash ip-tuple
```

Show command

The **`show acos-events messages`** show command is introduced to display the existing logs in the ACOS.

Scaleout

ACOS 6.0.0 introduces the following new feature and enhancement for Scaleout:

NOTE: For Scaleout specific configuration steps, refer *Scaleout Configuration Guide*.

The following topic is covered:

Scaleout Clusters Based on aVCS

ACOS uses aVCS for Scaleout internal database synchronization. For Scaleout to function efficiently, the Scaleout-related configurations on all devices in the cluster must be applied and synchronized. If you choose not to use aVCS, you must disable the aVCS configuration synchronization on all devices. The `vcs database-distribution enable` command enables the aVCS database synchronization for the Scaleout cluster. You must configure this command on each node in the cluster.

The basic Scaleout configuration is changed as shown in the following table:

Prior to ACOS 6.0.0 Release	In ACOS 6.0.0 Release

scaleout 1
  local-device
  priority 121
  id 3
  l2-redirect interface ethernet 4
  session-sync-interface
  ethernet 3
  ethernet 4
 	
  cluster-devices
  device-id 1
  ip 3.3.3.101
  device-id 2
  ip 3.3.3.102
  device-id 3
  ip 3.3.3.103
 	
  device-groups
  device-group 2
  device-id 1 to 3
  device-group 5
  device-id 3 to 6
 	
  scaleout apps enable
	scaleout 1
	  local-device
	  priority 121
	  l2-redirect interface ethernet 4
	  session-sync-interface
	  ethernet 3
	  ethernet 4
	  device-groups
	  device-group 2
	  device-id 1 to 3
	  device-group 5
	  device-id 3 to 6
	
	  scaleout apps enable
	vrrp-a common
	  device-id 3
	  set-id 3
	  vcs database-distribution enable
	  vcs unicast-election
	  port 12121
	  members
	  ip-address 3.3.3.101
	  ip-address 3.3.3.102
	  ip-address 3.3.3.103
	  vcs discovery-mode unicast
	  vcs device 3
	  enable

CLI Configurations

- To enable or disable the database cluster distribution, use the following command:

```
vcs database-distribution {enable | disable}
```

- To apply the configuration changes on the aVCS chassis, use the following command:

```
vcs reload {cluster-discovery}
```

- To configure the number of milliseconds the vBlade devices wait to receive a **keepalive** message from the vMaster, use the following command:

```
vcs dead-interval-mseconds milliseconds
```

- To configure the number of milliseconds between **keepalive** messages from the vMaster to vBlades:

```
vcs time-interval-mseconds milliseconds
```

SSL Insight

ACOS 6.0.0 introduces the following new features and enhancements for SSL Insight (SSLi):

NOTE: For SSLi configuration steps, see *SSL Insight Configuration Guide*. Similarly, for SSLi specific CLI commands, see *Command Line Reference Guide*.

The following topics are covered:

Certificate Pinning List Enhancement

The existing certificate pinning candidate list feature in SSLi is extended to support two types of certificate pinning lists:

- Local certificate pinning candidate list - This is the locally generated certificate pinning list maintained and available on the ACOS.
- Central certificate pinning candidate list - This is the centrally generated certificate pinning list available on the GLM server. ACOS uploads all the cert pinning data to A10's Central List Service that builds the central list and pushes it to the GLM server for the device to deploy.

The following capabilities are provided in this feature:

- Use the central or local cert pinning list for SSLi bypass decision making.
- Download or update the central cert pinning list for ACOS using the GLM server.
- Choose to upload all the cert pinning data to the central list service.
- View the statistics of central and local cert pinning list, bypassed count, connection failure, and TTL.
- View the SSLi-bypass log to indicate the certificate pinning bypass scenario in case the SSLi logging is enabled.

CLI Configuration

Local certificate pinning list CLI configurations:

- To configure the TTL of certificate pinning in SLB common, use the **`cert-pinning {ttl}`** command.
- To configure the forward-proxy bypass method in the SLB client-SSL template configuration mode, use **`forward-proxy-bypass local-cert-pin-list`** `{conn-fail-count}` command.
- To view the statistics of the local certificate pinning list, use the **`show slb ssl-cert-pinning-candidate-list {local-list | bypassed | alphabet-order}`** command.
- To clear the statistics of the local certificate pinning list, use the **`clear slb ssl-cert-pinning-candidate-list {local-list | SNI_name | stats-only}`** command.

Central certificate pinning list CLI configurations:

- To enable and upload the local certificate pinning list to the central list service in the SLB common configuration mode, use the **`cert-pinning candidate-list-`**

feedback-opt-in {enable | schedule | use-mgmt-port} command.

- To update the central certificate pinning list to the latest version from the GLM server, use **automatic-update check-now central-cert-pin-list** command.
- To revert to the previous version, use the **automatic-update revert central-cert-pin-list** command.
- To configure the schedule for updating the central certificate pinning list periodically, use the **automatic-update central-cert-pin-list schedule daily 12:30** command.
- To configure the forward-proxy bypass method in the SLB client-SSL template configuration mode, use the **forward-proxy-bypass central-cert-pin-list** command.
- To view the statistics of the central certificate pinning list, use the **show slb ssl-cert-pinning-candidate-list {central-list | bypassed | alphabet-order}** command.
- To clear the statistics of the central certificate pinning list, use the **clear slb ssl-cert-pinning-candidate-list {central-list | SNI_name | stats-only}** command.

GUI Configuration

- To configure the forward proxy bypass settings, go to **ADC > Templates > SSL Templates > Client SSL**.

The existing 'SSL Cert Pinning' GUI page under **ADC > SSL Management** is enhanced and updated with the following new GUI pages:

- To view the statistics of the local cert pinning list, go to **ADC > SSL Management > SSL Cert Pinning > Local**.
- To view the statistics of the central cert pinning list, go to **ADC > SSL Management > SSL Cert Pinning > Central**.
- To configure the certificate pinning settings, go to **ADC > SSL Management > SSL Cert Pinning > Settings**.

The existing 'Application Protocol Update' GUI page settings under **Security > Firewall > Configure** is removed and available under **System > Settings > Automatic Update** along with the following enhancement.

- To schedule and update the central certificate pinning list to the latest version from the GLM server, go to **System > Settings > Automatic Update**.

JA3 fingerprinting for TLS

ACOS supports the TLS fingerprinting with JA3, which is also known as the 'JA3 SSL Client Fingerprint' method. This method is used for fingerprinting a TLS client connection. It is the best approach for client identification and to increase the usage of encryption in the network.

This feature utilizes specific parameters from the ClientHello message and hashes the result using MD5 to produce a 32-character fingerprint.

The following functionalities are provided in this feature:

- Insert the JA3 fingerprint as an HTTP header and forward it to the backend HTTP server.
- Reject the SSL/TLS connections by class-list containing the JA3 fingerprints of the known malicious clients.
- Reject the SSL/TLS connections if the JA3 fingerprints amount of a client address exceeds a certain value.
- Supports all the SSL-modules including N5-old, N5-new, QAT, Software, and Software TLS1.3.
- Works with reverse proxy, HTTPS/SSL-Proxy virtual ports, inbound SSLi, and outbound SSLi.

CLI Configuration

The following CLI commands are introduced in the SLB Client-SSL template:

- To enable the JA3 feature, use the **`ja3-enable`** command.
- To insert the JA3 fingerprint as an HTTP header, use the **`ja3-insert-http-header`** `{HTTP_Header_Name}` command.
- To reject SSL/TLS connections by class-list, use the **`ja3-reject-class-list`** `{class_list_name}` command.
- To reject SSL/TLS connections by JA3 fingerprints amount, use the **`ja3-reject-max-number-per-host`**`{`**`number`** `<1-256>} {`**`ttl`** `<1-86400>}` command.

- To view the statistics of current numbers of JA3 amount, use the **`show slb ssl-ja3`** command.

GUI Configuration

- To enable the feature, the following options are introduced under **ADC > Templates > SSL > Client SSL and Security > SSLi > Templates > Client SS**L.
  - Enable JA3
  - JA3 Insert HTTP Header
  - JA3 Reject Class List
  - JA3 Reject Maximum Number Per Host
  - JA3 TTL
- To view the current JA3 amount statistics, the SSL JA3 page is introduced under **ADC > Statistics > L7 > SSL and Security > SSLi > Reports**.

Explicit Proxy with Dual-Stack Forwarding

ACOS is enhanced to support IPv4 and IPv6 dual stack forwarding in explicit proxy mode, starting with the DNS resolution. This solution allows the explicit proxy VIP to serve as a gateway between IPv4 (or IPv6) clients and dual-stacked servers, giving preference to IPv6.

Prior to this feature, although the dual-stacked operation was already supported in ACOS through DNS dynamic service templates as well as separate SLB policy templates, it lacked dynamic address translation or interconnectivity, which could lead to service outages or delays in some cases. For instance, you could configure IPv4 and IPv6 DNS servers on the same dynamic service template, but an IPv4 explicit proxy VIP serving an IPv4 client could only reach out to remote servers over IPv4. Similarly, an IPv6 explicit proxy VIP serving an IPv6 client could only reach out to remote servers over IPv6.

With this feature, once you configure IPv4 and IPv6 DNS servers under the dynamic service template, it behaves as follows:

- An IPv6 DNS server is given preference over an IPv4 server to send DNS requests.
- AAAA (IPv6) and A (IPv4) record requests are sent to the DNS server as two separate requests unless a cached record exists.

- AAAA record replies are preferred over A records.
- Based on the DNS response, the appropriate source NAT pool i.e., either IPv6 NAT-pool or IPv4 NAT-pool is used.

This enables an explicit proxy virtual port to forward HTTP or HTTPS requests via IPv4 or IPv6 networks. Additionally, when this feature is configured, the SSLi certificate fetching module also allows connections with IPv4 addresses on the client side and IPv6 addresses on the server side and vice versa.

NOTE: This feature is not applicable to Transparent Proxy and Proxy chaining.

CLI Configuration

To enable this feature, you need to configure the **dual-stack-action** command under **forward-policy** in the SLB template policy and then bind the action to any destination rule of the forward policy.

The following example demonstrates the **dual-stack-action** command usage:

```
ACOS(config)# slb template policyDUAL_Stack_6n4
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# dual-stack-action FWD_6n4
ACOS(config-policy-forward-policy-dual-st...)# ipv4 To_Internet_v4 snat
EP_POOL_v4
ACOS(config-policy-forward-policy-dual-st...)# ipv6 To_Internet_v6 snat
EP_POOL_v6
ACOS(config-policy-forward-policy-dual-st...)# fallback To_Internet_v6
snat fall_back_v6
ACOS(config-policy-forward-policy-dual-st...)# log
ACOS(config-policy-forward-policy-dual-st...)# exit

ACOS(config-policy-forward-policy)# source ANY
ACOS(config-policy-forward-policy-source)# match-any
ACOS(config-policy-forward-policy-source)# destination any dual-stack-
action FWD_6n4
```

Support Dynamic SNI Transmission for Inbound SSLi

SSLi is deployed in ACOS as a dual proxy, where client-side (decryption) and server-side (re-encryption) TLS negotiations are handled independently. Therefore, ACOS preserves the SNI (Server Name Indication) information from the client's TLS request while decrypting and forwards it to the server side while re-encrypting. This allows SSLi to inspect TLS sessions on multi-hosted servers.

For outbound (or forward-proxy) SSLi over HTTPS, ACOS forwards the SNI information when forward-proxy-enable is configured under the client-SSL and server-SSL templates. For non-HTTP-based TLS sessions, an additional command, ssli-sni-hash-enable under slb common, is also configured. The ssli-sni-hash-enable command allows ACOS to maintain an internal hashing mechanism for SNI forwarding as long as SSLi is deployed in a single appliance. For a dual-appliance SSLi setup, the SNI is conveyed through a special header in the decrypted payload.

For inbound (or reverse-proxy) SSLi, ACOS can leverage the HTTP HOST header from the decrypted HTTPS request in deriving the SNI for the re-encryption process. This does not require any additional CLI commands. However, it fails to derive the SNI if the decrypted HTTPS request does not contain any HOST header or is dealing with non-HTTP-based applications.

This release overcomes all the above-mentioned limitations with SNI forwarding by extending the SNI hashing mechanism to inbound SSLi and dual-appliance SSLi deployments.

This functionality applies to:

- Non-HTTP-based applications in outbound and inbound SSLi for dynamic port inspection.
- HTTP-based applications without a "HOST" header for the inbound SSLi.
- All SSLi Deployments on Thunder SSLi or Thunder CFW device platforms.
- SSL proxy and generic proxy configurations.
- All SSL modules except the new Nitrox V (N5), which only support inbound SSLi.

CLI Configuration

The new **`ssli-inbound-enable`** option is introduced in the client SSL template to enable the basic functions of inbound SSLi with SNI forwarding.

```
ACOS(config)# slb template client-ssl inbound_ssli
ACOS(config-client ssl)# ssli-inbound-enable
```

The following options are introduced to enhance SNI forwarding for dual-appliance deployments over a separate TCP connection through the device Management interface.

- To configure the client-side management IP address and port number on the server-side, use the following command:

```
ACOS(config)# slb common
ACOS(config-common)# ssli-sni-hash-enable {clientside-ip ipv4-address
| clientside-ipv6 ipv6-address port port-number}
```

- To configure the server-side management IP address and port number on the client-side, use the following command:

```
ACOS(config)# slb common
ACOS(config-common)# ssli-sni-hash-enable {serverside-ip ipv4-address
| serverside-ipv6 ipv6-address port port-number}
```

StartTLS SSLi Support with New SSL

ACOS supports StartTLS SSLi with virtual port type 'SSLi', which works only with the old SSL module (TLS1.2). This feature is extended to support the new SSL module such as software-tls1.3 and Quick Assist Technology (QAT).

Limitation

StartTLS SSLi is not supported with the new Nitrox V (N5) module.

SSLi Bypass and Intercept by IP Addresses

ACOS supports SSLi bypass and intercept decision-making based on SNI using the Aho-Corasick (AC) class list rules. To provide an optimal and scalable solution, this feature is extended to support SSLi bypass or intercept decision-making based on the specific client IP and/or server IP (IPv4 and IPv6) class lists.

CLI Configuration

The following CLI commands are introduced in the Client-SSL template.

- To configure the bypass rule if the client IP matches class-list, use **forward-proxy-bypass client-ip-list** {**ipv4** class-list-name | **ipv6** class-list-name}.
- To configure the intercept rule if the client IP matches class-list, use **forward-proxy-bypass exception-client-ip-list** {**ipv4** class-list-name | **ipv6** class-list-name}.
- To configure the bypass rule if the server IP matches class-list, use **forward-proxy-bypass server-ip-list** {**ipv4** class-list-name | **ipv6** class-list-name}.
- To configure the intercept rule if the server IP matches class-list, use **forward-proxy-bypass exception-server-ip-list** {**ipv4** class-list-name | **ipv6** class-list-name}.
- To view the SSLi bypass/intercept statistics, use **show ssl-forward-proxy-stats**.

GUI Configuration

To enable the feature, the following options are introduced under **ADC > Templates > SSL > Client SSL > Forward Proxy Bypass.**

- Client IPv4 Class List
- Client IPv6 Class List
- Exception Client IPv4 Class List
- Exception Client IPv6 Class List
- Server IPv4 Class List
- Server IPv6 Class List
- Exception Server IPv4 Class List
- Exception Server IPv6 Class List

SSL CPU Offload

With the growing SSL needs, encrypting and decrypting of network traffic have become highly CPU-intensive tasks. Therefore, SSLi introduces CPU offload infrastructure and SSL software offload engine to support offloading asynchronous SSL crypto operations.

This solution improves performance, handles many Connections per Second (CPS), reduces CPU load, and frees up more resources for other jobs.

This feature has the following implementation:

CPU Offload Infrastructure

- Supports configuration on the system level.
- Supports offload CPUs allocation.
- Supports job submission to handle offloading CPUs and displays their statistics.

SSL Software Offload Engine:

- Supports configuration on the SSL module level
- Supports SSL operations submission to offload infrastructure
- Supports the SSL connections suspension/resumption based on offload results.

CLI Configuration

For CPU offload infrastructure, the following commands are introduced and updated:

- To enable the CPU offload infrastructure, use the **`offload-cpus`** command.
- To view the CPU offload infrastructure statistics, use the **`show system job-offload [statistics]`** command.
- To view the CPU usage statistics, use the **`show cpu`** command.
- To view the number of offload CPUs, use the **`show run`** command.

For SSL offload engine, the following commands have been introduced and updated:

- To enable the SSL software offload infrastructure, use the **`software-tls13-offload`** command.
- To view the configured SSL offload engine, use the **`show slb ssl stats`** command.

GUI Configuration

To configure the CPU offload infrastructure and view the statistics, go to **System > Settings > Offload CPUs**.

Limitations

- The CPU Offload infrastructure supports 8192 jobs per data CPU
- The SSL offload engine supports both client and server SSL and does not support SSLi.

Next Generation Web Application Firewall

ACOS 6.0.0 introduces the following new features and enhancements for the Next Generation Web Application Firewall (NGWAF):

The following topic is covered:

Introducing Next Generation Web Application Firewall

Until now, A10 Networks' Web Application Firewall (WAF) protected the web applications against several Layer 7 attacks. To enhance the WAF functionality, A10 networks is now empowered with technology from Fastly/Signal Science (a two-time WAF Gartner visionaries' vendor) to bring the A10 Next Generation Web Application Firewall (A10 NGWAF) into ACOS.

The A10 NGWAF is an application security monitoring system that monitors suspicious and anomalous web traffic and protects against attacks directed at applications and origin servers. It provides superior protection for applications and APIs by delivering several advantages over legacy WAF.

For more information on the NGWAF architecture and configurations refer to the *Next Generation WAF Configuration Guide*.

NOTE: ACOS 6.0.0 release no longer support the legacy ACOS WAF. So, while upgrading to 6.0.0, all the WAF configurations will be unsupported. You will have to configure the NGWAF instead.

Features Supported in ACOS

- Supports the HTTP and HTTPS virtual ports
- Supports the HTTP and HTTP2 proxy
- Supports the AAM module for authentication. However, the requests are sent to NGWAF only after the authentication process completes.
- Delivers data to the Fastly Cloud Dashboard for monitoring the attack request records and modifying the NGWAF policies.

Limitations

Following are the NGWAF limitations in ACOS:

- A maximum of 8 partitions can be enabled
- A maximum of 63 virtual ports on the same partition can be enabled.
- One partition can have only one NGWAF agent. Therefore, all the virtual ports on a partition share the same statistics on the Fastly Dashboard.

NOTE: For the Fasty NGWAF limitations, refer to https://docs.fastly.com/products/signal-sciences-next-gen-waf#limitations.

CLI Configuration

The NGWAF agent needs to be imported and configured on each partition. The following commands are introduced:

- To import the latest NGWAF agent:

```
ACOS(config)# import ng-waf-module
https://dl.signalsciences.net/sigsci-agent/sigsci-agent_latest.tar.gz
```

- To register the NGWAF agent:

```
ACOS(config)# license-manager ng-waf-module access-key-id xxxxxxxx
secret-access-key xxxxxxxx
```

- To enable NGWAF on the virtual port:

```
ACOS(config)# slb virtual-server vip 192.168.15.10
ACOS(config-slb vserver))#  port 80 http
ACOS(config-slb vserver-vport)#  service group sg
ACOS(config-slb vserver-vport)#  ng-waf
```

- To check the NGWAF status:

```
ACOS(config)# show ng-waf status
```

- To view the NG-WAF statistics for a specified virtual port:

```
ACOS(config)# show ng-waf vip 80
```

GUI Configuration

- To import the latest NGWAF agent, navigate to **System > Settings > File Management > Import > NG WAF Module**.
- To register the NGWAF agent, navigate to **System > Admin > Licensing NG WAF Module**.
- To enable the NGWAF on the virtual port, navigate to **ADC > SLB > Virtual Services > Create (HTTP or HTTPS protocol) > Advanced Fields > Next-Gen WAF**.
- To specify a custom response code, navigate to **ADC > SLB > Global > NG WAF Custom Response Code**.
- To enable the NGWAF cache function, navigate to **ADC > SLB > Global > Enable NG WAF Pre-processing**.

Enhanced Cache Function

The NGWAF cache function reduces the processing time by storing checked and forwarded requests in the cache. To provide better cache control, the NGWAF cache function has been enhanced by introducing the following features:

- Configuring expiration time for the cache entries.
- Displaying the total number of cached entries.
- Clearing specific cache.
- Freeing the cache entries automatically in the following scenarios:

- The partition is disabled or deleted.
- The virtual port is deleted.
- NGWAF is disabled.

CLI Configuration

- To set the cache expiration time (1 to 480 minutes), configure the **pre-process-enable** command as shown:

```
ACOS (config)# slb common
ACOS (config-common)# ng-waf pre-process-enable 5
```

  In the above example, the cache expiration time is set to 5 minutes. The default value is 1 minute.

- To view the number of cache entries, use the **show ng-waf status** command.
- To clear all the NGWAF cache entries, use the **clear ng-waf cache** command.
  - For cache entries in the current partition:

```
ACOS(config)# clear ng-waf cache all
```

  - For cache entries of a specific virtual port:

```
ACOS(config)# clear ng-waf cache vip 80
```

Enhanced Monitor Mode

The monitor mode has been introduced in NGWAF to analyse and evaluate network traffic. When this mode is enabled, all the requests are monitored and allowed to pass; they are not blocked. However, the malicious requests, which would have been blocked otherwise, are highlighted in the syslogs and debug logs using the **marked** keyword.

NOTE: The monitor mode does not offer active protection.

CLI Configuration

- To enable the NGWAF monitor mode, configure the **monitor-mode-enable** command:

```
ACOS (config)# slb common
ACOS (config-common)# ng-waf monitor-mode-enable
```

- To view the number of **marked** requests, use the **show ng-waf** command.

Customizing Response Code

When a request is blocked by NGWAF, the Thunder device returns a default response code 410. NGWAF provides you with the flexibility to modify the response code based on your requirement. You need to configure the **attack-resp-code** command to specify an HTTP status code (400 to 599) to be returned when a request is blocked.

Additionally, you can also set a custom response code on the Fastly Dashboard. However, this setting overrides the configuration on the Thunder device i.e., if you set a response code on the Fastly Dashboard, the response code configured on the Thunder device is ignored.

If no response code is set on the Fastly Dashboard or the Thunder device, the status code 410 is returned by default.

CLI Configuration

- To configure a custom response code on the Thunder device:

```
ACOS (config)# slb common
ACOS (config-common)# ng-waf attack-resp-code 456
```

- To configure a custom response code on the Fastly Dashboard, see Fastly Custom Response Code.

Customizing Response Message

When a request is blocked by NGWAF, the Thunder device displays a default message. NGWAF provides you with the flexibility to modify this message. You can display a custom message and add some relevant information such as the attack type, the time, the session ID, and the request URI.

To enable this feature, you need to configure the **attack-resp-message** command. This command allows you to set a block message directly or an HTML webpage that

contains the message to be displayed. The reserved keywords can be specified to display the additional information.

CLI Configuration

- To configure a custom message:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-message "The request is denied!\n"
```

- To configure a custom webpage:

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf attack-resp-message custom-page mypage
```

- To import a custom HTML webpage for NGWAF, use the **import ng-waf-custom-page** command:

```
ACOS(config)# import ng-waf-custom-page mypage
scp://hostname@192.168.1.101/ngwaf/index.html
```

NOTE: The HTML file size should not exceed 100 KB.

- To view the custom HTML webpages, use the **show ng-waf custom-page** command.
- To delete a custom HTML webpage, use the **delete ng-waf-custom-page** command:

```
ACOS(config)# delete ng-waf-custom-page mypage
```

Tracking Custom Signals

Requests that are immediately blocked or allowed by rules (configured on the Fastly dashboard) are not visible in the console. To add visibility, rules are configured to add custom signals to the requests. The Thunder device can track these custom signals using enhanced show commands. However, these commands can track only the first 64 custom signals. To reserve and track important custom signals, you need to create a class-list and bind it to NGWAF.

CLI Configuration

- To track certain custom signals, create a string type class-list (*signal_list* in this example) and add the signal names to it as shown:

```
ACOS(config)# class-list signal_list string
ACOS(config-class list)# str site.login
ACOS(config-class list)# str site.error
ACOS(config-class list)# str site.logout
```

NOTE: The class-list cannot have more than 64 entries.

- To bind the class-list (of custom signals) to NGWAF, use the **custom-signal-clist** command.

```
ACOS(config)# slb common
ACOS(config-common)# ng-waf custom-signal-clist signal_list
```

- To view the custom signals that are triggered when requests are blocked, use the **show ng-waf** command.

NOTE: Only the first 64 signal counters are displayed; the later counters (65th and above) are counted as **Unknown**.

- To view the number of custom signals that are being tracked, use the **show ng-waf status** command.
- To view all the custom signals that are being tracked, use the **show ng-waf custom-signals** command.

  This command displays the signals reserved in class-list and the signals triggered by the blocked requests.
- To clear the NGWAF custom signals that are being tracked, use the **clear ng-waf custom-signals** command.

Thunder Container

ACOS 6.0.0 introduces the following new feature and enhancement for Thunder Container:

NOTE: For Thunder Container specific configuration steps, refer *Installing Thunder Container on Docker*. For more information and details on related aXAPI statistics and counters, refer *Installing Thunder Container on Kubernetes*.

The following topic is covered:

Thunder Container Security Hardening

To enhance the security level of the container, the Thunder Container hardening has been introduced to comply with running in non-privileged users, a read-only root file system, and a minimal set of required capabilities.

Running Thunder Container in the non-privileged mode is supported for vEth, Virtio-User, and vHost-User.

Limitations

- Starting with ACOS 6.0.0, the virtio-user server container will not be launched until the vhost-user client container connects to it.
- By default, SSH to a non-privileged container is not supported. Use buddy container in deployment or use `a10cli`.
- NTPD service is not supported in the non-privileged container.
- For E810-C NIC, creating a container with an SRIOV or PCI-PT interface using the vfio-pci driver is not supported.

Threat Protection System

ACOS 6.0.0 introduces Threat Protection System (TPS). For detailed information, see New Features and Enhancements.

NOTE: For TPS-related configuration, refer to *DDoS Mitigation Guide*. Similarly, for TPS-related CLI commands, refer to *DDoS Command Line Reference Guide*.

Enhancements in ACOS 5.2.1-P12

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P12 release:

The following topic is covered:

Security Updates

The following security vulnerabilities are addressed in the ACOS 5.2.1-P12 release:

- OpenSSL Vulnerabilities
  - CVE-2023-28484: A vulnerability in libxml2 parsing of certain invalid XSD schemas can lead to a NULL pointer, leading to a segmentation fault. This affects ACOS 5.2.1 and 4.1.4-GR1 when running the WAF. This is resolved in ACOS 5.2.1-P11 and 4.1.4-GR1-P14.
  - CVE-2024-38476: A vulnerability in Apache HTTP Server may allow information disclosure, SSRF, or local script execution via malicious backend response headers. This is resolved in 5.2.1-P12 and 4.1.4-GR1-P15.
  - CVE-2024-5535: A vulnerability in SSL_select_next_proto may cause a crash or unintended memory exposure due to a buffer overread when called with an empty client protocols list, leading to a low-severity confidentiality risk. The ACOS Data Plane may be affected and is resolved in 5.2.1-P12 and 4.1.4-GR1-P15.
  - CVE-2023-5678: The vulnerability related to slow generation or checking of long X9.42 DH keys, causing a low-severity denial-of-service risk.
- A10 Vulnerability
  - A10-2024-0011: A vulnerability on port 41216 exposes weak ciphers on the A10 management IP when VCS is enabled. This port is used for configuration

synchronization between vMaster and vBlade. This is resolved in 5.2.1-P12 and 4.1.4-GR1-P14-SP1.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 5.2.1-P11

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P11 release:

The following topics are covered:

Security Updates

The following security vulnerabilities are addressed in the ACOS 5.2.1-P11 release:

- OpenSSL Vulnerabilities
  - CVE-2022-38023: Netlogon RPC Elevation of Privilege Vulnerability in Samba 3.0.37 that may allow attackers to exploit weak RC4-HMAC encryption.
  - CVE-2024-0727: OpenSSL vulnerability in processing the PKCS12 files may allow for potential Denial of Service attacks via NULL pointer dereference.
  - CVE-2024-2511: The vulnerability related to non-default TLS server configurations causing unbounded memory growth when processing TLSv1.3 sessions resulting in a Denial of Service.
  - CVE-2023-5678: The vulnerability related to slow generation or checking of long X9.42 DH keys, causing a low-severity denial-of-service risk.
- A10 Vulnerabilities
  - A10-2023-0008: A vulnerability in the A10 ACOS CLI that allows unauthorized users to gain 'root' access to the underlying operating system. Any authenticated user can run the health-monitor scripts potentially exploiting the external health function, which presents a serious security concern.
  - A10-2023-0009: The vulnerability allows unauthorized users to exploit the A10 ACOS CLI health monitor functionality, potentially leading to unauthorized access and data exfiltration.

- A10-2023-0014: A vulnerability that allows unauthorized users to overwrite files with root privileges, leading to system compromise.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 5.2.1-P10

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P10 release:

The following topics are covered:

Platforms

ACOS 5.2.1-P10 introduces the following new feature and enhancement for ACOS Platforms:

The following topics are covered:

GLM License for Low Latency Platform

ACOS 5.2.1-P10 introduces a low latency license called "3745-FPM Software license." This license is specifically introduced for specialized Thunder platforms such as 3745, with custom software designed to meet the requirements of low-latency financial applications. For example, ACOS supports the low-latency feature for Financial Information eXchange (FIX) message load balancing.

The low latency license can be acquired from A10 Global License Manager (GLM) and activated on Thunder 3745 platforms. For more information on licenses, see *Global Licensing Manager*.

Show Command

After importing or activating the license, use the **`show license-info`** command to view the license information:

```
ACOS# show license-info
Host ID         : E4532248875ED021494A8C05D771054C31DAEBF6
USB ID          : Not Available
Billing Serials: vThdb8fe8ba70000, Th8be57bdbd0000, vTh30e6da9ac0000
Token           : Not Available
Product         : CFW
Platform        : Thunder Series Unified Application Service Gateway
Burst           : Disabled
Version         : Thunder Unlimited
GIM Ping Interval In Hours : 24
------------------------------------------------------------------------
Enabled Licenses       Expiry Date (UTC)       Notes
------------------------------------------------------------------------
SLB                     None
CGN                     None
GSLB                    None
RC                      None
DAF                     None
WAF                     None
AAM                     None
FP                      None
WEBROOT                 N/A     Requires an additional Webroot license.
THREATSTOP              N/A     Requires an additional ThreatSTOP license.
...
DISK ENCRYPTION         22-April-2024
LOW LATENCY             10-March-2024
```

CLI Configuration

After successfully activating the license, use the **`low-latency`** command to enable the low latency mode:

```
ACOS(config)# slb common
ACOS(config-common)# low-latency
```

For more information, see *Command Line Interface Reference* and *Application Delivery Controller* Guides.

Maximum Concurrent Connection Limit

The maximum concurrent session limit for vThunder has been increased to 384 million sessions when running on KVM with more than 256 GB of memory. This enhancement improves the system performance and enables concurrent processing of large-scale requests.

Show Command

To view the maximum session limit, use the **show system resource-usage** command.

```
ACOS(config)#show system resource-usage
Resource                    Current    Default    Minimum    Maximum
-------------------------------------------------------------------
l4-session-count           25165824   25165824    6291456   402653184
nat-pool-addr-count              10         10         10       15000
class-list-ipv6-addr-count   524288     524288     524288     1048576
class-list-ac-entry-count     65536      65536      65536     9216000
auth-portal-html-file-size       20         20          4         120
```

Security Updates

The following security vulnerabilities are addressed in the ACOS 5.2.1-P10 release:

- OpenSSL Vulnerabilities
  - CVE-2023-3446: A vulnerability with applications using DH_check(), DH_check_ex (), or EVP_PKEY_param_check() functions to check a DH key or DH parameters and experiencing long delays during the process and potentially leading to denial of service (DoS).
  - CVE-2023-3817: A vulnerability with applications using DH_check(), DH_check_ex (), or EVP_PKEY_param_check() functions to check a DH key or DH parameters and experiencing long delays during the process and potentially leading to denial of service (DoS).

  - CVE-2023-5678: A vulnerability related to slow generation or checking of long X9.42 DH keys, causing a risk of low-severity denial-of-service.

- A10 Vulnerability
  - A10-2023-0001: A vulnerability related to a system using a weak ssh-rsa algorithm (HostKeyAlgorithms).

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 5.2.1-P9

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P9 release:

The following topics are covered:

Platforms

ACOS 5.2.1-P9 introduces the following new feature and enhancement for ACOS Platforms:

The following topics are covered:

Security Enhancement in SSH Client

ACOS device utilizes SSH client to establish a secured connection between client and server. In this release, the ACOS device supports encryption based on the Elliptic Curve Digital Signature Algorithm (ECDSA) to enhance security and align with FIPS compliance. ECDSA provides a modern and efficient approach to cryptography. It offers strong security with shorter key lengths and provides improved performance. Additionally, the SSH client now lists SSH keys and allows you to choose the required key type.

The process of generating ECDSA keys involves using the 'ssh-keygen' tool, which is similar to RSA key generation. The tool allows you to create an authentication key pair using the ECDSA algorithm with SHA-256, SHA-382, or SHA-521 digest-type. Once generated, these keys can be regenerated, loaded, and imported to the ACOS device.

For more information, see *System Configuration and Administration Guide*.

Disk Encryption Support

Starting with ACOS 5.2.1-P9, the Disk Encryption feature is supported on Thunder 3745 and Thunder 3350 devices. This feature is supported only if the device has disk encryption license applied. Disk encryption is a security technique that is used to protect data stored on a computer's hard drive or other storage devices. Using encryption algorithms, it converts data into an unreadable format known as ciphertext. It prevents unauthorized users from accessing sensitive information from the disk or storage devices as it requires a decryption key to read the data.

For more information about Disk Encryption, see the *System Configuration and Administration Guide*.

Limitation

While a device is taking a backup for disk encryption, control CPU usage may hit up to 100%.

CLI Configuration

To encrypt disk, enter the following commands:

1. To check disk encryption status before a license is applied, use the following command:

```
ACOS#sh system disk-encryption status
```

2. To import the license provided for the disk-encryption, use the glm send request (**rimacli** command), or use the following command:

```
ACOS#import glm-license disk_encryption_lic use-mgmt-port <licence_
filepath>
```

3. To enable the disk encryption with a plain passphrase, use the following command:

```
ACOS(config)#$system enable-disk-encryption cipher aes passphrase
plainpassphrasestring
```

NOTE: The passphrase length must be greater than 16 characters and less than 32 characters.

4. To check the available ciphers for disk encryption, use the following command:

```
ACOS(config)#system enable-disk-encryption cipher ?
```

5. To enable the disk encryption with a base-64 encoded passphrase, use the following command:

```
ACOS(config)#$system enable-disk-encryption cipher aes passphrase-base64 base64encodedstring
```

NOTE: The base-64 length must be greater than 16 characters and less than 32 characters and the passphrase must be in base-64 encoded format.

6. To check the disk encryption status after backup, use the following command:

```
ACOS(config)#show system disk-encryption status
```

7. To check the disk encryption status after reboot, use the following command:

```
ACOS(config)#show system disk-encryption status
```

8. (Optional) To reconfigure the device with a new cipher or passphrase base-64, use the following command:

```
ACOS(config)#$system enable-disk-encryption cipher serpent passphrase-base64 base64encodedstring
```

9. (Optional) To reconfigure the device with a new cipher or plain passphrase, use the following command:

```
ACOS(config)#$system enable-disk-encryption cipher serpent passphrase plainpassphrasestring
```

10. To check the disk encryption status before reboot, use the following command:

```
ACOS(config)#show system disk-encryption status
```

11. To check the disk encryption status after reboot, use the following command:

```
ACOS(config)#show system disk-encryption status
```

Enhancements in ACOS 5.2.1-P8

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P8 release:

The following topics are covered:

Application Access Management

ACOS 5.2.1-P8 introduces the following new feature and enhancement for Application Access Management (AAM):

NOTE: For AAM specific configuration steps, refer *Application Access Management Guide*.

The following topic is covered:

Security Support for AAM Authentication Logon

ACOS 5.2.1-P8 provides feature compatibility with the security support for AAM authentication logon implemented in the ACOS 6.0.1 release.

The **AAM Authentication Logon Form-Based** page uses a set of web pages that contain data forms. ACOS sends the Logon page in response to a request to secure services.

ACOS provides additional security features to mitigate clickjacking attacks on the **AAM Authentication Logon Form-Based** page using the X-Frame Options (XFO) feature. Clickjacking (or click hijacking) is an interface-based cyberattack that involves tricking the user into clicking on actionable content on a hidden website element (iframe layer).

For more information on the feature implementation and configuration, see the "Security Support for AAM Authentication Logon" section in *ACOS 6.0.1 New Features and Enhancements*.

Application Delivery Controller

ACOS 5.2.1 -P8 introduces the following new feature and enhancement for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for CLI commands, refer *Command Line Reference Guide*.

The following topic is covered:

Least Request Load-Balancing Method

ACOS 5.2.1-P8 provides the least-request load-balancing method feature compatibility with the ACOS 6.0.1 release.

For the least-request load-balancing method, the server selection is now based on the HTTP/HTTPS request count sent to the real server instead of the weight configured.

Additionally, the pseudo-round-robin method is used as the second level of server selection, where the server that has not been selected for the longest time, based on its timestamp, is selected.

For more information on the feature implementation and configuration, see Least Request Load-Balancing Method Enhancement.

Firewall

ACOS 5.2.1-P8 introduces the following new feature and enhancement for Firewall:

NOTE: For Firewall specific configuration steps, refer *Firewall Configuration Guide*.

The following topic is covered:

Creating Full Sessions in DSR Mode

The ACOS device creates a TCP session after completing the standard 3-way TCP handshake. However, if the device is deployed in Direct Server Return (DSR) mode, the standard TCP three-way handshake cannot be completed and therefore fully established sessions cannot be created.

The **`fw dsr-mode-support`** command is introduced to allow session creation when the device is deployed in the DSR mode. When this command is configured, a fully established session is created on receiving a single IPv4 or IPv6 TCP packet even if the standard three-way handshake is incomplete. The session is created on receiving any TCP packet except RST and FIN.

NOTE: If the **`fw allow-non-syn-session-create`** command is also enabled, a full session is created even on receiving a SYN TCP packet.

CLI Configuration

The **`fw dsr-mode-support`** command allows sessions to be created in the DSR mode based on whether the incoming TCP packets are IPv4 or IPv6.

- To create sessions for IPv4 TCP packets:

```
ACOS(config)# fw dsr-mode-support ipv4
```

- To create sessions for IPv6 TCP packets:

```
ACOS(config)# fw dsr-mode-support ipv6
```

- To create sessions for any (IPv4 or IPv6) TCP packets:

```
ACOS(config)# fw dsr-mode-support all
```

Limitations

Following are the limitations of the **`fw dsr-mode-support`** command:

- Supports session creation for TCP traffic only.
- Does not support ALG session creation.

Disabling Immediate TCP Session Closure

After receiving a TCP RST packet, A10 Firewall immediately unlinks the TCP session from the active session table before adding the session to the delete queue. Since the subsequent packets do not match the session, the TCP session closes instantly, and no packets are forwarded. The **`fw tcp-rst-close-immediate`** command is enabled by default to support this behavior so that TCP sessions close immediately after receiving RST packets. This action proves to be useful in case of a TCP Reset attack.

However, in certain scenarios, ACOS needs to forward packets even after receiving an RST. For example, if ACOS receives an RST/ACK packet from the client immediately after receiving an RST, it needs to forward the RST/ACK packet to the server. Since the **`fw tcp-rst-close-immediate`** command is enabled by default, ACOS doesn't forward RST/ACK packet to the server; instead, it sends an RST to the client and closes the connection immediately. The **`fw tcp-rst-close-immediate disable`** command can be configured to change the above-mentioned behavior.

When this command is configured, the Firewall waits for a stipulated time (1 to 2 seconds) to unlink the TCP session from the active session table before adding it to the delete queue. If ACOS receives an RST/ACK packet from the client within this time frame, the packet is forwarded to the server.

CLI Configuration

- To disable the immediate closure of TCP sessions on receiving an RST packet:

```
ACOS(config)# fw tcp-rst-close-immediate disable
```

- To enable immediate closure of TCP sessions on receiving an RST packet:

```
ACOS(config)# fw tcp-rst-close-immediate enable
```

Supporting DMZ Interfaces on Multi-PU Platforms

In an architecture that consists of multiple Processing Units (PUs), ACOS needs to distribute the incoming traffic across these PUs. On such platforms, CGN and Firewall symmetrically distribute the incoming traffic so that the same PU is chosen for processing uplink and downlink traffic within each data session.

However, the traffic flow changes when a Demilitarized Zone (DMZ) is introduced in the network. With a DMZ in the network, the traffic can flow between DMZ to the inside interface (**ip client** or **ip nat inside**) and/or DMZ to the outside interface (**ip server** or **ip nat outside**). In such scenarios, to ensure stateful handling of the incoming traffic, the following new commands are introduced:

- To configure the interface connected to the DMZ network:

  For L3 mode, use the **ip dmz** tag.

```
ACOS(config)# interface ethernet 211
ACOS(config-if:ethernet:211)# enable
ACOS(config-if:ethernet:211)# ip address 211.1.1.1 255.255.255.0
ACOS(config-if:ethernet:211)# ip dmz
```

  For L2 mode, use **traffic-distribution-mode l3-lookup** command along with **ip dmz**.

```
ACOS(config)# interface ethernet 211
ACOS(config-if:ethernet:211)# enable
ACOS(config-if:ethernet:211)# ip address 211.1.1.1 255.255.255.0
ACOS(config-if:ethernet:211)# ip dmz
ACOS(config-if:ethernet:211)# traffic-distribution-mode l3-lookup
```

- To configure a list of client IP addresses, use the **fw client class-list** command. This list is used by ACOS to identify the inside network and ensure consistent hashing of uplink and downlink traffic on multi-PU platforms.

```
ACOS(config)# class-list s2-list
ACOS(config-class list)# 11.1.1.4/32
ACOS(config-class list)# 11.1.1.1/32
```

```
ACOS(config)# fw client class-list ipv4 s2-list
```

In case of CGN, every NAT-pool change i.e., addition or removal of Subnet/IP address must reflect in the class-list entries to ensure consistent hashing on multi-PU platforms.

NOTE:

- The commands **traffic-distribution-mode l3-lookup** and **fw client class-list** are only supported on multi-PU platforms.
- To ensure that a network conversation is NATted, **ip nat-inside** and **ip nat-outside** tags must be configured for both uplink and downlink directions. However, conversations occurring between interfaces, such as **ip nat-inside** and **ip dmz** (only) or **ip nat-outside** and **ip dmz** do not undergo NAT. To NAT a conversation within the DMZ, you must configure the **ip nat-outside** tag along with the **ip dmz** tag.
- The interface tags **ip nat inside** and **ip dmz** are mutually exclusive; they cannot be configured on the same interface.

Configuring the above-mentioned commands to support the DMZ interface is deployment dependent. The configuration depends on whether the device is single-PU or multi-PU, and if the device is part of a Scaleout cluster. The various deployment scenarios and the corresponding configurations are described in the *Firewall Configuration Guide*.

MIB

ACOS 5.2.1-P8 introduces the following new feature and enhancement for MIB:

NOTE: For more information about supported MIB object details, refer *MIB Reference*.

The following topic is covered:

SNMP Support for Firewall sessions

In this release, the following new MIB object-IDs (OIDs) are added to collect information about the Firewall sessions for all processing units using SNMP:

- axfirewallGlobalFullconeCreationFailure (1.3.6.1.4.1.22610.2.4.10.139.7.1.5)
- axfirewallGlobalDataSessionFreed (1.3.6.1.4.1.22610.2.4.10.139.7.1.7)

A10 Call Home Enhancement

The Call Home feature is now enabled by default. Call Home enables ACOS devices to send information securely on how A10 products are used to the A10 Product Research team. This information includes configuration and environmental data such as the ACOS device, its form factor, deployment location (such as on-premise, public cloud, and so on), number of interfaces, L3V partitions, VLANs, and more. Additionally, it collects information on the ACOS licenses activated on the device. All the information collected is used to improve the quality of the product.

The Call Home data is collected from the ACOS device every 24 hours at midnight. You can manually offset the Call Home time by 1 to 60 minutes.

All information collected by A10 is processed in accordance with A10 Networks' Data Processing Addendum. However, if any PII is received, it will be processed in accordance with A10 Networks' Data Processing Addendum. All information received through the Call Home feature is anonymized and used purely to enhance our products and improve quality.

NOTE: For detailed information about Call Home, refer *System Administration and Configuration Guide*.

For Call Home to work, the following conditions must be met:

- **Internet Connection** — The ACOS device must be able to reach the internet for Call Home to send diagnostic data to the A10 centralized collector. This feature does not work with proxy server configuration.

NOTE: Call Home uses the management interface to send data to the A10

centralized collector.

- **Port** — The Call Home data from your ACOS device is sent over TLS protocol using port 443 by default. It is important to note that, in order to send data from your ACOS device to the A10 Product Research team, you must whitelist the following:
  - Call Home Endpoint: callhome.a10networks.com
  - Static IP address: 129.153.110.25

NOTE: Call Home is enabled by default from ACOS 5.2.1-P8 and 6.0.2 versions onwards. You can choose to manually disable the Call Home feature on your ACOS device.

CLI Configuration

To disable Call Home, enter the following commands and save your configurations:

```
ACOS(config)# call-home profile
ACOS(config-profile)# deregister
```

The `deregister` command disables the Call Home service and stops the ACOS device from sending data to A10.

To reenable Call Home on the ACOS device, ensure that the device has internet connectivity from the management plane. Then, enter the following commands and save the configurations.

```
ACOS(config)# call-home profile
ACOS(config-profile)# register
```

The `register` command enables the Call Home service. Once enabled, the Call Home data is collected from the ACOS device every 24 hours at midnight. You can manually offset the Call Home time by 1 to 60 minutes.

```
ACOS(config-profile)# time <1-60> mins
```

For example, if you configure the offset time as 5 mins, the data will be exported at 12:05 AM.

Security Updates

The following security vulnerabilities are addressed in the ACOS 5.2.1-P8 release:

- OpenSSL Vulnerabilities
  - CVE-2023-0465: A vulnerability with applications using non-default options when verifying certificates may affect the ACOS data plane.
- ReDos Vulnerability
  - CVE-2022-3517: A vulnerability in the nodejs-minimatch package that allowed a Regular Expression Denial of Service (ReDoS) when calling the braceExpand function with specific arguments, resulting in a Denial of Service.
- A10 Vulnerability
  - A10-2023-0001: A vulnerability related to clickjacking in AAM Authentication form-based logon page. The AAM Authentication template has been enhanced to support X-Frame options.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 5.2.1-P7

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P7 release:

The following topics are covered:

Application Delivery Controller

ACOS 5.2.1 -P7 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for CLI commands, refer *Command Line Reference Guide*.

The following topics are covered:

ADC Support on Multi-PU

ADC implementation is supported on high-performance Multiple Processing Unit (multi-PU) platforms such as Thunder 7650/7655S. These platforms are built for large-scale traffic distribution, load balancing, and scalability. The multi-PU architecture has two active PUs; PU1 and PU2. The traffic for the same object is distributed to the two PUs running the specific object. All Layer 7 traffic, such as HTTP, HTTPS, SSL, and DNS, is distributed across all PUs.

In the previous releases, traffic distribution in the multi-PU was based on the VRID system, where each PU required a unique SLB virtual server with a separate odd-even VRID. This allowed SLB virtual server to be in active-standby mode.

With this release, multi-PU can also utilize client-side and server-side (odd-even NAT) IP addresses to determine the traffic distribution to PU1 and PU2. This means that traffic sent from an odd source IP to the same VIP is sent to PU1, while traffic sent from an even source IP to the same VIP is sent to PU2. This allows a single SLB virtual server to be shared across both PU1 and PU2. Additionally, the SLB traffic statistics are aggregated as a single device.

For detailed information on ADC multi-PU implementation, see *Application Delivery Controller Guide.*

CLI Configuration

A new command **odd-even-nat-enable** is introduced in the SLB common configuration to enable seamless traffic distribution.

```
ACOS(config)# slb common
ACOS(config-common)# odd-even-nat-enable
```

Show Commands

After configuring the **odd-even-nat-enable** command, the following show commands display the aggregated counters for PU1 and PU2 (PU1 + PU2):

- **show slb server** and its related commands.
- **show slb virtual-server** and its related commands.

  (except **show slb virtual-server** *<vs> <port_num> <port_type>***dns-cache entry**)

- **show ip nat pool** and its related commands.

For more information on these commands, see *Command Line Interface Reference*.

DNS Response Rate Limiting Enhancements

ACOS provides the DNS Response Rate Limiting (RRL) feature to prevent your network equipment from becoming the target of DNS reflection or amplification attacks. Additionally, DNS server responses are provided with RRL settings to avoid unnecessary load on authoritative DNS servers.

This release enhances the existing DNS RRL solution to support new rate-limiting capabilities to prevent DDoS attacks. The DNS responses or requests are monitored to detect any abnormal increase in rate or frequency. This effectively reduces the likelihood of the DNS resolver being used to launch a DDoS attack against a valid client.

The following RRL features are introduced in the SLB template DNS:

- TC-rate – This option configures the rate at which the DNS server responds with a truncated (TC) response. Every nth rate-limited request will get a response with the TC bit.
- Subnet matching (IPv4 or IPv6) - This option configures the IPv4 or IPv6 prefix length to indicate the subnet size in which the incoming queries are grouped, and rate limited.
- Source IP only - This option allows rate limiting based on source IP only instead of FQDN.

For more information, see *DDoS Mitigation Guide (For ADC)* and *Command Line Interface Reference*.

CLI Configuration

To enable the new RRL settings in the SLB template DNS, use the following commands:

```
ACOS(config)# slb template dns dns_rrl
ACOS(config-dns)# response-rate-limiting
ACOS(config-dns-response-rate-limiting)# TC-rate num
ACOS(config-dns-response-rate-limiting)# match-subnet {/masklength |
ipv4-address}
ACOS(config-dns-response-rate-limiting)# match-subnet-v6 num
ACOS(config-dns-response-rate-limiting)# src-ip-only
```

For example,

```
ACOS(config)# slb template dns dns_rrl
ACOS(config-dns)# response-rate-limiting
ACOS(config-dns-response-rate-limiting)# TC-rate 3
ACOS(config-dns-response-rate-limiting)# match-subnet 255.255.255.0
ACOS(config-dns-response-rate-limiting)# src-ip-only
```

NOTE: DNS RRL feature works only when the template is bound to virtual port type **dns-udp**.

Block HTTP Methods

ACOS provides a feature to block the HTTP method using disallowed HTTP method option. Some of the HTTP methods such as TRACE, HEAD, CONNECT and so on can be used for malicious purposes and pose security risk for the web application. Hence, to protect your web applications you can disallow the HTTP methods which are not used frequently.

This feature lets you block the HTTP methods and enables 'drop' action when the conditions are met. Before dropping the request, ACOS sends a 400 response to the client-side. This option can be used for all the HTTP protocol or versions (HTTP 1.1, HTTP/2, and HTTP/3).

The methods that can be disallowed are: GET, BIND, CONNECT, COPY, DELETE, HEAD, LABEL, LOCK, MERGE, MKCOL, MOVE, OPTIONS, PATCH, POST, PRI, PROPFIND, PROPPATCH, PUT, REBIND, TRACE, UNBIND, UNLINK, UNLOCK, UPDATE, PURGE, TRACK.

CLI Configuration

To block the HTTP methods, use the **disallowed-methods** command in the SLB template HTTP:

```
ACOS(config)# slb template http http_test
ACOS(config-http)# disallowed-methods "TRACE CONNECT" action drop
```

Enhancements to Persist Cookie Expiration

ACOS supports the Persist Cookie Expiration feature, which allows you to explicitly set the cookie's expiration time. This feature is enhanced further to include the following options:

- Max-age: When this attribute is used, ACOS sets an expiration time (in seconds) for the cookie. The 'max-age' attribute is useful when the client and ACOS are not synchronized with the Network Time Protocol (NTP) server. Unlike ‘expire’ attribute, this attribute is independent of the date and time configuration between ACOS and the client.

- Expires: When this attribute is set, ACOS sets an expiration date and time for the cookie instead of just time. This attribute works in the same way as the previous ‘expire’ option.
- All: When this attribute is set, ACOS inserts both the 'max-age' and 'expires' attributes for cookie expiration. The ‘all’ attribute is helpful when the client is using different browser versions and supports either the ‘max-age’ or ‘expires’ attributes for cookie expiration.

Example: A cookie with max-age set to 120 means, the cookie expires 120 seconds after it is received on the client. On the other hand, if the expires attribute is used and if the client clock is set to five minutes advanced time than the standard time, the cookie will expire as per the NTP server clock time, which can be immediately after it is received on the client.

CLI Configuration

The following commands are introduced in the expire command of SLB template HTTP:

```
ACOS(config)# slb template persist cookie template-name
ACOS(config-cookie persist)# expire seconds use-attribute {max-age | expires | all}
```

For example,

```
ACOS(config)# slb template persist cookie persist_test
ACOS(config-cookie persist)# expire 120 use-attribute max-age
```

Carrier Grade NAT

ACOS 5.2.1-P7 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

NOTE: For CGN or CGNAT specific configuration steps, refer *IPv4-to-IPv6 Transition Solutions Guide*.

The following topics are covered:

Additional IPFIX Information Element (IE)

ACOS supports fixed and custom IPFIX templates with different Information Elements (IEs) to export logging information to the collectors, where the information is stored and analyzed.

This release adds the following new RFC-defined IEs:

- Application Category Name
- Application Subcategory Name

  These IEs can be exported as NetFlow fields and are used to determine the application category for application visibility and category-based policing.

Also, for compliance with the RFC standards, the Private Enterprise Number (PEN) for the Application Name (ID 96) is removed.

For more information, see the *Traffic Logging Guide* and *Command Line Reference Guide*.

Enhanced DDoS Protection with RTBH

In case of a DDoS attack, if the Remotely Triggered Black Hole (RTBH) protection mechanism is triggered, ACOS initiates the Border Gateway Protocol (BGP) route and unconditionally drops all traffic directed to the victim IP (by routing it to the black hole). Rate limiting stops and the victim NAT IP is blackholed i.e., it is inaccessible.

However, in certain scenarios, it may be necessary to access the victim NAT IP. Consider a case where many subscribers use a NAT IP to communicate with the outside servers. When the RTBH is triggered, all traffic to the NAT IP is dropped unconditionally. Although the attack is mitigated, all subscriber connects are also interrupted since the NAT IP is inaccessible.

The **`forward`** option is introduced to handle such disruptions. When this option is configured, ACOS forwards the traffic instead of dropping it unconditionally. This allows subscribers to access the NAT IP under attack even when RTBH is in effect.

CLI Configuration

To enable this feature, the **forward** option needs to be specified while configuring the RTBH action. The following example demonstrates the usage:

```
ACOS(config)# cgnv6 ddos-protection packets-per-second ip <threshold>
action redistribute-route <map> forward
```

Support for RFC Standard Field Length

ACOS supports several IPFIX Information Elements (IEs) that use non-standard field lengths that the collectors (that follow the RFC standard field length) do not recognize. As a result, the IPFIX packets sent by the ACOS devices are not parsed correctly by the collectors without customization.

Additionally, in the fixed templates, some predefined fields use non-standard field lengths. These can confuse the collectors if they receive two different template definitions of the same ID.

The following are introduced to support both standard and non-standard RFC field lengths to ease the integration with the collector:

- A new command - `system rfc-ipfix-ie-spec <enable | disable>` to enable or disable the use of RFC-defined IPFIX information element lengths.
- New fixed template IDs to use the RFC standard field lengths.

CLI Configuration

- To use the RFC-defined field lengths for the Information Element (IE) identifier:

  ```
  system rfc-ipfix-ie-spec enable
  ```

- To use the non-standard field lengths for the Information Element (IE) identifier:

  ```
  system rfc-ipfix-ie-spec disable
  ```

Known Limitation

The ACOS device cannot be configured to support both RFC and non-RFC standards.

For more information, see the *Traffic Logging Guide* and *Command Line Reference Guide*.

Firewall

ACOS 5.2.1 -P7 introduces the following new features and enhancements for Firewall:

NOTE: For Firewall specific configuration steps, refer *Firewall Configuration Guide*.

The following topics are covered:

Enhanced Automatic Update Feature

In the earlier releases, the automatic-update feature for the Application Aware Firewall bundle was not supported on the dual blade chassis platform. Hence, the bundle updates were only available on PU1.

In this release, the automatic-update feature has been enhanced for Thunder 14045 and Thunder 7650 dual chassis platforms to support actions such as check-now, schedule, revert, and reset. The application aware firewall bundle, CA certificate bundle, and a10-threat-intel class list are automatically synced from PU1 to PU2 when the automatic update schedule is triggered.

Additionally, the **`show rule-set <rule-set name> application`** command is enhanced to display the aggregated counters of PU1 and PU2 (PU1 + PU2) on the chassis platform.

For more information, see *Command Line Interface Reference*.

Enhanced DDoS Protection with RTBH

In case of a DDoS attack, if the Remotely Triggered Black Hole (RTBH) protection mechanism is triggered, ACOS initiates the Border Gateway Protocol (BGP) route and unconditionally drops all traffic directed to the victim IP (by routing it to the black hole). Rate limiting stops and the victim IP is blackholed i.e., it is inaccessible.

However, there are certain scenarios where subscribers might need to reach the victim IP. Consider an example where the victim IP is a DNS server. When ACOS detects a DDoS attack, when RTBH action is initiated, all traffic to the DNS server is dropped. Although the attack is mitigated, the DNS server users are unable to access the DNS service.

The **forward** option is introduced to handle such situations. When this option is configured, ACOS forwards the traffic (instead of dropping it unconditionally) and continues to rate-limit the traffic directed to the victim IP. This allows subscribers to access the DNS service even when RTBH is in effect.

CLI Configuration

To enable this feature, the **forward** option needs to be specified while configuring the RTBH action. The following example demonstrates the usage:

```
ACOS(config)# fw ddos-protection action redistribute-route <map> forward
```

Distributed Rate-Limiting for Multi-PU Platforms and Scaleout Cluster

In a Scaleout cluster or a Multi-PU environment, if the scope associated with a rate limit entry is **subscriber-ip** or **subscriber-prefix**, rate limiting can be applied since the whole traffic is directed to a single PU (or node) in the Multi-PU platform or Scaleout cluster (assuming that the system's **ipv6-prefix-length** is set correctly). However, if the scope associated with the rate-limit entry is **aggregate**, the traffic to be rate-limited cannot be directed to a single PU (or node). The packets land on multiple PUs (or nodes) in the Multi-PU platform or cluster, making rate-limiting difficult. Distributed rate limiting is introduced to enforce rate-limiting in such cases. It ensures a uniform division of resources across PUs in a Scaleout cluster or Multi-PU platform.

Distributed rate-limiting is applicable in the following scenarios, only for rate-limit entries having scope **`aggregate`**:

- Scaleout cluster – Rate limiting is applied to the traffic stream if the packets land on multiple nodes in the cluster. Every node in the Scaleout cluster periodically checks the current number of active nodes (n) in the cluster and utilizes an effective rate-limit, which is 1/n times the configured rate-limit. For example, if the configured rate limit is 20 Mbps and there are five nodes currently active in the cluster, each node in the cluster will enforce a rate-limit of 4 Mbps (20/4).
- Dual-PU platform – Rate limiting is applied to the traffic stream if the packets land on both PUs. However, the rate limit distribution depends on whether the PUs (in a multi-PU node) are part of a Scaleout cluster or not.
  - If the PUs are not part of a Scaleout cluster, each PU periodically checks the current number of PUs (m) in the node and utilizes an effective rate-limit, which is 1/m times the configured rate-limit. For example, on a Dual-PU platform, if the configured rate limit is 20 Mbps, each PU will enforce a rate-limit of 10 Mbps (20/2).
  - If the PUs are part of a Scaleout cluster, each PU periodically checks the current number of active nodes (n) in the cluster as well as the current number of PUs (m) in the node and then utilizes an effective rate-limit, which is 1/(m*n) times the configured rate-limit. For example, on a Dual-PU platform, if the configured rate limit is 20 Mbps and there are five nodes in the cluster, each PU will enforce a rate-limit of 2 Mbps (20/2*5).

NOTE: Rate-limiting accuracy depends on whether the traffic distribution is balanced between nodes/PUs. If all the nodes or PUs receive traffic (roughly) equally, the enforced rate limit will be in accordance with the above-mentioned distribution scheme.

Limitations

- Only applicable for rate-limit entries with scope aggregate.
- Does not create a shadow session if rate-limit is configured for the flow. Shadow sessions mimic the Active node sessions and help minimize the redirection of packets.

iDDoS Enhancement for Firewall Deny Rules

Prior to this release, iDDoS protection could only be associated with Permit rules, i.e., the DDoS rate-limiting template policy could only be bound to the Permit rules. This left a security hole in infrastructure protection as the traffic that matched the Deny rules was not considered for DDoS protection.

To enhance the security level and infrastructure protection capabilities, the iDDoS functionality can now be associated with Deny rules. Binding the DDoS rate limiting policy to the Deny rules makes it possible to track the packets that are being denied separately. When the number of packets exceeds the configured DDoS protection threshold, a DDoS attack is detected. Once the attack is detected, the upstream router can be signalled so that the network can provide DDoS mitigation for this BGP announcement. Thus, this technique enables early detection and mitigation of DDoS attacks and provides infrastructure protection to the Gi Firewall layer as well.

NOTE: The template limit-policy cannot be bound to an implicit deny rule. You must configure an explicit deny rule for this mechanism to function as expected.

CLI Configuration

In the following configuration example, a DDoS rate limiting policy (10) is bound to a deny rule.

```
ACOS(config)# template limit-policy 10
ACOS(config-limit-policy)# limit-pps downlink 100 ddos-protection-factor
2

ACOS(config)# rule-set firewall
ACOS(config-rule set:firewall)# rule r1
ACOS(config-rule set:firewall-rule:1)# source ipv4-address any
ACOS(config-rule set:firewall-rule:1)# source zone any
ACOS(config-rule set:firewall-rule:1)# dest ipv4-address 20.20.20.141/32
ACOS(config-rule set:firewall-rule:1)# dest zone any
ACOS(config-rule set:firewall-rule:1)# service any
ACOS(config-rule set:firewall-rule:1)# application any
ACOS(config-rule set:firewall-rule:1)# action-group
ACOS(config-rule set:firewall-rule:1-acti...)# deny limit-policy 10
```

Limitations

- Only supported for Packets-Per-Second downlink traffic.
- Only supported for the Access control rule-set i.e., the DDoS rate limit policy cannot be bound to a deny rule configured under the Traffic control rule-set.

Supporting DMZ Interfaces

GiFW supports interface level tags such as **ip nat inside**, **ip client**, and **map-e inside** to identify the interface connected to the subscriber network, thereby identifying the private IP (to be NATted to a public IP). Similarly, the tags **ip nat outside**, **ip server**, and **map-e outside** are used to identify the internet or destination network that the subscriber is trying to access.

The **ip dmz** interface tag is introduced to identify the interfaces connected to the Demilitarized Zone (DMZ).

CLI Configuration

Use the **ip dmz** command to configure the DMZ-facing interface. This command can be configured under **interface ethernet** as well as **interface ve**.

- To configure **ip dmz** under **interface ethernet**:

```
ACOS(config)# interface ethernet 3
ACOS(config-if:ethernet:3)# ip address 10.0.3.18 255.255.255.0
ACOS(config-if:ethernet:3)# ip dmz
```

- To configure **ip dmz** under **interface ve**:

```
ACOS(config)# interface ve 3250
ACOS(config-if:ve:3250)# ip address 10.0.3.18 255.255.255.0
ACOS(config-if:ve:3250)# ip dmz
```

Limitations

Following are the limitations while supporting a DMZ interface:

- DMZ configuration is not supported for Multi-PU appliances in a Firewall deployment.

- The interface tags **ip nat inside** and **ip dmz** are mutually exclusive; they cannot be configured on the same interface. However, **ip nat outside** and **ip dmz** can be configured on the same interface.

Supporting Throughput Rate Limits in Kbps

Prior to this release, while configuring the template limit policy, the threshold for the throughput rate limit could only be configured in Megabits per second (Mbps). To increase the granularity, the template limit policy has been enhanced so that you can configure the throughput threshold limits in Kilobits per second (Kbps). However, the configured rate limit must be greater than or equal to 100 Kbps.

NOTE: Mbps is the default unit while configuring the throughput limit.

CLI Configuration

The following commands configure the throughput rate limit on the uplink, downlink, and total traffic in Kbps.

```
ACOS(config)# template limit-policy1023
ACOS(config-limit-policy)# limit-scope subscriber-prefix24
ACOS(config-limit-policy)# limit-throughput downlink200Kbps
ACOS(config-limit-policy)# limit-throughput uplink300Kbps
ACOS(config-limit-policy)# limit-throughput total600Kbps
```

Additionally, the **show fw rate-limit** command is enhanced to display the throughput limits for the rate limit entries in Bits per second instead of Bytes per second.

GTP Firewall

ACOS 5.2.1-P7 introduces the following new feature and enhancement forGTP Firewall:

NOTE: For more information, refer ‘GTP Firewall’ in the Firewall Configuration Guide.

The following topic is covered:

Multi-PU Support for GTP Firewall

Starting with ACOS 5.2.1-P7, GTP Firewall supports multi-blade and multi-processing unit platforms. In this release, the GTP Firewall has been enhanced to allow legitimate traffic to be distributed and processed seamlessly across multiple PUs.

Limitation

Rate-limiting may not work as expected on multi-PU platforms.

Harmony Controller Integration

ACOS 5.2.1-P7 introduces the following new feature and enhancement for Harmony Controller (HC) Integration:

NOTE: For more information, refer *Harmony Controller Integration Guide*.

The following topic is covered:

Enable or Disable Harmony Controller Analytics

In the previous releases, ACOS exported all the device data to Harmony Controller (HC) by default when the ACOS device is registered in HC. This had significant impact on the capacity of HC.

To manage the capacity of HC and the exported data more efficiently, ACOS provides a feature to choose which type of analytics can be exported to HC. Depending on the requirement, you can enable one of the following options:

- System - If HC has only the device management license, you can export only the system-level data to HC.
- Disable - If you do not want to export any device data to HC, you can disable or turn off HC analytics.

- All - If you want to re-enable exporting all the device analytics to HC, you can choose ‘All’. This is the default option.

CLI Configuration

To enable this feature, use the following command:

```
ACOS(config)# harmony-controller profile
ACOS(config-profile)# analytics {all | system | disable}
```

For more information, see *Command Line Interface Reference*.

GUI Configuration

To enable this feature, navigate to **System > Admin > Controller** and select one of the following options from the **Analytics** drop-down list:

- All
- System
- Disable

For more information, see *Online Help*.

MIB

ACOS 5.2.1-P7 introduces the following new feature and enhancement for MIB:

NOTE: For more information about supported MIB object details, refer *MIB Reference*.

The following topic is covered:

SNMP OIDs Support for Multi-PU

In the earlier releases, the SNMP OIDs were not supported on the multi-PU platforms. Hence, accurate data was only available on single-PU platforms.

In this release, new SNMP OIDs are added under A10-AX-CHASSIS to support both single-PU and multi-PU platforms. This enhancement helps to detect network faults on the multi-PU platform using aXAPI.

In multi-PU platforms, the slot filters are used to collect data from each Processing Unit (PU) or aggregated data from both PUs. By default, aXAPI automatically aggregates statistical data from both PUs.

A value is set with the slot filter that indicates the 'slot ID' for PU1, PU2, or both.

For multi-PU platforms:

- When the ‘slot ID’ is set to 1, the statistical and operational data is fetched from PU1.
- When the ‘slot ID’ is set to 2, the statistical and operational data is fetched from PU2.
- When the 'slot ID' is set to 0, all the statistical data is aggregated for PU1 and PU2. But not all the operational data has aggregated counters for PU1 and PU2.

For single-PU platforms, there is no aggregate or slot ID = 0.

Table 2 lists the SNMP OIDs on single-PU platforms and their corresponding SNMP OIDs supported on multi-PU platforms:

Table 2 : SNMP OIDs on Single-PU and Multi-PU platforms

SNMP OIDs on Single-PU Platforms	SNMP OIDs on Multi-PU Platforms
• axInterfaceStatErrorsOut (1.3.6.1.4.1.22610.2.4.1.7.1.2.1.1.9) • axInterfaceStatDropsIn (1.3.6.1.4.1.22610.2.4.1.7.1.2.1.1.10) • axInterfaceStatDropsOut (1.3.6.1.4.1.22610.2.4.1.7.1.2.1.1.11) • axInterfaceStatCollisions (1.3.6.1.4.1.22610.2.4.1.7.1.2.1.1	A new table axEthIntfStatsTable is added containing the following OIDs: • axEthIntfStatsSlotId (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.1) • axEthIntfStatsIfNum (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.2) • axEthIntfStatsRateBitsRcv (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.3) • axEthIntfStatsRateBitsSend (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.4)

Table 2 : SNMP OIDs on Single-PU and Multi-PU platforms

SNMP OIDs on Single-PU Platforms	SNMP OIDs on Multi-PU Platforms
.12) • axInterfaceStatUtilPercentIn (1.3.6.1.4.1.22610.2.4.1.7.1.2.1.1.15) • axInterfaceStatUtilPercentOut (1.3.6.1.4.1.22610.2.4.1.7.1.2.1.1.18)	• axEthIntfStatErrorsIn (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.5) • axEthIntfStatErrorsOut (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.6) • axEthIntfStatDropsIn (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.1.7) • axEthIntfStatDropsOut (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.8) • axEthIntfStatCollisions (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.9) • axEthIntfStatUtilPercentIn (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.10) • axEthIntfStatUtilPercentOut (1.3.6.1.4.1.22610.2.4.4.1.2.2.3.1.11)
• customSessionEventNat44CreationRecordsSentFailure (1.3.6.1.4.1.22610.2.4.10.126.2.1.1.1.43) • customSessionEventNat44DeletionRecordsSentFailure (1.3.6.1.4.1.22610.2.4.10.126.2.1.1.1.49)	A new table axNetflowMonitorStatsTable is added with the following OIDs: • axNetflowMonitorStatsSlotId (1.3.6.1.4.1.22610.2.4.4.1.2.6.1.1.1) • axNetflowMonitorStatsCustomSessionEventNat44CreationRecordsSentFailure (1.3.6.1.4.1.22610.2.4.4.1.2.6.1.1.3) • axNetflowMonitorStatsCustomSessionEventNat44DeletionRecordsSentFailure (1.3.6.1.4.1.22610.2.4.4.1.2.6.1.1.4)
• tcpEstCounter (1.3.6.1.4.1.22610.2.4.10.39.55.1.10) • tcpHalfOpenCounter	Three new OIDs are added to an existing table axSessionStatsTable: • axSessionStatsTcpEstCounter (1.3.6.1.4.1.22610.2.4.4.1.2.1.3.1.13)

Table 2 : SNMP OIDs on Single-PU and Multi-PU platforms

SNMP OIDs on Single-PU Platforms	SNMP OIDs on Multi-PU Platforms
(1.3.6.1.4.1.22610.2.4.10.39.55.1.11) • tcpEstabRate: ((100*tcpEstCounter)/ ((tcpEstCounter)+ (tcpHalfOpenCounter))) (This is a new added object.)	• axSessionStatsTcpHalfOpenCounter (1.3.6.1.4.1.22610.2.4.4.1.2.1.3.1.14) • axSessionStatsTcpEstabRate (1.3.6.1.4.1.22610.2.4.4.1.2.1.3.1.97)
• axAppGlobalTotalNewIPNatConnections (1.3.6.1.4.1.22610.2.4.3.1.2.5)	The following OID is added to an existing table axSystemAppPerformanceTable: • axSystemAppPerformanceNatCpi (1.3.6.1.4.1.22610.2.4.4.1.2.1.2.1.4)
• axGlobalTotalL4SessionInteger (1.3.6.1.4.1.22610.2.4.3.1.2.12)	An existing OID is used from the table axSessionStatsTable: • axSessionStatsConnCount (.1.3.6.1.4.1.22610.2.4.4.1.2.1.3.1.5)
• axSysCpuUsage (1.3.6.1.4.1.22610.2.4.1.3.2.1.2)	The existing OIDs are used from the table axCurrFiveSecDataCpuUsageTable: • axCurrFiveSecDataCpuUsageSlotId (.1.3.6.1.4.1.22610.2.4.4.1.1.1.9.1.1) • axCurrFiveSecDataCpuId (.1.3.6.1.4.1.22610.2.4.4.1.1.1.9.1.2) • axCurrFiveSecDataCpuUsage (.1.3.6.1.4.1.22610.2.4.4.1.1.1.9.1.3)
• axSysCpuCtrlCpuFlag (1.3.6.1.4.1.22610.2.4.1.3.2.1.4)	The existing OIDs are used from the table axCurrFiveSecCtrlCpuUsageTable: • axCurrFiveSecCtrlCpuUsageSlotId (.1.3.6.1.4.1.22610.2.4.4.1.1.1.10.1.1)

Table 2 : SNMP OIDs on Single-PU and Multi-PU platforms

SNMP OIDs on Single-PU Platforms	SNMP OIDs on Multi-PU Platforms
	• axCurrFiveSecCtrlCpuId (.1.3.6.1.4.1.22610.2.4.4.1.1.1.10.1.2) • axCurrFiveSecCtrlCpuUsage (.1.3.6.1.4.1.22610.2.4.4.1.1.1.10.1.3)
• axGlobalAppPacketDrop (1.3.6.1.4.1.22610.2.4.3.1.2.8) • axGlobalTotalAppPacketDrop (1.3.6.1.4.1.22610.2.4.3.1.2.9)	A new table axSystemAppBufferTable is added with the following OIDs: • axSystemAppBufferSlotId (1.3.6.1.4.1.22610.2.4.4.1.2.1.5.1.1) • axSystemAppBufferDrop (1.3.6.1.4.1.22610.2.4.4.1.2.1.5.1.2) • axSystemAppBufferTotalDrop (1.3.6.1.4.1.22610.2.4.4.1.2.1.5.1.3)

Limitation

- The multi-PU platform support is available for a limited number of interfaces, netflow, and system session SNMP OIDs. Hence, the SNMP OIDs that are not under A10-AX-CHASSIS may not provide accurate data for the multi-PU platforms.

For more information, refer *aXAPIv3 ReferenceGuide*.

Overlay Networks

ACOS 5.2.1-P7 introduces the following new feature and enhancement for Overlay Networks:

NOTE: For more information, refer *Configuring Overlay Networks Guide*.

The following topic is covered:

Adhoc VTEP Remote-IP Support for GRE and IPinIP Tunnels

ACOS supports both point-to-point and point-to-multipoint tunnels. A Virtual Private Network (VPN) in a point-to-point tunnel is set up between a Thunder device and a single destination. Similarly, multiple destinations virtual tunnel endpoints (VTEPs) are connected to the Thunder device in a point-to-multipoint tunnel.

In a point-to-multipoint tunnel configuration, there are large number of remote tunnels and their remote IP addresses are unknown to ACOS. It is practically not possible to configure all the remote tunnel endpoints. Therefore, ACOS dynamically creates a single tunnel using GRE and IPinIP encapsulation without specifying a remote IP address for every tunnel endpoint. Such a tunnel is called an 'adhoc' tunnel.

The adhoc tunnel originates from the remote tunnel endpoint and ends at the local IP address. Each endpoint connected to the Thunder device through an adhoc tunnel has a unique IP address.

For an adhoc tunnel configuration:

- A dedicated unique Logical Interface (LIF) is configured to hold multiple remote tunnel endpoints.
- A local IP address is configured for every remote tunnel endpoint and every overlay tunnel in the partition.
- A class-list can be bound to the remote IP address.

The adhoc tunnel supports:

- IPv4 and IPv6 addresses
- Fragmentation and Jumbo frames
- CGNAT (NAT44 and NAT64 translation) and Firewall traffic
- L3V partition

For more information, see the *Configuring Overlay Networks* and *Command Line Interface Reference*.

CLI Configuration

To configure an adhoc tunnel with IP limiting, a new option **`class-list`** is

introduced in the **remote-ip-address** command.

```
ACOS(config)# overlay-tunnel vtep vtep-id
ACOS(config-overlay-tunnel:vtep-id)# remote-ip-address 0.0.0.0 /0 class-list name
```

Show Commands

- To view the encap table entries, a new option **encap-table** is introduced in the **show overlay-tunnel** command.
- To view the VTEP information, the **show arp** and **show ipv6 neighbour** commands are modified.

Limitations

- The number of adhoc tunnel endpoints supported is 16K.
- GRE tunnel keepalives are supported only with point-to-point GRE tunnels but not with an adhoc GRE tunnel.
- IP-Encap health monitoring is unavailable for the adhoc tunnel endpoints.
- The class-list modifications (IPv4/IPv6 addition or removal) are effective only on the new encap entries being added in the encap table after the class-list has been modified but not on the existing encap entries.
- Scaleout is not supported.
- Multi-PU systems such as Thunder 7650(S) are not supported.
- The adhoc overlay and LIF configurations must be in the same partition.
- IPv6 GRE underlay is not supported.

Platforms

ACOS 5.2.1-P7 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

Support for Thunder 5840-QSSL

This release supports Thunder 5840-QSSL SKU(s), a Thunder 5840 series platform powered by Intel QuickAssist Technology (QAT). QAT provides ACOS with a hardware-enabled foundation for SSL Insight with TLS 1.3 protocol.

CLI Configuration

To check if your Thunder series platform supports QAT, use the **`show hardware`** command.

```
Thunder Series Unified Application Service Gateway TH5840
      Serial No  : TH5840000000002
      CPU        : Intel(R) Xeon(R) Gold 6138T CPU @ 2.00GHz
                   80 cores
                   4 stepping
      Storage    : Total 476G drive
      Memory     : Total System Memory 193602 Mbytes
      SSL Cards  : 6 device(s) present
                   6 QAT SSL device(s)
      L2/3 ASIC  : 3 device(s) present
      IPMI       : IPMI Present
      Ports      : 16
      Flags      : CF
      SMBIOS     : Build  5
                    06/11/2022
      FPGA       : 8 instance(s) present
Date: 07/23/2022
```

Increased L4 Concurrent Sessions

The number of L4 concurrent sessions per processing unit (PU) has been increased based on the system memory size. This enhancement improves the system performance and enables concurrent processing of large-scale requests.

The software enhancements have been integrated into ACOS 5.2.1-P6-SP1 release onwards. The following Thunder models support the increased L4 concurrent sessions:

- Thunder 7655S - up to 768M (million)
- Thunder 6655S - up to 384M

This means that per PU can support 384M concurrent sessions if the memory per PU is 192 GB and above.

CLI Configuration

To set the total concurrent sessions, use the **system resource-usage l4-session-count** command.

```
TH7655S(config)# system resource-usage l4-session-count ?
<16777216-402653184> Total Sessions in the System
```

NOTE: A reboot is required to apply the setting.

Show Command

- To view the hardware information, use the **show hardware detail** command.

```
TH7655S#show hardware detail
Thunder Series Unified Application Service Gateway TH7655S
      Serial No  : TH76025020240018
      CPU        : Intel(R) Xeon(R) Gold 6258R CPU @ 2.70GHz
                   56 cores
                   7 stepping
      Storage    : Single 238G drive, Free storage is 89G
      Memory     : Total System Memory 191699 Mbytes, Free Memory
122074 Mbytes
      SSL Cards  : 9 device(s) present
                   9 QAT SSL device(s)

      L2/3 ASIC  : 3 device(s) present
      IPMI       : IPMI Present
      SP Engine  : Present

      Ports      : 16
      Flags      : CF
      SMBIOS     : Build  5.14
                     07/22/2020
```

```
      FPGA       : 4 instance(s) present
                   Date: 12/02/2021
      MCPLD Type : 4
                   Date: 05/05/2020
```

- To view the sessions per PU, use the **`show session`** command.

```
TH7655S# show session
Processing-Unit 1
Traffic Type                          Total
---------------------------------------------
Total Sessions                        0
TCP Established                       0
TCP Half Open                         0
Server TCP Established                0
Server TCP Half Open                  0
SCTP Established                      0
SCTP Half Open                        0
UDP                                   0
Non TCP/UDP IP sessions               0
Other                                 0
Reverse NAT TCP                       0
Reverse NAT UDP                       0
Curr Free Conn                        402562828  (384*1024*1024)
Conn Count                            0
Conn Freed                            0
TCP SYN Half Open                     0
Blacklist sessions                    0
Blacklist sessions Created            0
Blacklist sessions Freed              0
Conn SMP Alloc                        189
Conn SMP Free                         0
Conn SMP Aged                         0
Conn Type 0 Available                 801570816
Conn Type 1 Available                 402554826
Conn Type 2 Available                 200392704
Conn Type 3 Available                 100196352
Conn Type 4 Available                 50098176
```

```
Conn SMP Type 0 Available           801570816
Conn SMP Type 1 Available           400785408
Conn SMP Type 2 Available           200392704
Conn SMP Type 3 Available           100204354
Conn SMP Type 4 Available           50098176
Total Local Sessions                0
```

- To view the maximum capacity per PU, refresh the command every second. (Press ^C to quit)

```
TH7655S# show session
Processing-Unit 1
Traffic Type                        Total
---------------------------------------------
Total Sessions                      402542595
TCP Established                     0
TCP Half Open                       0
Server TCP Established              0
Server TCP Half Open                0
SCTP Established                    0
SCTP Half Open                      0
UDP                                 402542595
Non TCP/UDP IP sessions             0
Other                               0
Reverse NAT TCP                     0
Reverse NAT UDP                     0
Curr Free Conn                      8075
Conn Count                          402542595
Conn Freed                          0
TCP SYN Half Open                   0
Blacklist sessions                  0
Blacklist sessions Created          0
Blacklist sessions Freed            0
Conn SMP Alloc                      116
Conn SMP Free                       0
Conn SMP Aged                       0
Conn Type 0 Available               0
Conn Type 1 Available               0
```

```
Conn Type 2 Available                0
Conn Type 3 Available                0
Conn Type 4 Available                0
Conn SMP Type 0 Available            0
Conn SMP Type 1 Available            0
Conn SMP Type 2 Available            0
Conn SMP Type 3 Available            8075
Conn SMP Type 4 Available            0
Total Local Sessions                 0
```

- To view the memory usage information, use the **show memory** command.

```
TH7655S# show memory
          Total(KB)      Used          Free         Usage
-----------------------------------------------------------------
Memory:   191699152      68985250      122713902    35.90%
```

Monitoring and Managing System Directory Logs

Previously, there was no provision to view and remove unwanted logs present in the system directories (**a10log**/**syslog**/**varlog**). The **show file-system** and **file-system** commands are introduced to monitor and manage these logs in a better manner.

You can use the **show file-system** command to view the log file information for any of the system directories, and then use the **file-system rm** command to delete a particular log file.

CLI Configuration

- To view the log file information for the specified system directory:

```
ACOS(config)# show file-system [a10log | syslog | varlog]
```

- To delete a log file from the specified system directory:

```
ACOS(config)# file-system [a10log | syslog | varlog] rmfile_name
```

Example: The following command deletes *clear.log* present in **syslog** directory:

```
ACOS(config)# file-system syslog rmclear.log
```

Scaleout

ACOS 5.2.1-P7 introduces the following new feature and enhancement for Scaleout:

NOTE: For Scaleout specific configuration steps, refer *Scaleout Configuration Guide*.

The following topic is covered:

IPv6 Interface Support in L3 Mode

In the Scaleout configuration, the traffic redirection and session synchronization currently support IPv4 interfaces only. This release adds support for IPv6 interfaces in L3 mode.

Starting with ACOS 5.2.1-P7, the redirection of IPv6 traffic is through IPv6 VxLAN encapsulation.

The following features are available in this release:

- In L3 mode:
  - For IPv4 traffic, the redirection takes place over the IPv4 VxLAN tunnel.
  - For IPv6 traffic, the redirection takes place over the IPv6 VxLAN tunnel.

NOTE: Ensure IPv6 connectivity between the nodes.

- The `use-v4-vxlan` CLI, which is configured under `encap vxlan`, has been introduced under `traffic-redirection`. This command can be used to force all redirections to occur over IPv4 VxLAN tunnels during an upgrade from the older releases to 5.2.1-P7 and the later releases.
- The IPv4 interfaces handle the session synchronization by default. If the IPv4 interfaces are unavailable, then the session synchronization is handled by the IPv6 interfaces.

Known Limitation

IPv6 Link Local addresses are not supported for computing redirection or session synchronization.

For more information, see the *Scaleout Configuration Guide* and *Command Line Reference Guide*.

SSL Insight

ACOS 5.2.1-P7 introduces the following new feature and enhancement for SSL Insight (SSLi):

NOTE: For SSLi configuration steps, refer *SSL Insight Configuration Guide*. Similarly, for CLI commands, refer *Command Line Reference Guide*.

The following topic is covered:

Safe Elliptical Curves Support

ACOS now supports the modern and safe Elliptical Curves Cryptography (ECC) algorithm ‘secp521r1’ and ‘x25519’ for secured key exchange. ACOS will continue to support both the legacy (‘secp256r1’ and ‘secp384r1’) and safe ECC algorithms for SSL offloading and acceleration.

The safe ECC is supported for the following SSL modules and TLS versions:

- Intel QuickAssist Technology (QAT) SSL module with TLS 1.2 and TLS 1.3 security versions.
- Software TLS 1.3 SSL module with TLS 1.2 and 1.3 security versions.

You can configure all the EC name curves in the SSL templates and bind it to the virtual server port. The key exchange takes place based on the SSL modules and TLS versions negotiated between the client and server.

CLI Configuration

- To configure the new EC curve names in the SLB template client SSL, use the

following commands:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# ec-name secp521r1
ACOS(config-client ssl)# ec-name x25519
ACOS(config-client ssl)# version 34 33
```

- To configure the new EC curve names in the SLB template server SSL, use the following commands:

```
ACOS(config)# slb template server-ssl serverssl
ACOS(config-server ssl)# ec-name secp521r1
ACOS(config-server ssl)# ec-name x25519
ACOS(config-client ssl)# version 34 33
```

System Configuration and Administration

ACOS 5.2.1-P7 introduces the following new feature and enhancement for System Configuration and Administration:

NOTE: For more information and details, refer *System Configuration and Administration Guide*.

The following topic is covered:

Call Home

Call Home enables ACOS devices to send diagnostic information securely to the A10 Product Research end-point. This diagnostic information includes configuration and environmental data such as the ACOS device, its form factor, deployment location, number of interfaces, L3V partitions, VLANs, and more. It also collects information on the ACOS licenses activated on the device. All the information collected is used to improve the product quality.

Call Home is not enabled by default. You can manually enable Call Home on your ACOS devices. When enabled, the ACOS device pushes the collected diagnostic

information to the A10 end-point daily at midnight . You can choose to manually offset the call home time by 0 to 23 minutes after midnight, if needed.

The following conditions must be met for A10 Call Home to work:

- **Internet Connection** — The ACOS device must be able to reach the internet for Call Home to send diagnostic data to the A10 end-point. This feature does not work with proxy server configuration.
- **Port 443** — The Call Home data from your ACOS device is sent over TLS protocol using port 443 by default.

CLI Configuration

To enable Call Home, verify internet connectivity and configure the call-home profile on the ACOS device:

```
ACOS(config)# call-home profile
ACOS(config-profile)# register
```

The 'register' command enables the call-home service. Once enabled, the Call Home data is collected from the ACOS device every 24 hours at midnight. You can choose to manually offset the Call Home time by 0 to 23 minutes.

To offset the export time:

```
ACOS(config-profile)# time <0-23> mins
```

For example, if you configure the offset time as 5 mins, the data will be exported at 12:05 AM.

Import-Periodic Chassis Platform Support

When the `import-periodic` command is used on the chassis platform, Processing Unit 1 (PU1) and Processing Unit 2 (PU2) try to fetch files from the remote server. However, PU2 may encounter issues while fetching the files from the remote server if the management interface is not connected.

In this release, the imported files are automatically synced from PU1 to PU2, ensuring that PU2 can periodically and locally update the files. This also helps both PU1 and PU2 to import the same files.

The `import-periodic` command supports the following file types:

```
aflex                aFleX Script Source File
auth-jwks            JSON web key
auth-portal          Portal file for http authentication
bw-list              Black white list files
ca-cert              SSL CA Cert File(enter bulk when import an archive
file)
class-list           Class list files
class-list-convert   Convert Class List File to A10 format
dnssec-dnskey        DNSSEC DNSKEY(KSK) file for child zone
dnssec-ds            DNSSEC DS file for child zone
geo-location         Geo-location CSV File
local-uri-file       Local URI files for http response
policy               WAF policy File
rpz                  Response Policy Zone File
ssl-cert             SSL Cert File(enter bulk when import an archive file)
ssl-cert-key         Bulk file
ssl-crl              SSL Crl File
ssl-key              SSL Key File(enter bulk when import an archive file)
thales-kmdata        import Thales Kmdata files
thales-secworld      import Thales security world files
wsdl                 Web Services Definition Language File
xml-schema           XML-Schema File
```

The following is an example of the `import-periodic` command of the scp file type:

```
import-periodic ssl-crl ssl-crl-file use-mgmt-port
scp://root:password@10.64.44.106/root/dataFile/crl.dat period 300
```

NOTE: When the import-periodic task is removed, the task will be deleted from the PU2.

For more information about the `import-periodic` command, see the *Command Line Reference Guide*.

Security Updates

The following security vulnerabilities are addressed in the ACOS 5.2.1-P7 release:

- OpenSSL Vulnerabilities
  - CVE-2022-4450: A double-free vulnerability related to PEM_read_bio_ex() and SSL_CTX_use_serverinfo_file() functions.
  - CVE-2023-0286: A Type confusion vulnerability related to processing of X.400 address.
- Linux Kernel Vulnerability
  - CVE-2023-0394: A NULL pointer dereference vulnerability related to rawv6_push_pending_frames.

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 5.2.1-P6

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P6 release:

The following topics are covered:

Application Delivery Controller

ACOS 5.2.1 -P6 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for CLI commands, refer *Command Line Reference Guide*.

The following topics are covered:

ADC GUI Support Thunder 7650 and 7655

ACOS provides GUI support for ADC in the Thunder 7650 and 7655 devices. In addition, a new 'Chassis Application Type' option is introduced for configuring the 'ADC' or 'CGNv6' as the application type. Using GUI, you can manage Virtual Servers, Virtual Services, Service Groups, Applications, Health Monitoring, and many more.

The following are not supported on Thunder 7650 and 7655:

- 'SSL Cert Pinning' under **ADC > SSL Management**
- 'SSLi Certs' and 'Cert Revocation' under **ADC > Statistics > L7 > SSL**.
- 'SSL Forward Proxy' and 'SSLi Errors' counters under **ADC > Statistics > L7 > SSL > SSL Stats**

For more information, see GUI *Online Help*.

Known Limitation

- The GSLB, AAM, and Log main menus are unavailable on the Chassis GUI.

- The 'VRRP-A Status' icon on the Home page (top right corner) is hidden by default when more than one VRID is present. Since the VRIDs are always in pairs in the chassis, the 'VRRP-A Status' icon is unavailable on the Chassis GUI.

Scaled Wildcard VIPs Per Device

ACOS supports wildcard VIPs through Access Control Lists (ACLs) to filter client requests, thus preventing potential miscreants from causing damage to network resources located behind the wildcard VIP. Currently, the maximum number of wildcard VIPs is 200 per partition.

With this release, the maximum number of wildcard VIPs per device will vary based on the system memory size. Though the maximum wildcard VIP limit is 200 per partition, the IPv4 and IPv6 VIPs are calculated separately. For example, with 64 GB of memory, you can configure up to 1200 IPv4 VIP and 1200 IPv6 VIP.

For more information, see and .
Wildcard VIPs Limit on vThunder

Memory (GB RAM)	Maximum Wildcard VIP ACL
1 - 16	200
32	800
64	1200

Wildcard VIPs Limit on Hardware Platform

Memory (GB RAM)	Maximum Wildcard VIP
1 - 24	200
32	800
64 - 128	1200

Idle Timeout Support for HTTP Connections

ACOS supports the idle timeout feature for HTTP/1.1 and HTTP/2 client connections. This feature allows you to specify the maximum time an HTTP client connection can remain idle in the ACOS device. If no data is sent or received after the idle timeout period expires, the load balancer closes the connection. This prevents unused or stalled connections from consuming server resources indefinitely.

To enable this feature, a new command 'client-idle-timeout' is introduced under SLB Template HTTP.

CLI Configuration

```
ACOS(config)# slb template http http1
ACOS(config-http)# client-idle-timeout <seconds>
```

TTL Value Adjustment for Cached DNS Response

The existing DNS Cache feature is extended to support updated TTL values for cached DNS entries. When ACOS responds to DNS queries with a cached DNS response, it copies the same TTL value as the original cached content.

This release introduces the option to update the TTL value in the cached DNS response to reflect the real time TTL of the original cached content.

You can enable the TTL value adjustment on the global DNS cache, or apply per VIP using the SLB DNS Templates.

CLI Configuration

- The following CLI commands enable the TTL value adjustment on the global DNS cache:

```
ACOS(config)#slb common
ACOS(config-common)#dns-cache-ttl-adjustment-enable
```

- The following CLI commands enable the TTL value adjustment on DNS cache entries per VIP:

```
ACOS(config)#slb template dns test
ACOS(config-dns)#cache-ttl-adjustment-enable
```

These options are disabled by default.

Immediate Removal of Expired DNS Cache Entry

If the DNS TTL value for a particular domain expires, the entry for the expired domain is removed from the cache within 60 seconds.

With this release, if the DNS TTL value for a particular domain expires, the entry for the expired domain is immediately removed from the cache. This avoids displaying the expired DNS cache entries when the command `show dns cache entry` is run.

Carrier Grade NAT

ACOS 5.2.1-P6 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

NOTE: For CGN or CGNAT specific configuration steps, refer *IPv4-to-IPv6 Transition Solutions Guide*.

The following topics are covered:

Enhanced DNAT Action with Domain-name

From this release, ACOS supports Destination NAT based on domain name. A new DNAT action is provided in the lsn-rule-list which translates a particular destination IP address to an IP address which is resolved from a DNS domain.

If there are multiple IP entries which are resolved from the DNS domain, the DNAT IP address is chosen randomly based on hashing of source IP address and same DNAT IP address is used for all sessions of the client.

This feature allows the mobile-edge computing customer to deploy a ‘DNS-proxy’ in a DNS domain. The proxy sends a dns-response to mobile subscribers with preconfigured dns-records in order to redirect the traffic towards their Value-added Service (VAS) application servers. This traffic is then forwarded back to A10 CGNAT

for performing the DNAT action before reaching out to the application servers on Internet.

It has the following highlights:

- Increased maximum number of IP nodes or subnet nodes per lsn-rule-list from 1K to 3K.
- Both NAT44 and NAT64 translation support.
- DNAT and SNAT are supported natively.

CLI Configuration

```
ACOS(config)# cgnv6 lsn-rule-list 1
ACOS(config-lsn-rule-list)# ip ipv4addr/mask-length
ACOS(config-lsn-rule-list-ip)# tcp port port-num action dnat domain
domain-name
ACOS(config-lsn-rule-list-ip)# udp port port-num action dnat domain
domain-name
ACOS(config-lsn-rule-list-ip)# icmp action dnat domain domain-name
ACOS(config-lsn-rule-list-ip)# others action dnat domain domain-name
```

OR

```
ACOS(config)# cgnv6 lsn-rule-list 1
ACOS(config-lsn-rule-list)# ip ipv4addr/mask-length
ACOS(config-lsn-rule-list-ip)# default action dnat  domain domain-name
```

Known Limitation

The `dnat domain` action is supported only for IP nodes in lsn-rule-list and not for subnet nodes or hostname nodes.

Disabling Inbound Refresh for LSN Full-Cone Sessions

ACOS provides the option to refresh LSN full-cone sessions upon receiving inbound traffic. This default behavior prevents sessions from aging out for the Outbound (client to server) and Inbound (server to client) traffic. Although inbound refresh is useful for applications with no outgoing UDP traffic, it allows external attackers and misbehaving applications to keep the mapping alive indefinitely, causing a security risk.

The enhanced CGNAT now has the provision to disable the inbound refresh so that session age refresh for LSN full-cone sessions is disabled even while receiving inbound traffic. This allows the LSN full-cone sessions to age out and to be freed, thereby reducing the security risk.

NOTE: This feature is already supported for LSN and Fixed NAT sessions.

CLI Configuration

- To disable inbound refresh for LSN full-cone sessions, configure the following command at the partition level:

```
ACOS(config)# cgnv6 lsn inbound-refresh-full-cone disable
```

NOTE: These commands do not apply to outbound packets i.e., the sessions continue to refresh if outbound packets are sent.

- To view the session statistics, use the **`show cgnv6 lsn full-cone-sessions`** command. It is enhanced to display active and inactive LSN full-cone sessions.

Firewall

ACOS 5.2.1 -P6 introduces the following new feature and enhancement for Firewall:

NOTE: For Firewall specific configuration steps, refer *Firewall Configuration Guide*.

The following topics are covered:

Hierarchical Rate-Limiting Support

Bandwidth rate limiting enables multiple users to access the internet during periods of high demand for the throughput. However, currently, there is no mechanism to prevent the overconsumption of resources by certain users and allow fair distribution of bandwidth among all active users. To make bandwidth rate-limiting more flexible and manageable at several levels, hierarchical rate limiting is introduced.

With this advanced feature, you can apply one set of limits (specified by a child template limit-policy) to the traffic belonging to an individual subscriber while applying the second set of limits (specified by a parent template limit-policy) to the aggregated traffic of all the subscribers. This mechanism enables hassle-free traffic management at multiple levels that allows you to:

- Monitor resource utilization of all subscribers and rate-limit the hyperactive ones to ensure high-quality services for all/most of the currently active subscribers.
- Distribute resources in a **max-min-fair** manner so that the unutilized portion of a subscriber's fair-share can be distributed among other subscribers who are capable of utilizing more than their fair share.

CLI Configuration

The following tags are introduced in the **`template limit-policy`** to support hierarchical rate-limiting:

- To define a hierarchy among a set of template limit-policies, use the **`parent`** tag. This tag is used by a child template limit-policy to identify its parent template limit-policy.

  There is no limit on the number of hierarchies that can be present in a configuration. Each hierarchy may extend to any number of levels.

  NOTE: The ID of the parent template limit-policy must be lower than that of the child template. Else, the parent configuration from the child limit-policy might be lost when the device restarts.

- To distribute resources in a **max-min-fair** manner, configure the **`max-min-fair`** tag in the parent template limit-policy.

- To allow the child rate limit entry to consume more resources than the configured rate limit, use the **relaxed** tag.

The following configuration demonstrates the usage of these tags. Here, the **template limit-policy***10* is the parent, whereas the **template limit-policy** *20* is the child.

```
ACOS(config)# template limit-policy 10
ACOS(config-limit-policy)# limit-throughput downlink 10240
ACOS(config-limit-policy)# limit-scope aggregate
ACOS(config-limit-policy)# max-min-fair

ACOS(config-limit)# template limit-policy 20
ACOS(config-limit-policy)# limit-scope subscriber-prefix 64
ACOS(config-limit-policy)# parent 10
ACOS(config-limit-policy)# limit-throughput downlink 10 relaxed
```

Additionally, the **show fw rate-limit** command is enhanced to view the rate limit entries created from a given template limit policy.

NOTE:

- Hierarchical rate-limiting functionality is only supported by Traffic Control rules. It is not possible to invoke this functionality using the Access Control rules.
- Template limit-policies in a hierarchy may have any scope: subscriber IP, subscriber prefix, or aggregate, as long as a parent template's scope is NOT more specific than that of any of its children templates.

Known Limitations

Hierarchical rate limiting has the following limitations:

- It is not supported for:
  - Scaleout clusters
  - Deployment on multi-PU platforms
- It does not support Packet-per-second rate-limiting.
- It does not work as expected for lightweight 4 over 6, MAP-E, and GTP tunnels.

- A **limit-concurrent-sessions** configuration in a parent template limit-policy is not inherited by the children template limit-policies.
- A **limit-scope subscriber-ip** configuration in the parent template limit-policy is not supported for IPv6.

Enhanced DDoS Protection with Blacklisting

When the platform intercepts a volumetric DDoS attack, a lot of traffic hits the deny rules, and packets are dropped based on the per-packet rule lookup. However, due to the high amount of traffic, the overhead of the per-packet rule lookup can cause CPU usage to spike. To drop these packets more efficiently i.e., with minimum processing, the **fw ddos-protection dynamic-blacklist** command is introduced at the partition level. When this command is enabled, a blacklist session is created dynamically when a particular firewall deny rule is matched. Subsequent traffic that matches the blacklist session is dropped.

Blacklist session creation is triggered only when the CPU usage exceeds the pre-configured threshold limit.

CLI Configuration

- To enable this feature, configure **fw ddos-protection dynamic-blacklist** command:

```
ACOS(config)# fw ddos-protection dynamic-blacklist [ enable | disable ] [ inbound | outbound | both ] [timeout seconds ]
```

- To view the number of blacklist sessions created and freed, use any of the following show commands:
  - **show session**
  - **show session brief**
  - **show counters fw global**
  - **show counters system session**

Known Limitations

- This feature is less effective if the attack traffic continuously changes the IP addresses.

- If application classification is enabled, the blacklist session is created only after the application is classified. Prior to that, a regular firewall session is created that allows packets to flow through. After classification, when a deny rule is matched, the firewall session is replaced with a blacklist session.
- The creation and deletion of the blacklist sessions is not logged. Moreover, if the logging option is specified in the rule, it is ignored when this feature is active.

Multiple Rule-Set Support

The firewall rule-sets allow you to configure certain actions based on the traffic matched. Earlier, the firewall supported only one rule-set type that was shared by several firewall applications such as security control, NAT, traffic control, and DDoS. However, managing the rule-set became challenging when different applications tried to classify the traffic in different ways.

The firewall is now enhanced to support multiple rule-set types so that you can configure different rule-sets for different firewall applications, thereby providing better flexibility and improved usability.

Based on the actions performed, the following two rule-set types are supported:

- Access Control rule-set

  This rule-set allows access control i.e., permits or denies packets. It also enables logging, decides how the traffic is forwarded, and includes packet rewrite functions like NAT. To ensure backward compatibility, the existing firewall rule-set is now referred to as the Access Control rule-set.

- Traffic Control rule-set

  This new rule-set applies bandwidth control to the network traffic by using rate limiting policies. It is introduced to implement advanced features such as hierarchical rate-limiting. Although the Access Control rule-set supports basic rate-limiting, you are recommended to configure this rule-set for improved performance.

NOTE: The Traffic Control rule-set is not a standalone rule-set; the Access Control rule-set must be configured along with it for the firewall policies to function as expected.

CLI Configuration

- For Access Control rule-set

  Use the existing **rule-set** command to create this rule-set and the **fw active-rule-set** command to activate it. No new commands are introduced for this rule-set.

- For Traffic Control rule-set
  - To create the rule-set:

    ```
    ACOS(config)# traffic-control rule-settcrs1
    ACOS(config-rule set:tcrs1)# rulerule1
    ```

  - To activate the rule-set:

    ```
    ACOS(config)# traffic-control active-rule-settcrs1
    ```

  - To view the rule-set statistics:

    ```
    ACOS(config)# show traffic-control rule-settcrs1
    ```

Rule-Specific Logging Templates

The logging templates are defined globally and enabled at the rule level using the `action permit log` or `action group permit log` commands. As logging templates are bound globally for all rules, you cannot use specific log template for the traffic matched by the certain rule.

The improved logging mechanism allows you to configure the following logging templates in a rule:

- Firewall Logging - `permit log fw-logging-template <template name>`
- CGNv6 Logging - `permit log cgnv6-logging-template <template name>`
- NetFlow Monitor - `permit log netflow-monitor <monitor name>`

The template configured under a rule is bound locally to the rule. This selective rule-level application of a template allows using unique logging type and format for certain subscriber traffic. Selective logging ensures visibility and flexibility for a subset of subscribers of interest or selected traffic type and reduces the load at the platform by eliminating redundant logging data.

CLI Configuration

In the following example, `permit log fw-logging-template fw_logging`, `permit log cgnv6-logging-template lsn_log`, `permit log netflow-monitor netflow_monitor1` commands configure the Firewall, CGNv6, Netflow Monitor templates in a rule, respectively.

These new commands work in addition to `permit log` and `permit cgnv6` commands. So, you must use these existing commands to enable logging and then use the new commands to configure the logging templates.

For a netflow monitor to work selectively for a rule, you must configure the scope in the netflow monitor template. Use `scope firewall-rule` command as shown in the example to define the scope of the template. The default scope is global.

```
ACOS(config)#fw logging fw_logging
ACOS(config)# netflow monitor netflow_monitor1
ACOS(config-netflow-monitor)# scope firewall-rule
ACOS(config-netflow-monitor)# record sesn-event-fw4 both
ACOS(config)# rule-set test
ACOS(config-rule set:test)# rule 3
ACOS(config-rule set:test-rule:3)# source ipv4-address 3.3.3.89/32
ACOS(config-rule set:test-rule:3)# source zone any
ACOS(config-rule set:test-rule:3)# dest ipv4-address 15.15.15.90/32
ACOS(config-rule set:test-rule:3)# dest zone any
ACOS(config-rule set:test-rule:3)# service proto-id 47
ACOS(config-rule set:test-rule:3)# action-group
ACOS(config-rule set:test-rule:3-acti...)# permit log
ACOS(config-rule set:test-rule:3-acti...)# permit log fw-logging-
template fw_logging
ACOS(config-rule set:test-rule:3-acti...)# permit cgnv6
ACOS(config-rule set:test-rule:3-acti...)# permit log cgnv6-logging-
template lsn_log
ACOS(config-rule set:test-rule:3-acti...)# permit log netflow-monitor
netflow_monitor1
```

Known Limitation

If you change the template after the session is created, the creation and deletion events might get logged on to different servers.

Disabling Inbound Refresh for Firewall Full-Cone Sessions

ACOS provides the option to refresh the session age for full-cone sessions when the new data sessions are created upon receiving the inbound TCP SYN or UDP packets. This default behavior prevents sessions from aging out for the Outbound (client to server) and Inbound (server to client) traffic. However, it allows external attackers and misbehaving applications to keep the mapping alive indefinitely, causing a security risk.

The enhanced firewall now has the provision to disable the session refresh upon receiving inbound packets. This allows the full-cone and data sessions to age out and to be freed, thereby reducing the security risk.

CLI Configuration

- To disable inbound refresh, configure the following commands at the partition level:
  - For firewall full-cone sessions

    ```
    ACOS(config)# fw inbound-refresh-full-cone disable
    ```

  - For firewall data sessions

    ```
    ACOS(config)# fw inbound-refresh disable
    ```

NOTE: These commands do not apply to outbound packets i.e., the sessions continue to refresh if outbound packets are sent.

- To view the session statistics, use the **`show fw full-cone-sessions`** command. It is enhanced to display active and inactive full-cone sessions.

New Periodic Session Log and Drop Log Information

A new **`session-periodic-log interval`** command is introduced. While configuring logging templates, you can set session periodic log interval in minutes. The interval indicates how frequently a log is sent and stored on the server. Periodic session logging is disabled by default.

In addition, for matched permitted sessions, all firewall logs will now have the following drop log information:

- Forward drop bytes
- Forward drop packets
- Reverse drop bytes
- Reverse drop packets

Drop log in this context refers to packets dropped because of rate-limiting configurations.

NOTE: The drop attributes are logged only when the session-statistic is enabled for a rule-set.

CLI Configuration

In the following example, **session-periodic-log interval** of 2 minutes is configured for fw_logging template. The **session-statistic** must be enabled for a rule set for periodical session logging to work.

```
ACOS(config)# fw template logging fw_loggging
ACOS(config-logging)# service-group sg1
ACOS(config-logging)# session-periodic-log interval 2
ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# session-statistic enable
```

MIB

ACOS 5.2.1-P6 introduces the following new feature and enhancement for MIB:

NOTE: For more information about supported MIB object details, refer *MIB Guide*.

The following topic is covered:

SNMP Support for Vendor, Model, and Operating System Version

In this release, the following new object-ID (OID) is introduced to collect information about Vendor, Model, and Operating System version via SNMP:

- axSysVendorModelVersion (1.3.6.1.4.1.22610.2.4.1.6.5)

Network Configuration

ACOS 5.2.1-P6 introduces the following new feature and enhancement for the Network Configuration.

NOTE: For configuration and CLI commands, refer *Network Configuration Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topic is covered:

Support for Advertising IPv4 Routes Using Global IPv6 Next Hop

ACOS supports advertising IPv4 routes over an IPv6 BGP connection using Global IPv6 next hops.

Platforms

ACOS 5.2.1-P6 introduces the following new feature and enhancement for ACOS Platforms:

The following topic is covered:

PCAP Next Generation (PCAPNG) Support in axDebug

In the prior releases, the ACOS debugging (axDebug) utility supported capturing packets in the PCAP file format, which is widely understood by third-party diagnostic applications such as Wireshark (formerly Ethereal) or tcpdump.

With this release, ACOS supports capturing packets in the PCAP Next Generation (PCAPNG) file format to enhance debugging capabilities. Wireshark fully supports the PCAPNG file format, whereas libpcap has partial support for the PCAPNG file format.

For more information on PCAPNG, see https://datatracker.ietf.org/doc/html/draft-tuexen-opsawg-pcapng.

Each PCAPNG file has numerous data blocks containing various types of information. In this release, the following block types are supported:

- Section Header Block (SHB) – Includes a list of blocks such as interfaces and packets that are logically correlated.
- Interface Description Block (IDB) – Contains information describing an interface on which the packet data is captured.
- Enhanced Packet Block (EPB) – Stores the packets coming from the network.
- Decryption Secrets Block (DSB) – Stores session secrets (including pre-master secret key of SSL session) that enable decryption of packets within the capture file.

Under axDebug, a new option called **`pcapng-config`** is added for configuring the PCAPNG file format using CLI and GUI.

For more information, see the *Command Line Reference Guide*.

CLI Configuration

- To enable PCAPNG , use the following commands:

```
ACOS# axdebug
ACOS(axdebug)# pcapng-config
ACOS(axdebug-pcapng)# pcapng-enable
```

- To enable SSL key tracking, use the following commands:

```
ACOS# axdebug
ACOS(axdebug)# pcapng-config
```

```
ACOS(axdebug-pcapng)# pcapng-enable
ACOS(axdebug-pcapng)# ssl-key-enable
```

Show Commands

To view the packet capture information, refer to the following show commands:

- **show axdebug file**
- **show axdebug config-file**
- **show axdebug pcapng**
- **show axdebug status**

GUI Configuration

To enable or disable PCAPNG and SSL Key tracking, go to **System** > **Diagnostics** > **PCAPNG Config**.

For more information, see *Online Help*.

Known Limitations

- The names of the packet capture files must be unique.
- When using the **ssl-key-enable** under **pcapng-config**, the Wireshark version 3.6.5 (or prior versions) will not show the server certificate key. As a workaround, you must change the following settings in the capture file:
  - For HTTPv1/HTTPv2:

    Under Analyze Option: Decode As- +TCP port 443 and select HTTP
  - For HTTPv3:

    Under Analyze Option: Decode As - +UDP port 443 and select HTTP

CPU Packet Prioritization

With this release, the Thunder for Bare Metal and ESXi support the CPU packet prioritization feature. The feature uses the NVIDIA Mellanox ConnectX-6 and NVIDIA Mellanox ConnectX-5 cards hardware programmable flow rules to classify and prioritize control packets, such as BFD, BGPv4, BGPv6, OSPFv2, OSPFv3, RIP, RIPng, LACP, STP, VCS, Scaleout, and VRRP packets over the data packets.

To enable the control packet prioritization, run the following command:

```
ACOS(config)# system cpu-packet-prio-support enable
```

Scaleout

ACOS 5.2.1-P6 introduces the following new feature and enhancement for Scaleout:

NOTE: For Scaleout specific configuration steps, refer *Scaleout Configuration Guide*.

The following topic is covered:

IPv6 Interface Support for Scaleout

In the Scaleout configuration, the traffic redirection and session synchronization currently support IPv6 interfaces, in addition to the previously supported IPv4 interfaces.

Consider the following points:

- For IPv4 traffic, the redirection takes place over the IPv4 interfaces. If the IPv4 interfaces are unavailable and the IPv6 interfaces are available, then the traffic will be redirected using the IPv6 interfaces.
- For IPv6 traffic, the redirection takes place over the IPv6 interfaces. If the IPv6 interfaces are unavailable and the IPv4 interfaces are available, then the traffic will be redirected using the IPv4 interfaces.
- The IPv4 interfaces handle session synchronization by default. If the IPv4 interfaces are unavailable, then the session synchronization is handled by the IPv6 interfaces.

Known Limitation

IPv6 Link Local addresses are not supported for computing redirection or session synchronization.

For more information, see the *Scaleout Configuration Guide* and *Command Line Reference Guide*.

Security Updates

The following security vulnerabilities are addressed in the ACOS 5.2.1-P6 release:

- Strong Swan Vulnerabilities
  - CVE-2021-45079
  - CVE-2021-41991
- Expat Vulnerabilities
  - CVE-2022-22822
  - CVE-2022-22823
  - CVE-2022-22824
- HTTPD Vulnerability
  - CVE-2022-22720

For detailed information about security updates, see A10 Networks Security Advisories.

Enhancements in ACOS 5.2.1-P5

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P5 release:

The following topics are covered:

Application Delivery Controller

ACOS 5.2.1 -P5 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for CLI commands, refer *Command Line Reference Guide*.

The following topics are covered:

HTTP/1.1 to HTTP/2 Communication Support

ACOS supports communication between HTTP/1.1 to HTTP/2 when only HTTP/2 is configured on the server side, and the incoming traffic on the client side is HTTP/1.1. This capability is useful when you wish to have separate policies on the client side and the server side.

The following new CLI commands are introduced to enable this feature:

- `support-http2 only` under SLB real port
- `server-support-http2-only auto-detect` under SLB template HTTP
- `server-support-http2-only force` under SLB template HTTP

Known Limitation

This feature is not supported for SSLi virtual port.

CLI Configuration

To enable `support-http2 only` option under the SLB real port:

```
ACOS(config)# slb server s1 10.20.20.20
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# support-http2 only
```

To enable `server-support-http2-only` option under the SLB template HTTP:

```
ACOS(config)# slb template http http-2
ACOS(config-client ssl)# server-support-http2-only {auto-detect | force}
```

HTTP Request Smuggling Enhancement

The existing HTTP request compliance feature is enhanced to configure HTTP header filter rules. You can specify the header-name to be detected and enable the 'drop' action when the header-name matches the filter rules. The HTTP headers are filtered using full-text or regular expressions (regex).

A new `header-filter-rule` option is introduced for the `http-protocol-check` CLI command under SLB HTTP template. The following options are also provided to set the matching filters:

- `match-type` - supports full-text and PCER regular expressions
- `action` - supports drop action only
- `header-name` - supports regular expression
- `header-value` - supports regular expression

CLI Configuration

```
ACOS(config)# slb template http abc
ACOS(config-http)# http-protocol-check
ACOS(config-http-http-protocol-check)# header-filter-rule
ACOS(config-http-http-protocol-check-head...)# match-type full-text
ACOS(config-http-http-protocol-check-head...)# action drop
ACOS(config-http-http-protocol-check-head...)# header-name content-
encoding
ACOS(config-http-http-protocol-check-head...)# header-value chunked
```

SIP Health Monitoring Enhancement

ACOS provides additional support to the SIP health monitoring feature that sends the SIP hostname in the request URI instead of the IP address. This functionality is beneficial in the environments where the integrated health monitor SIP or SBC server requires a SIP hostname rather than an IP address. You can also configure the customized header content, which will append the SIP health check request header after the original header. The existing headers are not overwritten.

To enable this feature, the following CLI options are introduced under the `health monitor` command:

- `hostname` - Sends the SIP request with the hostname that is used in the request header.
- `header-insert` - Customizes or configures the header content with the *name:value* pair.

NOTE: The header insertion feature is supported only for SIP methods such as SIP over UDP and SIP over TCP/TLS.

CLI Configuration

```
ACOS(config)#health monitor sip_monitor
ACOS(config-health:monitor)# method sip hostname a10networks.com
ACOS(config-health:monitor)# header-insert Expires:1800
ACOS(config-health:monitor)# header-insert Reply-
To:Bob<sip:bob@biloxi.com>
ACOS(config-health:monitor)# exit
```

PBSLB Timeout Support for Better Performance

ACOS now supports the age timeout configuration for global Policy-based SLB (PBSLB) entries, which was previously set to 6 minutes by default. This feature is advantageous when the CPU usage is high due to large amount of PBSLB entries. Therefore, lower the age timeout value, better is the CPU performance.

To configure this feature, the `pbslb-entry-age` CLI command is introduced under SLB common configuration.

CLI Configuration

```
ACOS(config)# slb common
ACOS(config-common)# pbslb-entry-age 4
```

Configuring Global DNS Cache Weight

ACOS supports DNS cache weight only for the VIP DNS cache table. The option is available under glid with reference to the classlist.

With this release, the weight for global DNS cache entry can also be set. The specified weight deletes the entries as mentioned below:

- If the cache is more than 60% full, entries with weight 1 are eligible to be deleted.
- If the cache is more than 70% full, entries with weight 1-2 are eligible to be deleted.
- If the cache is more than 80% full, entries with weights 1-4 are eligible to be deleted.
- If the cache is more than 90% full, entries with weights 1-6 are eligible to be deleted.

NOTE: The setting applies to the global DNS cache table.

CLI Configuration

The command `dns-cache-aging-weight <num>` is introduced to set the weight for global DNS cache entry. `<num>` can be replaced with a value between 1 to 7. For example,

```
ACOS(config)#slb common
ACOS(config-common)#dns-cache-enable
ACOS(config-common)#dns-cache-aging-weight 3
```

Configuring Global DNS Cache Capacity on a vThunder

The maximum number of DNS cache entries for vThunder was 65536 irrespective of the memory allocated to it.

With this release, the maximum limit for DNS cache entry size changes dynamically

with the RAM size allocated to the vThunder. The maximum limit as per the RAM size is mentioned below:

- If RAM is less than or equal to 4G, the maximum number of entries that can be specified is 65535.
- If RAM is 4G to 16G, the maximum number of entries that can be specified is 512000.
- If RAM is 16G to 128G, the maximum number of entries that can be specified is 2097152.

CLI Configuration

The maximum limit for the command `dns-cache-size <num>` is updated, and `<num>` can be replaced with a value between 0 to 2097152, depending on the RAM size allocated to the vThunder. For example,

With 8G RAM,

```
vThunder(config)#slb template dns test
vThunder(config-dns)#max-cache-size ?
<0-512000>  Maximum cache entry per VIP
```

With 32G RAM,

```
vThunder(config)#slb template dns test
vThunder(config-dns)#max-cache-size ?
<0-2097152>  Maximum cache entry per VIP
```

Connections Per Second (CPS) and Sessions Thresholds

With this release, a new CPS and Sessions Threshold configuration is added. When the CPS or number of sessions exceed the configured threshold, a Syslog and an SNMP trap are generated.

There are new CLIs added to set the threshold for the CPS and the number of sessions, and also to enable the respective traps in the SNMP MIB.

CLI Configuration

```
ACOS(config)# system apps-global cps-threshold num
ACOS(config)# system apps-global sessions-threshold num
ACOS(config)# snmp-server enable traps system apps-global cps-threshold
```

```
ACOS(config)# snmp-server enable traps system apps-global sessions-
threshold
```

aFlex

ACOS 5.2.1-P5 introduces the following new features and enhancements for aFlex.

NOTE: For more information, refer *aFleX Scripting Language Reference*.

The following topics are covered:

IP Stats Enhancement

With this release, the maximum byte counter size for 'IP::stats bytes [in | out] aFlex command' is increased from 22-bit to 48-bit for both IPv4 and IPv6 address families. This feature is added to provide accurate byte count when the traffic size increases (more than 4MB).

Known Limitation

This support is available for full-proxy connection only.

Log Limit Enhancement

The existing upper limit of the log message length per line for the ACOS log events' output is increased from 1024 bytes to 8000 bytes. The generated log message is sent to remote Syslog server instead of local buffer.

A new command `acos-events log-properties enable-8K-tcp-syslog` is added to enable 8K size remote TCP syslog. If this option is enabled, the existing proxy output of about 8000 bytes is displayed completely which increases the memory utilization.

Known Limitations

- This feature supports Syslog sent via TCP in ACOS event logging infrastructure

only.

- When large size logs are sent, the performance may decrease with an increase in the memory usage.

CLI Configuration

```
ACOS(config)# acos-events log-properties enable-8K-tcp-syslog
```

FIPS 140-2 Level 2 Enhancements

ACOS 5.2.1-P5 introduces the following new feature, capabilities, and enhancements for the FIPS.

The following topic is covered:

Support for FIPS Mode with Fourth Generation SSL Modules

This release supports FIPS 140-2 for Security Level 2 on A10 Thunder platforms with fourth generation SSL modules and related ACOS capabilities to comply with FIPS Level 2.

For more information about FIPS Level 2 support, refer to the *System Configuration and Administration Guide*.

Firewall

ACOS 5.2.1 -P5 introduces the following new feature and enhancement for Firewall:

NOTE: For Firewall specific configuration steps, refer *Firewall Configuration Guide*.

The following topics are covered:

Enhanced Firewall Logging

Currently, when the Firewall is configured, some logs having undetermined rules are generated in the Syslog (cs2 field for CEF format and RULE field for ASCII format). To reduce excessive logging and improve Syslog readability, you can disable the undetermined rule logs that are sent to the Syslog server.

CLI Configuration

To enable this feature, the **`fw disable-undetermined-rule-logs`** command is introduced at the partition level.

```
ACOS(config)# fw disable-undetermined-rule-logs
```

NOTE: This command does not affect the Firewall logs sent to the Harmony Controller and IPFIX collectors.

Additionally, to view the number of logs with undetermined rules, the **`Undetermined rule detected counter`** is introduced in the **`show counters fw global`** command.

Enhanced Show Firewall Rate Limit Command

Earlier, the **`show fw rate-limit`** command displayed only the configured rate limits. The command is now enhanced to additionally display the actual values of traffic received for the following rate-limit entries:

- Connections Per Second (CPS)
- Packets Per Second (PPS)
- Throughput

CLI Configuration

```
ACOS(config)# show fw rate-limit
IP Address       Prefix   Rule    Type   CPS-Received     CPS-Limit
Uplink-Received   Uplink-Limit   Downlink-Received   Downlink-Limit
Total-Received    Total-Limit    Cumulative Dropped Packets
```

```
------------------------------------------------------------------------
------------------------------------------------------------------------
------
```

```
47.27.10.10       32         1       PPS       0                0
0                  0              0                    100
   0                   0              424
Total Rate Limit Entries Shown:1
```

Processing Traffic without Matching Session

The firewall processes and forwards TCP SYN packets by creating a data session. Normally, the firewall drops packets that don't belong to any matched session. However, in certain cases when sessions are created before the firewall becomes active or during reconfiguration/reconnection, legitimate traffic could get dropped unnecessarily. For example, while recovering from a failover or while returning from a bypass, initial packets of the session might be dropped.

The **`fw allow-non-session-create`** command enables preserving the traffic unmatched to any session by creating a session **on the fly**. The command is introduced at the partition level to allow accepting and inspecting non-SYN TCP packets (except FIN and RST).

The command supports IPv4 and IPv6 traffic.

NOTE: Since DNS uses port 53 as a default port for transmitting DNS queries, the non-SYN TCP packets are dropped even if the **`fw allow-non-session-create`** command is enabled. To transmit non-SYN TCP packets from port 53, you need to disable the default port by executing the command **`fw alg dns default-port-disable`**.

CLI Configuration

- To forward non-SYN TCP packets, configure the following command:

```
ACOS(config)# fw allow-non-syn-session-create
```

- The **`Non-SYN pkt forward allowed`** counter is incremented each time a non-SYN packet is forwarded by the firewall. To view this counter, use the following command:

```
ACOS(config)# show counters fw global
```

Known Limitations

- You cannot configure this command when **fw tcp syn-cookie** is enabled.
- Rule actions for CGN and IPsec are not supported.
- If the rule matching criteria includes application/category evaluation, the classification result may not be available if the beginning of the session is missed. The packet will be considered as not matched and the configured policy action will be applied.

MIB

ACOS 5.2.1-P5 introduces the following new features and enhancements forMIB:

NOTE: For more information about supported MIB object details, refer *MIB Guide*.

The following topic is covered:

SNMP Traps for BGP Routing

With this release, SNMP traps are enhanced to support both IPv4 and IPv6 address families for BGP routing using the new proprietary AX-BGP-MIB.

CLI Configuration

```
ACOS(config)# snmp-server enable traps routing bgp ax
bgpEstablishedNotification
ACOS(config)# snmp-server enable traps routing bgp ax
bgpBackwardTransNotification
ACOS(config)# snmp-server enable traps routing bgp ax
bgpPrefixThresholdExceededNotification
ACOS(config)# snmp-server enable traps routing bgp ax
bgpPrefixThresholdClearNotification
```

Platforms

ACOS 5.2.1-P5 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

CPU Packet Prioritization

With this release, the Thunder for Bare Metal supports the CPU packet prioritization feature. The feature uses the NVIDIA Mellanox ConnectX-5 card hardware programmable flow rules to classify and prioritize control packets, such as BGP, LACP, and OSPF packets over the data packets.

To enable the control packet prioritization, run the following command:

```
ACOS(config)# system cpu-packet-prio-support enable
```

Intel Ethernet Network Adapter E810 Support

With this release, both the Thunders for Bare Metal and ESXi support Intel Ethernet Network Adapter E810.

Scaleout

ACOS 5.2.1-P5 introduces the following new feature and enhancement for Scaleout:

NOTE: For Scaleout specific configuration steps, refer *Scaleout Configuration Guide*.

The following topic is covered:

Distributed Forwarding

ACOS provides an ability to reduce the number of packet redirections in the Firewall Scaleout deployments and improve the packet handling performance by creating the shadow sessions. After a shadow session creation, the corresponding traffic can be processed by the node where the traffic flows based on the protocol (UDP or TCP) in the uplink or downlink or both directions (by default).

CLI Configuration

To enable the Scaleout distributed-forwarding for the Firewall:

```
ACOS(config)# scaleout distributed-forwarding fw enable
```

To disable the Scaleout distributed-forwarding for the Firewall:

```
ACOS(config)# scaleout distributed-forwarding fw disable
```

To configure the session offload in the uplink direction:

```
ACOS(config)# scaleout distributed-forwarding fw session-offload-
direction uplink
```

To configure the session offload in the downlink direction:

```
ACOS(config)# scaleout distributed-forwarding fw session-offload-
direction downlink
```

To configure the session offload in both the directions:

```
ACOS(config)# scaleout distributed-forwarding fw session-offload-
direction both
```

To configure the packet threshold value to offload the udp or tcp sessions:

```
ACOS(config)# scaleout distributed-forwarding fw threshold  <4-63> <udp
| tcp>
```

To disable the packet threshold value to offload the udp or tcp sessions:

```
ACOS(config)# no scaleout distributed-forwarding fw threshold <4-63>
<udp | tcp>
```

The following configuration example enables the scaleout distributed forwarding for the Firewall with the session offload in the uplink direction and the threshold value set to 6.

```
ACOS(config)# scaleout distributed-forwarding fw enable
ACOS(config)# scaleout distributed-forwarding fw session-offload-
direction uplink
ACOS(config)# scaleout distributed-forwarding fw threshold 6
```

Known Limitations

Consider the following limitations:

- Distributed Forwarding is applicable for both TCP and UDP sessions and does not apply to IP-in-IP, ICMP, SCTP, GTP, or UDP-DNS protocols.
- In the L3 Scaleout mode, the Distributed Forwarding does not support fragmented packets (for both Outer IP and Inner IP).
- TCP Window Check (currently enabled by default) is not supported along with Distributed Forwarding.
- Firewall Rate Limiting is not supported with Distributed Forwarding.

Secure Sockets Layer Insight

ACOS 5.2.1-P5 introduces the following new features and enhancements for Secure Sockets Layer Insight (SSLi):

NOTE: For SSLi configuration steps, refer *SSL Insight Configuration Guide*. Similarly, for CLI commands, refer *Command Line Reference Guide*.

The following topic is covered:

External Account Binding Support in ACME Protocol

ACOS currently works with Let's Encrypt to support the Automatic Certificate Management Environment (ACME) protocol for CA certificate management in SSLi. This functionality is enhanced to support External Account Binding (EAB), which allows an ACME account to be linked to an existing account in a non-ACME system, such as a CA customer database.

To enable this feature, you must configure the EAB credentials (EAB key ID and HMAC key) under `pki acme-cert` configuration.

CLI Configuration

```
ACOS(config)# pki acme-cert test
ACOS(config-acme cert:test)# eab-hmac-key {name | encrypted name}
ACOS(config-acme cert:test)# eab-key-id name
```

GUI Configuration

To enable EAB feature, go to **ADC > SSL Management > ACME Certificates** and configure the following options:

- EAB HMAC Key
- EAB Key ID

Enhancements in ACOS 5.2.1-P4

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P4 release:

The following topics are covered:

Application Access Management

ACOS 5.2.1 -P4 introduces the following new feature and enhancement for Application Access Management (AAM):

NOTE: For AAM specific configuration steps, refer *Application Access Management Guide*.

The following topic is covered:

Kerberos Key Distribution Centre (KDC) Service Ticket Validation

Prior to the ACOS 5.2.1-P4 release, only the authentication service exchange phase was supported. The security issues such as an attacker returning a fake TGT (Ticket Granting Ticket) and bypassing the Kerberos authentication were identified.

Starting from this release, the KDC service ticket validation feature is enhanced to validate the KDC with a specified account and password to prevent an attack.

NOTE: The KDC validation for KRB5 on Linux is not supported as the encryption type used by ACOS is not supported on KRB5.

The following CLI command is introduced in AAM Windows Kerberos Server profile:

```
auth-protocol kerberos-validate-kdc spn <spn> account <account> password <pwd>
```

CLI Configuration

```
ACOS(config)# aam authentication server windows krb2
ACOS(config-windows auth server:krb2)#host <Kerberos_ip_address>
ACOS(config-windows auth server:krb2)#auth-protocol ntlm-disable
ACOS(config-windows auth server:krb2)#auth-protocol kerberos-validate-kdc spn <spn> account <account> password <pwd>
ACOS(config-windows auth server:krb2)#realm <Kerberos_realm>
```

GUI Configuration

To configure KDC Service Validation, go to **AAM > Auth Servers > Windows**.

The following new fields are added to configure the KDC service validation:

- KDC Validation
- SPN for KDC Validation
- Account for KDC Validation
- Password

Application Delivery Controller

ACOS 5.2.1 -P4 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for ADC specific CLI commands, refer *Command Line Reference for ADC Guide*.

The following topics are covered:

Defend against HTTP Request Smuggling

ACOS provides HTTP request compliance check capabilities to defend from HTTP/1 and HTTP/2 smuggling attacks. HTTP request smuggling exploits differences in how the front-end servers (proxies) and back-end servers execute requests from multiple senders.

You can configure HTTP protocol compliance checks or conditions and enable 'drop' action when the conditions are met. For example, ACOS will send a 400 response to the client-side before dropping the request.

The following CLI commands are introduced in the SLB HTTP template under 'http-protocol-check':

- get-and-payload
- h2up-content-length-alias
- h2up-with-host-and-auth
- h2up-with-transfer-encoding
- malformed-h2up-header-value
- malformed-h2up-scheme-value
- multiple-content-length
- multiple-transfer-encoding
- transfer-encoding-and-content-length

CLI Configuration

```
ACOS(config)# slb template http abc
ACOS(config-http)# http-protocol-check
ACOS(config-http-http-protocol-check)# h2up-content-length-alias drop
ACOS(config-http-http-protocol-check)# malformed-h2up-header-value drop
```

Enhanced TCP Acknowledgment

ACOS now supports a naked ACK feature for piggybacking protocol in TCP. When this feature is set, the TCP handshake will first complete with a naked ACK (or ‘pure’ ACK) packet before any data gets sent.

This is useful when you need an option to disable piggybacking on the last ACK especially in case of SSLi or Explicit proxy environments. However, most modern server implementations do not require naked ACK as it increases the traffic overhead for transmitting extra packets.

A new ‘naked-ack-on-handshake’ command is introduced in the SLB TCP Proxy template.

CLI Configuration

```
ACOS(config)# slb template tcp-proxy default
ACOS(config-tcp proxy)# naked-ack-on-handshake
```

HTTP Syslog Enhancement

The existing ACOS Syslog for HTTP is enhanced to include Layer 3-4 information for better logging and troubleshooting. This information includes Source IP, Source Port, Destination IP, Destination Port, Virtual Server IP, and Virtual Port.

The Layer 3-4 information is added to the following HTTP Syslog messages:

- header_count
- header_detail
- header_invalid
- header_too_long
- http_line_too_long
- http_request_log
- http_resp_not_beg_hdr
- log_line
- too_many_headers
- too_many_response_header

Known Limitation

The logging infrastructure works for a string length which is less than 1024 bytes.

Caching NS Delegations and A/AAAA Records from Glue Records

In ACOS, when a query is received for a virtual server port configured with recursive resolution, by default it is forwarded to the root DNS servers. If the root DNS server does not have the final answer, it responds with a NS (nameserver) delegation (referral) response. ACOS then initiates a query to the server that is pointed to in the referral response. This process is repeated until the final response is fetched and

delivered to the client. If the **dns-cache** feature is enabled, only the final response is cached.

With this release, the NS delegations are cached as well. The NS records that are extracted from the authority section, and the A/AAAA glue records that are extracted from the additional section in the DNS (referral) responses are cached along with the final response.

When a new query is received from the client, ACOS first searches the dns-cache for a DNS response matching the client's FQDN, query type, and the query class. If not found, NS records are searched in the cache before starting the recursive resolution process. The NS record search is done to find the authoritative name server that is closest to the client's requested FQDN in order to start the recursive resolution process instead of approaching the default root DNS servers. The closest NS match from the cache is then used only if a corresponding valid A/AAAA record also exists in the cache.

NOTE: For the closest NS match, if ACOS does not find a corresponding A/AAAA record in the cache, full resolution process is used (the recursive resolution will start from the root DNS servers).

The entire process is explained with an example below:

To resolve www.google.com, ACOS first approaches the root DNS servers and gets the referral for .com, then it approaches the .com server to get the referral for google.com. Further, it approaches the google DNS server to get the final response for www.google.com.

With current cache support, ACOS caches only the final answer that corresponds with www.google.com. If the client now requests for mail.google.com, then the whole process is repeated, which starts from approaching the root DNS servers.

With this feature, ACOS caches the NS records for the .com server as well as google.com and also any associated A/AAAA glue records extracted from the referral responses. This way, the resolution for mail.google.com can start directly with the NS of google.com instead of the root DNS servers.

CLI Configuration

The following commands are introduced under `recursive-dns-resolution` to support the enhancement for caching NS delegations and A/AAAA records from glue records:

- `ns-cache-lookup` – This option is used to enable or disable the caching of the NS delegations and A/AAAA records from glue records. This operation accelerates the resolution process. By default, the option is enabled.
  The option can be used as shown in the example below:

```
vThunder(config-dns-recursive-dns-resolution)#ns-cache-lookup enabled
```

- `use-service-group-response` – This option is used to enable or disable the backend service group response and skip the recursive resolver.
  The option can be used as shown in the example below:

```
vThunder(config-dns-recursive-dns-resolution)#use-service-group-response enabled
```

NOTE: The dns-cache feature must be enabled globally using the command `dns-cache-enable` under 'slb common'.

Minimal Response Support for Recursive Resolution

With this release, minimal response is supported for recursive resolution. By default, the ‘Authority’ and ‘Additional’ sections are removed from the response before returning the output to the client.

Minimal response is the default behavior, and full response can be configured for recursive resolution as mentioned below in the CLI Configuration. When full response is configured, the ‘Authority’ and ‘Additional’ sections are displayed in the response.

NOTE:

Consider the following points:

- The EDNS, which is in the ‘Additional section’, is not removed in case of the default setting for this option.
- Complete response is saved in the cache. If the cache is shared, other users can access the response.

CLI Configuration

To enable full response, configure the following command:

```
vThunder(config-dns-recursive-dns-resolution)#full-response
```

Configure Default Authoritative NS for DNS Recursive Resolver

The current DNS recursive resolver uses a list of root NS (name servers) as default authoritative servers to send the first query in each layer of recursive process.

With this release, ACOS supports configuration of the default authoritative name servers for the DNS recursive resolver instead of using the list of root NS.

NOTE: Consider the following points:

- Maximum of 16 IPv4 or IPv6 name servers can be configured for each L3v partition.
- If customized name servers are configured, the recursive DNS resolver uses these servers as default authoritative servers to send the first query in each layer of recursive process instead of the root name servers.

CLI Configuration

The following command and the options are introduced to configure the default authoritative NS:

- `system dns recursive-nameserver` – This command configures the default DNS authoritative NS for recursive DNS resolver.

  The following options are added under `recursive-nameserver`:

  - `A.B.C.D` - Specify IPv4 server address.
  - `A:B:C:D:E:F:G:H` - Specify IPv6 server address.
  - `follow-shared` - This option is available only for private L3v partition. Specify this option to use the configured name server of the shared partition in the private partition.

    NOTE: The `follow-shared` option and the configurable name server cannot be enabled at the same time.

Example to configure follow-shared option for private partition p1 is shown below:

```
vThunder (config)#active-partition p1
vThunder (config)#system dns recursive-nameserver
vThunder [p1] (config-recursive-nameserver)#follow-shared
```

Carrier Grade NAT

ACOS 5.2.1-P4 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

NOTE: For CGN or CGNAT specific configuration steps, refer *IPv4-to-IPv6 Transition Solutions Guide*.

The following topics are covered:

Enhanced L4-based Selective Filtering

L4 based selective filtering is enhanced with the following options:

- **`action log`** – This action is used for logging events without dropping the packets.
- **`expiration`** *`seconds`* – This option is added after the action type and specifies the L4 entry's' expiration time.

Additionally, the **`show cgnv6 ddos-protection l4-entries`** command is modified to display the expiration time in the output.

CLI Configuration

In the following example, L4 based selective filtering is configured with the logging action and an expiration time of 70 seconds,

```
ACOS(config)# cgnv6 ddos-protection packets-per-second udp 30 action log
expiration 70
```

GUI Configuration

To configure the action log and expiration options, go to **CGN > DDoS Protection > CGNv6 DDoS Protection > Advanced**.

Support for Logging One-to-One NAT44 Sessions

With ACOS 5.2.1-P4, you can enable logging for One-to-One NAT44 sessions with RADIUS attributes using the "`log one-to-one-nat sessions`" command under the logging template.

CLI Configuration

The following highlighted command enables logging for One-to-One NAT44 sessions:

```
ACOS(config)# cgnv6 template logging log1
ACOS(config-logging:log1)# log one-to-one-nat sessions
ACOS(config-logging:log1)# log http-requests url
ACOS(config-logging:log1)# log user-data
ACOS(config-logging:log1)# log sessions
ACOS(config-logging:log1)# include-destination
ACOS(config-logging:log1)# include-inside-user-mac
ACOS(config-logging:log1)# include-partition-name
ACOS(config-logging:log1)# rule port-mappings interim-update 30
ACOS(config-logging:log1)# format [cef|ascii]
ACOS(config-logging:log1)# service-group syslog
```

The following highlighted command configures the RADIUS attributes and sends the One-to-One NAT44 logs to the RADIUS server:

```
ACOS(config)# cgnv6 template logging log
ACOS(config-logging:log)# log one-to-one-nat sessions
ACOS(config-logging:log)# log http-requests url
ACOS(config-logging:log)# log sessions
ACOS(config-logging:log)# include-radius-attribute imei sessions
ACOS(config-logging:log)# include-radius-attribute imsi sessions
ACOS(config-logging:log)# service-group cgn-log-group
ACOS(config-logging:log)# exit
```

NetFlow Template Enhancement

Currently, ACOS provides the timestamp for the first packet (`flow-start-msec`) of the flow. Starting with ACOS 5.2.1-P4, ACOS provides a `flow-end-msec` field for viewing the timestamp of the last packet of the flow.

NOTE: This is supported only in Custom IPFIX templates.

For more information, refer to *Command Line Reference Guide* and *Traffic Logging Guide*.

FIPS

ACOS 5.2.1-P4 introduces the following new features and enhancements for the FIPS.

The following topic is covered:

IPSec Support for FIPS Compliance

Starting with ACOS 5.2.1-P4, FIPS mode is supported in IPsec.

For more information, refer to the *System Configuration and Administration Guide*.

Firewall

ACOS 5.2.1 -P4 introduces the following new feature and enhancement for Firewall:

NOTE: For Firewall specific configuration steps, refer *Firewall Configuration Guide*.

The following topic is covered:

DS-Lite Traffic Processing Support

The firewall now supports Dual-Stack Lite (DS-Lite) traffic processing by enhancing the rule-set to inspect the encapsulated payload (IPv4) of the DS-Lite traffic.

The following operations are now supported on DS-Lite traffic:

- Classifying applications - The classification happens only on the encapsulated payload (IP4) of the DS-Lite packet.
- Performing IP Threat list lookup – The decapsulated DS-Lite traffic (IPv4) can go through an IPv4 Threat list lookup.
- Applying rate-limiting policies - Rate limiting can be applied at a rule level using template policies for the encapsulated payload (IPv4) only.
- Configuring logging and Netflow/IPFIX

To process DS-Lite traffic, you need to configure a firewall rule-set with two rules having specific commands. The first rule is configured to inspect and match the outer IPv6 header of the DS-Lite traffic. When the rule matches, the encapsulated IPv4 payload is inspected against the second rule to determine the final action to be taken on the DS-Lite packet.

CLI Configuration

In the following configuration, the **rule-set test** contains **outer-v6** and **inner-v4** rules to process DS-Lite traffic:

```
rule-set test
  rule inner-v4
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
    service any
    application protocol http
    action-group
      permit log
      permit limit-policy 123
  rule outer-v6
    ip-version v6
    action permit cgnv6 ds-lite lsn-lid 2 inspect-payload
    source ipv6-address any
    source zone any
    dest ipv6-address any
    dest zone any
    service any
    application any
```

```
!
```

Network Configuration

ACOS 5.2.1-P4 introduces the following new features and enhancements for the Network Configuration.

NOTE: For configuration and CLI commands, refer *Network Configuration Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topics are covered:

BFD Show and Log Enhancement

The BFD show command is updated to include CPU and RX/TX BFD packet timestamp information.

```
ACOS# show bfd neighbors details
```

The BFD show log messages are enhanced to provide the reason for a BFD session down transition.

CLI Configuration

In the example below, the BFD Session Down Transition occurred due to the “Detect timer expiry” reason.

```
ACOS# show log
Log Buffer: 30000
Dec 03 2021 05:22:52 Notice [L3]:BFD Session DOWN: proto 128:
Local(Down on Detect timer expiry):50.50.50.60 -> Remote(Up):50.50.50.1
```

For more information, refer to the *Command Line Reference Guide*.

Increased L2/L3 Resource Limits

The following L2/L3 resources for the 64 GB, 96 GB, and 128 GB vThunder platforms have increased limits.

- Number of L3V partitions
- Number of Static Routes
- Number of OSPF and IS-IS routes
- Number of BGP routes
- Number of BGP peers
- Number of BGP paths
- Number of ARP and ND6 entries
- Number of MAC entries
- Number of VLANS per interface

For more information, refer to the datasheets.

IPv4 Unnumbered for IP Tunnels

ACOS allows users to configure Logical Interfaces (LIFs) as unnumbered interfaces. The packets can originate from or terminate to the unnumbered interface. Logical Interfaces can be configured in shared or L3V partitions.

Any packet originated or destined to unnumbered interface will use the following IP address as the source IP address:

```
ip unnumbered
   use-source-ip 12.12.12.12
```

CLI Configuration

The following command is used to configure ip unnumbered on the logical interface.

```
ACOS (config) # int lif 123
ACOS (config-if:lif:123) # ip unnumbered
```

Scaleout

ACOS 5.2.1-P4 introduces the following new feature and enhancement for Scaleout:

NOTE: For Scaleout specific configuration steps, refer *Scaleout Configuration Guide*.

The following topics are covered:

IPv6 Prefix Length

Starting with ACOS 5.2.1-P4, the `ipv6-prefix-length` command is introduced. It is a system-level attribute that indicates the length of the source and destination IPv6 prefix.

This prefix is used for the following:

- In a Dual-blade chassis platform, to determine the Processing Unit (PU) to process a received packet.
- In a Scaleout cluster, to determine the user group for the packet, which in turn determines the active node for this packet.
- The IPv6 prefix length must be less than or equal to all configured values for the user-quota-prefix-length. If the IPv6 prefix length is greater than the user-quota-prefix-length, all packets with the same user-quota prefix will not receive the same NAT IPv4 address.

The IPv6 prefix length can be configured only in the shared partition but is applicable to all L3V partitions, LIDs, and Class-lists. The default value is set to 128 on all devices.

CLI Configuration

The following command is used to configure the IPv6 prefix length:

```
ACOS(config)#system ipv6-prefix-length length
```

You can select a value between 16 and 128 for length. By default, the IPv6 prefix length is 128.

NOTE: The IPv6 prefix length must be modified only when the device or cluster is not in use. Else, unpredictable disruptions may occur to the traffic.

For more information, refer to the *IPv4-to-IPv6 Transition Solutions Guide*, *Command Line Reference Guide*, *Scaleout Configuration Guide*, and *Configuring VRRP-A High Availability Guide*.

Support IPv6 NAT for Scaleout

Starting from ACOS 5.2.1-P4 release, ACOS takes over the IPv6 address if the previous owner is down and releases the address when the old owner is up again, and it advertises route only for the address it owns.

The IPv6 nat pool configuration is moved after the Scaleout configuration as shown in the below example.

For example:

```
scaleout 1
  local-device
    priority 150
    id 3
    cluster-mode layer-3
    traffic-redirection
      interfaces
        ethernet 3
    session-sync
      interfaces
        ethernet 3
  cluster-devices
    device-id 3
      ip 10.64.6.44
    device-id 4
      ip 10.64.6.45
    device-id 5
      ip 10.64.6.46
```

```
  device-groups
    device-group 2
      device-id 3 to 5
  service-config
    template adc1
      device-group 2
!
ipv6 nat pool p63 2000::10:214:7:103 2000::10:214:7:103 netmask 128
scaleout-device-id 3
!
ipv6 nat pool p65 2000::10:214:7:105 2000::10:214:7:105 netmask 128
scaleout-device-id 5
!
ipv6 nat pool p64 2000::10:214:7:104 2000::10:214:7:104 netmask 128
scaleout-device-id 4
!
ipv6 nat pool-group pg6
  member p63
  member p64
  member p65
!
```

VRRP-A High Availability

ACOS 5.2.1-P4 introduces the following new feature and enhancement for VRRP-A High Availability:

NOTE: For configuration and CLI commands, refer *Configuring VRRP-A High Availability*. Similarly, for GUI, refer *ACOS Online Help*.

The following topic is covered:

Show Traffic Engineering (TE) MAC Enhancement

The following show commands are implemented to view the TE MAC address.

- ACOS# **show vrrp-a te-mac**
- ACOS# **show system platform te-mac**

NOTE: These commands are supported only on the chassis platform.

To view the TE MAC address when VRRP-A is not enabled, use the following command:

```
ACOS# show system platform te-mac
```

To view the TE-MAC address of each VRRP VRID configured, use the following command:

```
ACOS# show vrrp-a te-mac
```

For more information, refer to the *Command Line Reference Guide* and *Configuring VRRP-A High Availability*.

Enhancements in ACOS 5.2.1-P3

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P3 release:

The following topics are covered:

MIB

ACOS 5.2.1-P3 introduces the following new features and enhancements forMIB:

NOTE: For more information about supported MIB object details, refer *MIB Guide*.

The following topics are covered:

- SNMPv3 Support for L3V MIB Retrieval
- SNMP Traps for Scaleout
- SNMP OIDs Enhancements for Processing Units

SNMPv3 Support for L3V MIB Retrieval

With this release, SNMPv3 supports L3V MIB information retrieval. For SNMPv3, attach the partition name to the user (example user_name@p1) to retrieve MIB information for the L3V.

NOTE: The SNMPv2 MIB retrieval is unchanged and it requires attaching the partition name to the community string (example: public@p1).

Known Limitations

- Users cannot retrieve data from all partitions using a single SNMP request. When a large number of partitions (> 64) are configured, functionality to retrieve data for all the partitions by providing community string from the share partition is no longer supported.

SNMP Traps for Scaleout

With this release, SNMP traps can be sent to alert you of Scaleout state transitions such as nodes joining or leaving the cluster, a node entering a single-node mode, a master node calling for re-election, traffic map update, and so on.

The following SNMP traps are introduced to monitor and send notifications on Scaleout performance, failure, and health of Scaleout deployment:

- Node Status - Node joined or left cluster
- Single Node status - Node enter single node mode
- Service-Master - Node is service or master
- Cluster election - Election time
- Master calling re-election - Master is calling for re-election
- Local Node disabled - Local node is disabled
- Traffic map Update - Traffic map update
- Traffic map distribution - TMAP distribution
- vServer Traffic map update - vServer TMAP update

CLI Configuration

```
ACOS(config)# snmp-server enable traps scaleout
```

SNMP OIDs Enhancements for Processing Units

In this release, the following new object-ID's (OIDs) are added to collect information about the L3V partition for all processing units via SNMP:

- axFwSystemStatusTable(.1.3.6.1.4.1.22610.2.4.4.1.2.4.4)
- axAverageControlCpuUsageTable(.1.3.6.1.4.1.22610.2.4.4.1.1.1.3)
- axAverageDataCpuUsageTable(.1.3.6.1.4.1.22610.2.4.4.1.1.1.4)
- axCurrFiveSecCtrlCpuUsageTable(.1.3.6.1.4.1.22610.2.4.4.1.1.1.10)
- axCurrFiveSecDataCpuUsageTable(.1.3.6.1.4.1.22610.2.4.4.1.1.1.9)
- axFwGlobalStatsTable(.1.3.6.1.4.1.22610.2.4.4.1.2.4.1)
- axLifIntfStatsTable(.1.3.6.1.4.1.22610.2.4.4.1.2.2.2)
- axLsnGlobalStatsTable(.1.3.6.1.4.1.22610.2.4.4.1.2.3.1.4)
- axLsnFullConeSessionStatsTable(.1.3.6.1.4.1.22610.2.4.4.1.2.3.1.5.1)
- axLsnSystemStatusNatPortUsageTable(.1.3.6.1.4.1.22610.2.4.4.1.2.3.1.3)
- axLsnSystemStatusSessionTable(.1.3.6.1.4.1.22610.2.4.4.1.2.3.1.2)
- axLsnUserQuotaSessionTable(.1.3.6.1.4.1.22610.2.4.4.1.2.3.1.1.1)
- axNatPoolStatTable(.1.3.6.1.4.1.22610.2.4.4.1.2.3.2.1)
- axSessionStatsTable(.1.3.6.1.4.1.22610.2.4.4.1.2.1.3)
- axSystemAppPerformanceTable(.1.3.6.1.4.1.22610.2.4.4.1.2.1.2)
- axVEIntfStatsTable(.1.3.6.1.4.1.22610.2.4.4.1.2.2.1)

The following new OIDs can retrieve information such as current CPU usages and rate of interfaces for all processing units:

- axCurrFiveSecDataCpuUsageTable(1.3.6.1.4.1.22610.2.4.4.1.1.1.9)
- axCurrFiveSecCtrlCpuUsageTable(.1.3.6.1.4.1.22610.2.4.4.1.1.1.10)
- axVEIntfStatsTable(.1.3.6.1.4.1.22610.2.4.4.1.2.2.1)
- axLifIntfStatsTable(.1.3.6.1.4.1.22610.2.4.4.1.2.2.2)

Platform

ACOS 5.2.1-P3 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

Disable Access to NTP Server on ACOS

To prevent ACOS from acting as an NTP server and responding to the requests received from NTP clients, you can use the `disable-management service ntp` CLI command. Configuring the `disable-management service ntp` CLI command at the configuration level disables access to the NTP service and stops ACOS from responding to the NTP client requests.

An Access Control List (ACL) permits or denies management access through the interface by specific hosts or subnets. You can use the `enable-management service acl-v4` command to apply ACL on incoming NTP requests on any or all interfaces OR apply ACL on all interfaces. Configuring the `enable-management service acl-v4` command at the management level stops the services from responding to the incoming NTP client requests.

The following example shows how to stop ACOS from responding to the incoming NTP client requests on the specified port using the disable-management service.

```
ACOS(config)# disable-management service ntp
You may lose connection by disabling the ntp service.
Continue? [yes or no]: yes
ACOS(config-disable-management ntp)#ethernet 3
```

The following example shows how to configure an ACL for incoming NTP request on any or all interfaces using the enable-management service.

```
ACOS(config)# enable-management service ntp
ACOS(config-enable-management ntp)#acl-v4 1
ACOS(config-enable-management ntp-acl-v4)#ethernet 1
```

The following show command is updated to include the new feature information:

```
ACOS# show management
```

GUI Configuration

Under **System > Access Control**, a new field **NTP** is added.

For more information, refer to the *Command Line Reference Guide* and *Management Access and Security Guide*.

NTP Logging Enhancement

With this release, the system time change event in NTP logging is enhanced to log multi-source servers involved in the NTP time synchronization.

Scaleout

ACOS 5.2.1-P3 introduces the following new feature and enhancement for Scaleout:

NOTE: For Scaleout specific configuration steps, refer *Scaleout Configuration Guide*.

The following topic is covered:

Resource Tracking Across L3V Partition

Starting from ACOS 5.2.1-P3 release, the following features are supported:

- L2 redirection in the L3V partition. The L2 dedicated redirection interface may only be configured in the shared partition. All shared and L3V redirected packets will use this configured redirection interface.
- Multiple policy-based failover templates can be created and associated to a Scaleout cluster to resource track L3V partition objects such as BGP or routes or Gateway across the partition.

CLI Configuration

```
ACOS(config)#scaleout 1
ACOS(config-cluster:1)#local-device
ACOS(config-cluster:1-local-device)#priority 1
ACOS(config-cluster:1-local-device)#id 3
ACOS(config-cluster:1-local-device)#tracking-template
```

```
ACOS(config-cluster:1-local-device-tracki...)#multi-template multi
ACOS(config-cluster:1-local-device-tracki...)#template BGP partition
PART-2
ACOS(config-cluster:1-local-device-tracki...)#template BGP partition
PART-3
ACOS(config-cluster:1-local-device-tracki...)#threshold 100 down
```

vThunder

ACOS 5.2.1-P3 introduces the following new features and enhancements forvThunder (Virtual Thunder):

The following topic is covered:

Cloud-init Script Enhancement

During vThunder Openstack deployment, when an system is configured with the commands that require reload or reboot, like `system promiscuous-mode` and `system-jumbo-global enable-jumbo` commands using the `cloud-init` script, the system must be manually reloaded for the configuration to take effect.

With this release, a new command `reload_cmd` is added under the `cloud-init` script to automatically reload the system after configuring the above commands.

Configuration Example

```
a10_blob: |
      hostname vThunder
      system promiscuous-mode
      system-jumbo-global enable-jumbo
      wr mem
reload_cmd:
      enable:
```

Enhancements in ACOS 5.2.1-P2

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P2 release:

The following topics are covered:

aXAPI

ACOS 5.2.1 -P2 introduces the following new features and enhancements foraXAPI:

NOTE: For aXAPI specific configuration steps, refer aXAPIv3 Reference Document. Similarly, for ADC specific CLI commands, refer *Command Line Reference Guide*.

The following topic is covered:

Support for 1000 aXAPI Concurrent Connection

With this enhancement, 1000 TCP concurrent aXAPI connections can be established using worker MPM module. Before, aXAPI used prefork MPM module to handle multiple connections which is single threaded and only one connection was allowed per thread. The 1000 TCP concurrent aXAPI connections will increase the system performance as multiple clients can be served at the same time with a limited number of control CPUs and memory. Moreover, multiple requests processed will have the same turnaround time.

CLI Configuration

Following are the new CLI commands added under `web-services`

```
ACOS(config)# web-service mpm-max-conn num
ACOS(config)# web-service mpm-min-spare-conn num
ACOS(config)# web-service mpm-max-conn-per-child num
ACOS(config)# web-service public-apis  /axapi/v3/<sub path>
```

Carrier Grade NAT

ACOS 5.2.1-P2 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

The following topics are covered:

Introducing A10 Threat Intel List and Internet Host Lists

Until now, third-party databases such as ThreatSTOP and WebRoot were imported to create IP Threat lists. In this release, ACOS has introduced the A10 Threat Intel List that can also be imported to create an IP Threat list. This threat list can be used by

the Carrier Grade NAT (CGN) to detect malicious sources and drop the traffic associated with the anomalous IPs. This list has the capability to drive the Threat IP protection feature by protecting against DDoS attacks as well.

The **a10-ip-threatList** class-list is generated by the A10 Research Team and can be downloaded from the GLM server only with a valid A10 Threat Intel license. The list must be bound to an IP Threat list by using the **system ip-threat-list** command.

NOTE: The IPs in the threat list are common for all partitions.

Known Limitations:

- IPv6 addresses are not supported.
- L3V level configuration is not supported.
- Only a single class-list is supported.

The **system ip-threat-list** command is also enhanced by introducing the following IP threat lists:

- IPv4 Internet Host List (**ipv4-internet-host-list**)
- IPv6 Internet Host List (**ipv6-internet-host-list**)

These threat lists contain a list of internet-hosts and subscriber addresses and can track malicious internet IPs in both the directions. Therefore, instead of two separate threat lists (source list and destination list), a single internet host list can be used.

CLI Configuration

The **automatic-update** command is enhanced by introducing the following options to update and download A10 Threat Intel list:

- To update the A10 Threat Intel list daily:

```
ACOS(config)# automatic-update a10-threat-intel schedule daily 12:30
```

- To update the A10 Threat Intel list on a weekly basis:

```
ACOS(config)# automatic-update a10-threat-intel schedule weekly
Tuesday 12:30
```

- To stop the automatic updates:

```
ACOS(config)# no automatic-update a10-threat-intel schedule daily
12:30
```

- To view the automatic update schedule:

```
ACOS (config)# show automatic-update
```

The following examples demonstrate Internet Host List usage:

- To create an IPV4 Host List by binding to A10 Threat Intel list:

```
ACOS(config)# system ip-threat-list
ACOS(config-ip-threat-list)# ipv4-internet-host-list
ACOS(config-ip-threat-list-ipv4-internet-host)# class-list a10-ip-
threatList
```

- To create an IPV6 Host List:

```
ACOS(config)# system ip-threat-list
ACOS(config-ip-threat-list)# ipv6-internet-host-list
ACOS(config-ip-threat-list-ipv6-internet-host)# class-list
mythreatlist
```

For more information refer to the *Firewall Configuration* guide and *Command Line Interface Reference* guide.

Additional Custom RADIUS Attributes

In addition to the three custom RADIUS attributes that already existed in the prior releases, there are three additional custom RADIUS attributes now supported under system radius server configuration. These attributes help in logging custom messages that may be required for satisfying regulatory requirements.

Configuration Example

```
ACOS(config)# system radius server
ACOS(config-radius-server)# remote ip-list RADIUS_IP_LIST
ACOS(config-radius-server)# secret a10
ACOS(config-radius-server)# attribute inside-ipv6 vendor 22610 number 29
ACOS(config-radius-server)# attribute msisdn number 31
ACOS(config-radius-server)# attribute imei vendor 10415 number 20
ACOS(config-radius-server)# attribute imsi vendor 10415 number 1
```

```
ACOS(config-radius-server)# attribute custom1 l3v-c1 vendor 22610 number
42
ACOS(config-radius-server)# attribute custom2 l3v-c2 vendor 22610 number
43
ACOS(config-radius-server)# attribute custom3 cus3 vendor 22610 number
44
ACOS(config-radius-server)# attribute custom4 cus4 vendor 22610 number
81
ACOS(config-radius-server)# attribute custom5 cus5 vendor 22610 number
82
ACOS(config-radius-server)# attribute custom6 cus6 vendor 22610 number
83
ACOS(config-radius-server)# exit
```

The new custom attributes can be configured under the logging template in the same way as the other custom attributes.

For more information, see *IPv4-to-IPv6 Transition Solutions Guide* and *Traffic Logging Guide*.

Maximum Number of One-to-One NAT IP Addresses

For platforms with 128 GB memory, the maximum number of One-to-One NAT IP addresses you can configure is increased to 2 million IP addresses.

For more information, see *IPv4-to-IPv6 Transition Solution Guide*.

Support for Logging One-to-One NAT64 Sessions

With ACOS 5.2.1-P2, you can enable logging for One-to-One NAT64 sessions with RADIUS attributes. For enabling logging for One-to-One NAT64 sessions, use the "log one-to-one-nat sessions" command under the logging template.

NOTE: The One-to-One logging is not supported for NAT44 and NAT64 with Fixed NAT sessions.

Example Configuration:

The following commands enable logging for One-to-One NAT64 sessions:

```
ACOS(config)# cgnv6 template logging log1
ACOS(config-logging:log1)# log one-to-one-nat sessions
ACOS(config-logging:log1)# log http-requests url
ACOS(config-logging:log1)# log user-data
ACOS(config-logging:log1)# log sessions
ACOS(config-logging:log1)# include-destination
ACOS(config-logging:log1)# include-inside-user-mac
ACOS(config-logging:log1)# include-partition-name
ACOS(config-logging:log1)# rule port-mappings interim-update 30
ACOS(config-logging:log1)# format [cef|ascii]
ACOS(config-logging:log1)# service-group syslog
```

The following commands configure the RADIUS attributes and send the One-to-One NAT64 logs to the RADIUS server:

```
ACOS(config)# cgnv6 template logging log
ACOS(config-logging:log)# log one-to-one-nat sessions
ACOS(config-logging:log)# log http-requests url
ACOS(config-logging:log)# log sessions
ACOS(config-logging:log)# include-radius-attribute imei sessions
ACOS(config-logging:log)# include-radius-attribute imsi sessions
ACOS(config-logging:log)# service-group cgn-log-group
ACOS(config-logging:log)# exit
```

Port Batch Duration

To log the duration of the Port Batch bindings for lawful inspection, a new RADIUS attribute by the name "A10_CGN_PORT_BATCH_DURATION" is introduced in ACOS 5.2.1-P2. This attribute can be added to the RADIUS log messages when the ACOS event is Port Batch Freed or Port Batch Interim Update. The A10-CGN-PORT_BATCH_DURATION shows the duration for which the port batch is allocated to the subscriber. This attribute is displayed only when **`include-port-block-account`** is configured under the logging template.

Configuration Example

```
ACOS(config)# cgnv6 template logging log
ACOS(config-logging:log)# log sessions
ACOS(config-logging:log)# include-port-block-account
ACOS(config-logging:log)# rule port-mappings interim-update 15
```

```
ACOS(config-logging:log)# log-receiver radius secret 123456
ACOS(config-logging:log)# service-group sg_udp
```

The A10_CGN_PORT_BATCH_DURATION is supported for Binary, CEF, Compact, Custom, and Default formats.

Port Batch Interim Update Log Example

```
Attributes : {
Acct-Status-Type(40) l=6 val=Stop(2)
Acct-Session-Id(44) l=18 val=000032384DDFB3
NAS-Identifier(32) l=25 val=vThunder@192.168.97.108
Vendor-Specific(26) {
A10-CGN-Timestamp(6) l=6 val=May 27, 2021 22:40:43.000000000
A10-CGN-Protocol(7) l=6 val=TCP(1)
A10-CGN-Action(20) l=6 val=Port-Batch-Pool-Freed(12)
A10-CGN-IMEI(26) l=5 val=111
A10-CGN-Radius-Custom-1(42) l=6 val=a111
A10-CGN-Radius-Custom-2(43) l=9 val=bbbb111
A10-CGN-Radius-Custom-3(44) l=9 val=cbbb111
A10-CGN-Inside-Addr(10) l=6 val=10.0.1.105
A10-CGN-NAT-Addr(12) l=6 val=10.1.1.91
A10-CGN-Port-Batch-Pool-Port-Start(59) l=4 val=29632
A10-CGN-Port-Batch-Pool-Port-End(60) l=4 val=29695
A10-CGN-Port-Block-Acct-Upload-Bytes(79) l=10 val=135779
A10-CGN-Port-Block-Acct-Download-Bytes(80) l=10 val=94326
A10-CGN-PORT_BATCH_DURATION(84) l=6 val=1437
```

For more information, see *Traffic Logging Guide*.

Global License Manager

ACOS 5.2.1-P2 introduces the following new features and enhancements for the Global License Manager (GLM):

The following topics are covered:

Modular Licensing

Earlier, under the Perpetual license, the ACOS devices provided unrestricted hardware and software capabilities irrespective of the business requirements. However, in some cases, the devices were not utilized to their full capacity.

Now, the Modular license is introduced to customize the ACOS products as per your business needs. You have the flexibility to select the license based on the allocation of the following device parameters:

- Number of CPU Cores
- Number and type of ports
- Bandwidth
- Memory
- SSL Chipset: Software Only / QAT / N5

These hardware parameters drive the device performance characteristics such as the number of Layer 4/Layer 7 sessions, the number of Connections-Per-Second (CPS), the Packets-Per-Second (PPS), throughput, and so on.

Modular Licensing provides the following features and advantages:

- Enables performance-based tiering of the hardware platform (for example: Low, Medium and High).
- Provides the agility to upgrade from a lower end performance model to a higher end performance model without changing the hardware platform.
- Offers pay-as-you-go purchasing plan. You need to pay only for the selected performance model instead of the whole package.
- Enables the hardware platform to be provisioned with the desired product i.e., ADC, CGN, CFW, SSLi or TPS without changing the hardware.

For more information, refer to the *Global License Manager User Guide*.

NOTE: The naming convention for the license types i.e., Low, Medium and High is subject to change. It is mentioned here only as an example.

GTP

ACOS 5.2.1-P2 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

The following topic is covered:

Show GTP Sessions

Starting with ACOS 5.2.1-P2, the GTP session information can be viewed using the **show session gtp** CLI command. You can also use **show session gtp rev-dest-teid <tied number>** to view the GTP session matching rev tuple dest-teid. The **show session gtp** command displays information such as the following:

- Number of GTP-C sessions established
- Number of GTP-C sessions half-open
- Total number of GTP-U sessions
- Total number of GTP Echo sessions
- Number of GTP sessions that can be created
- Cumulative number of GTP connections created including GTP-C, GTP-U and GTP Echo
- Cumulative number of GTP connections freed

Show Command Example

```
ACOS(config)#show session gtp
Traffic Type Total
-------------------------------------------
GTP-C Established 0
GTP-C Half Open 0
GTP-U Count 0
GTP-Echo Count 0
GTP Current Available Conn 203979
GTP Conn Created(cumulative) 0
GTP Conn Freed(cumulative) 0
```

For more information, see *Firewall Configuration Guide*.

IPsec Virtual Private Network

ACOS 5.2.1-P2 introduces the following new features and enhancements for IPsec Virtual Private Network:

NOTE: For configuration and CLI commands, refer *IPsec Configuration Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topics are covered:

Enhancement to Avoid Use of Weaker Ciphers

For a secure environment, the following conditions should be fulfilled to ensure that weaker ciphers are not used:

- IKE SA should not use weaker cipher than IPSec SA.
- Both IKE SA and IPsec SA should not use weaker ciphers such as Des/3DES/MD5.

CLI Configuration

To enable the function where the IPsec tunnel is not established if the conditions mentioned above are not fulfilled, a new CLI command has been introduced in the **Global Configuration** mode:

```
vpn ipsec-cipher-check
```

GUI Configuration

Go to **Security > IPsec VPN > Settings**. On the **VPN Global Settings** page, **Cipher Check** option is available with this release. When this option is selected, it enables the function where the IPsec tunnel is not established if the conditions mentioned above are not fulfilled.

Loading a CA certificate into VPN daemon

When a CA certificate is imported into ACOS, it is loaded into a VPN daemon. With this release, the following validity checks are performed before loading the CA certificate into the VPN daemon:

- The CA certificate is loaded only when the CA flag is TRUE.
- The ECDSA (Elliptic Curve Digital Signature Algorithm) CA certificate is not loaded if it uses the explicit EC (Elliptic Curve) parameter.

Enhancement to VPN IKE Negotiation

With this release, VPN IKE negotiation log can be sent to syslog.

CLI Configuration

To enable the function where the VPN IKE negotiation log can be sent to syslog, a new CLI command has been introduced in the **Global Configuration** mode:

```
vpn ike-logging-enable
```

The log can then be displayed by using the command ‘show log’.

GUI Configuration

Go to **Security > IPsec VPN > Settings**. On the **VPN Global Settings** page, **Enable IKE Logging** option is available with this release. When this option is selected, it enables the function where the VPN IKE negotiation log can be sent to syslog.

Secure Sockets Layer Insight

ACOS 5.2.1-P2 introduces the following new features and enhancements forSecure Sockets Layer Insight (SSLi):

NOTE: For SSLi configuration steps, refer *SSL Insight Configuration Guide*. Similarly, for SSLi specific CLI commands, refer *Command Line Reference for ADC Guide*.

The following topics are covered:

SSL Certificate Management Enhancement

The 'certificate' command was introduced in the previous releases for SSL offloading features to configure the cert, key, and chain-cert information together. However, the forward proxy features still utilize separate commands to configure chain-cert.

To improve the certificate management, ACOS now supports configuring cert, key, and chain-cert information together for forward proxy features.

This feature can be configured using both CLI and GUI. It supports partition option as well.

NOTE:

- If the old commands are already in use, then the behavior will be same as before. However, A10 Networks recommends to use the new certificate commands for easy upgrade and migration.
- After upgrading, the old CLI and GUI options will no longer be visible. So, utilize the new options to configure the new certificates. For more information about certificate management during upgrade, refer to *Changes to Default Behavior* section in the *Release Notes*.

CLI Configuration

- **ACOS (config)# forward-proxy-ca-certificate** *<cert-name>* **key** *<key-name>* **[pass-phrase** *<pass-phrase>***] [chain-cert** *<chain-cert-name>***] [partition** *<shared>***]**
- **ACOS (config)# forward-proxy-alt-sign cert** *cert-name>* **key** *<key-name>* **[pass-phrase** *<pass-phrase>***] [chain-cert** *<chain-cert-name>***] [partition** *<shared>***]**

GUI Configuration

- Go to **ADC > Template > SSL > Client SSL**:
  - Forward Proxy Chain Cert
  - Forward Proxy Chain Cert From Shared Partition

- Forward Proxy Alternate Signing Chain Cert
- Forward Proxy Alternate Signing Chain Cert From shared partition

- Go to **Security > SSLi > Templates > Client SSL**:
  - Under Forward Proxy > Chain Cert and Chain Cert From Shared Partition
  - Under Forward Proxy Alt Sign > Chain Cert and Chain Cert From Shared Partition

GUI Certificate Page Enhancement

The existing **Certificate** page under **System** module is enhanced to display the detailed certificate information in a new **Info** tab.

GUI Configuration

Go to **System > Settings > Certificate** and select:

- **Upload** tab - To upload the certificate files.
- **Info** tab - To view the certificate detailed information.

Direct Client-Server Authentication Solution

The direct client-server authentication is enhanced to verify the SSL state for packet forwarding. This functionality is primarily designed to work with the old Nitrox V (N5) and Rivest–Shamir–Adleman (RSA) key exchange algorithms.

NOTE:	This feature does not work for TLS 1.3 and new SSL.

Restructured Signature Signing Algorithm

The signature signing algorithm is restructured to manage the Secure Hashing Algorithm (SHA) in the old software SSL. ACOS will choose the signature algorithm from the signature_algorithms list in the ClientHello extension. If the client and ACOS share no signature algorithm, then SHA will be used as the default hash algorithm.

SSLi Error Logging Enhancement

The existing SSLi error logging messages are enhanced with additional information for debugging SSLi failures effectively. This enhancement is implemented in the following areas:

- CEF
- Syslog
- Harmony Controller

Application Delivery Controller

ACOS 5.2.1 -P2 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for ADC specific CLI commands, refer *Command Line Reference for ADC Guide*.

The following topics are covered:

TLS Session Resumption Support

The existing session ticket feature is extended to support Transport Layer Security (TLS) session resumption within the HTTPS health monitoring method. Session resumption using session tickets is a beneficial mechanism for various reasons like fewer round trips, fewer computations, and a lower congestion window, all without burdening the server. For information about this mechanism, refer to RFC 5077.

When HTTPS monitor uses specific SSL cipher suites to match the specified SSL ciphers used by the resource pool, the full SSL handshake negotiation may impact the CPU utilization and performance. On the other hand, the TLS session resumption reuses the recently valid TLS session ticket and resumes using a single resumption

request rather than a full handshake negotiation. This efficiently manages large volumes of HTTPS traffic and ensures the fastest performance.

The following capabilities are provided in this feature:

- Supports all the TLS versions - 1.0, 1.1, 1.2, and 1.3.
- Cache session tickets up to 5,000 on a ACOS device.
- Delete expired session tickets automatically and manually according to its lifetime.
- Displays the total tickets currently cached in the show command.

CLI Configuration

The following commands configure SSL session ticket for HTTPS health monitor:

- To configure SSL session ticket:

```
ACOS(config)# health monitor hm-https
ACOS(config-health:monitor)# ssl-ticket
ACOS(config-health:monitor)# method https
```

- To configure SSL session ticket timeout value:

```
ACOS(config)# health monitor hm-https
ACOS(config-health:monitor)# ssl-ticket lifetime 4200
ACOS(config-health:monitor)# method https
```

- To configure preferred SSL version for negotiation:

```
ACOS(config)# health monitor hm-https
ACOS(config-health:monitor)# ssl-version 34 34
ACOS(config-health:monitor)# method https
```

- To automatically clear all the SSL session ticket:

```
ACOS(config)# clear health https ssl-tickets
```

- To manually clear the specified health monitor SSL session ticket:

```
ACOS(config)# clear health https ssl-tickets hm-https
```

- To view the SSL health check PINs aggregate:

```
ACOS#show health https
Total HTTPS number:                    : 2
Total SSL Tickets:                     : 2
```

```
Status UP:                                : 2
Status DOWN:                              : 0
Status UNKN:                              : 0
Status OTHER:                             : 0

IP address    Port  Health monitor Status Version Ticket Cipher
-----------------------------------------------------------------
10.212.3.100    443   test-ssl       UP    TLSv1.3 X     TLS_AES_256_
GCM_SHA384
10.212.3.100    443   test-ssl2      UP    TLSv1.3 -      TLS_AES_256_
GCM_SHA384
```

GUI Configuration

- To enable the feature, go to **ADC > Health Monitor > Create > General Fields**:
  - SSL Ticket
  - SSL Ticket Lifetime(Seconds)
  - SSL Version
  - SSL Downgradable Version
- To view the statistics and clear the SSL ticket, go to **ADC > Health Monitor > Statistics > HTTPS Page**.

SLB Template Secure Deletion Support on GUI

Under the **ADC** module, the existing Delete functionality on the **SLB Template** page is enhanced to display a warning dialog before the deletion. This dialog will list the associated virtual services or objects and the total count of the bound objects. You can now review all the bound objects, unbind them securely, and then delete them.

For more information, refer GUI *Online Help*.

The following protocols are supported in this feature:

- Connection Re-Use
- Persist Cookie
- Persist Source IP

- HTTP
- TCP Proxy
- Client SSL
- Server SSL
- TCP

Network Configuration

ACOS 5.2.1-P2 introduces the following new features and enhancements for the Network Configuration:

NOTE: For configuration and CLI commands, refer *Network Configuration Guide*. Similarly, for GUI, refer *ACOS Online Help*.

The following topics are covered:

802.1Q-in-Q VLAN Tagging Support

802.1Q-in-Q (Q-in-Q) VLAN tagging support is implemented to expand the VLAN space by tagging the tagged packets, thus creating a double-tagged frame. Double tagging enables the service provider to separate the traffic from different customers and transparently transfer it throughout the network. It also allows the service provider to provide certain services on specific VLANs for specific customers.

To configure this feature, **`system q-in-q`** command is introduced.

For more information, refer to the *Network Configuration* guide and *Command Line Interface Reference* guide.

Known Limitations

- Supports virtual wire and L2-IPless topologies only.
- Supported on shared partition only. An L3V partition can support Q-in-Q if the configuration is set on a shared partition.

CLI Configuration

The following command demonstrates system q-in-q command usage:

```
ACOS(config)# system q-in-q
ACOS(config-q-in-q)# inner-tpid 9100
ACOS(config-q-in-q)# enable-all-ports
```

Preventing Loops in Networks

Packet brokers (active and passive paths) are used in some enterprise network topologies/environments to route traffic to security devices as service chains. A network loop upstream may occur when the firewall performs a failover to the passive paths. Since ACOS retains VLAN layer 2 information, it cannot be updated after the failover. Hence, it sends the old VLAN information to the sessions and sends packets over the passive route. This results in an indefinite traffic loop and the network never recovers by itself.

To prevent network loop in such topologies, **update-l2-info** command is introduced to detect the changes in the session's L2 information and update the cache accordingly. Additionally, **virtual-wire-global** command is introduced to set the virtual wire update period and to update the active VLANs.

This enhancement supports both VLAN tagged and Q-in-Q VLAN tagged environments. However, it is not supported on fast path.

CLI Configuration

The following command demonstrates **update-l2-info** usage:

```
(config)# interface ethernet 1
(config-if:ethernet:1)# enable
(config-if:ethernet:1)# virtual-wire update-l2-info vlan-learning
disable mac-learning enable
```

The following command demonstrates **virtual-wire-global** usage:

```
(config)# virtual-wire-global
(config-virtual-wire-global)# vlan-update-period 60
(config-virtual-wire-global)# update-active-vlan all
```

`show virtual-wire-global` command is also provided to display the current active VLAN members in a bridge-vlan-group and the global counters.

GUI Configuration

To enable this feature, navigate to:

- **Network** > **Interface** > **LAN**
- **Network** > **Interface** > **Trunk**
- **Network** > **Interfaces** > **Virtual Wire** > **Global**
- **Network** > **Interfaces** > **Virtual Wire** > **Statistics** > **Counters**
- **Network** > **Interfaces** > **Virtual Wire** > **Statistics** > **Active VLAN Member**

For more information, refer to the *Command Line Interface Reference* guide and *Network Interface* guide.

Platforms

ACOS 5.2.1-P2 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

AX Debug Enhancement: tcpdump

The packet of the tcpdump is enabled to display options and filter expressions to view and filter packets. The protocol-aware packet printing functions are used to display packets and the filter expressions are used to filter packets. The tcpdump expressions are used to filter packets and print them.

Known Issues and Limitations

- VLAN is not supported. The packets cannot be captured based on the VLAN filter.
- Inbound/outbound filter is not supported.
- For jumbo packets, the data is not printed completely.

CLI Configuration

The following command can be used to display and filter the packets:

```
ACOS#(axdebug)tcpdump

NAME<length:1-255> Specify tcpdump in quotes ex:"[ -AeqStvxX][
expression]"
```

Open VM Tools Support for vThunder on ESXi

Starting with ACOS 5.2.1-P2, the open-vm-tool is used for installing ACOS 5.2.1-P2 vThunder on the ESXi platform. It helps vThunder to communicate all the IP addresses of the vThunder with the guest OS on the ESXi host.

For more information, refer to the *Installing vThunder on VMware ESXi* guide.

System Table Integrity Support

This feature checks the table integrity and auto-sync options for the following tables:

- Address Resolution Protocol (ARP)
- Neighbor Discovery (ND6)
- IPv4 forwarding information base (FIB)
- IPv6 forwarding information base (FIB)
- Media Access Control (MAC)

Additionally, it detects and fixes any discrepancies across the tables on the Master and Blade.

CLI Configuration

- To enable or disable the table integrity checks and auto-sync options

```
ACOS(config)# system table-integrity all audit [enable | disable]
auto-sync [enable | disable]
```

- To manually sync all the tables between the processing units

  For Shared partition:

  ```
  ACOS(config)# clear system table-integrity [all| arp | ipv4-fib |
  ipv6-fib | mac | nd6 ]
  ```

  For L3V partition:

  ```
  ACOS(config)# clear system table-integrity [all| ipv4-fib | ipv6-fib]
  ```

- To view system table integrity statistics and details

  ```
  ACOS(config)# show system table-integrity statistics [ detail | arp-
  table [detail] | ipv4-fib-table [detail] | ipv6-fib-table [detail] |
  mac-table [detail] | nd6-table [detail] ]
  ```

For more information, refer to Command Line Reference Guide.

vThunder Support on ESXi 7.0

The vThunder software can now be installed on a hardware platform that is running on VMware ESXi 7.0 platform.

For more information, refer to the *Installing vThunder on VMware ESXi* guide.

Thunder Container

ACOS 5.2.1-P2 introduces the following new features and enhancements for ACOS Thunder Container:

NOTE: For more information, refer *Installing Thunder Container on Docker Guide* and *Installing Thunder Container on Kubernetes Guide*.

The following topics are covered:

IO CPU Management for Thunder Container

Currently, in Thunder Container with more than 24 CPUs allocated, the maximum number of I/O CPUs is eight. A new command `system io-cpu max-core` and a new environment variable `ACOS_CTH_IO_CORES_MAX` is added to enhance the maximum number of I/O CPUs.

Login to Thunder Container from Docker

In the Thunder Container, to avoid the users logging in to a10 CLI without authentication, the “a10login” is added. This allows logging with a prompt of User and Password.

VRRP-A High Availability

ACOS 5.2.1-P2 introduces the following new feature and enhancement for VRRP-A High Availability:

The following topic is covered:

Configuration Synchronization Status on User Interface

In this release, the user interface is enhanced to show the status of configuration synchronization of all the devices in the cluster.

For more information, refer *Configuring VRRP-A High Availability*.

Enhancements in ACOS 5.2.1-P1

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1-P1 release:

The following topics are covered:

Carrier Grade NAT

ACOS 5.2.1-P1 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

The following topics are covered:

Increased Custom Attributes Length for RADIUS attributes

The length of the custom attributes for RADIUS entries is increased from 32 bytes to 64 bytes.

For more information, see IPv4-to-IPv6 Transition Solution Guide

Gi or SGi Firewall

ACOS 5.2.1-P1 introduces the following new features and enhancements for Gi or SGi Firewall:

NOTE: For more information, refer *Firewall Configuration Guide*.

The following topics are covered:

Support for Persistent Storage of Firewall Security Logs

With this enhancement, storing the firewall security logs is possible in Thunder appliances when the connection to syslog servers is down. When the remote log server is available again, the persisted logs and the subsequent real-time logs are sent to syslog servers.

Known Limitations

- IPv6 is not supported.

- Partition is not supported for TCP log servers.
- Specified source address is not supported.
- Hashing is not supported.

CLI Configuration

The local-logging can be configured under `acos-events`.

```
ACOS(config)#acos-events local-logging
ACOS(config-local-log)#rate-limit 20
ACOS(config-local-log)#max-disk-space 150
ACOS(config-local-log)#enable
ACOS(config-local-log)#delete-old-logs-in-disk
```

GUI Configuration

To configure GUI, go to **System> Setting > ACOS Event**.

GTP Firewall

ACOS 5.2.1-P1 introduces the following new features and enhancements for GTP Firewall:

NOTE: For more information, refer 'GTP Firewall' in the Firewall Configuration Guide.

The following topics are covered:

Support for GTP Inline Monitoring

Starting with ACOS 5.2.1-P1, GTP firewall can be inserted inline and set to monitor mode.

The monitor mode allows for monitoring and evaluating the traffic without dropping or altering the packets. Configuring the monitor mode and generating the reports during the initial phase of GTP deployment or when there are too many packet drops helps the operator to learn and understand the type of attacks occurring in the network before activating the full protection mode.

You can configure the monitor mode at the GTP firewall configuration level or the sub policy level. When configured at the GTP configuration level, it overrides the monitor mode configured at the sub-policy level.

Use the following command to deploy GTP in the insertion mode and enable the **monitor** mode:

```
ACOS(config)# fw gtp insertion-mode monitor
```

The `GTP messages forwarded via monitor mode` counter is incremented each time an invalid packet is forwarded. To view this counter, use the `show counters fw gtp` command.

Use the following command to change the GTP configuration from the monitor mode to the full-protection mode:

```
ACOS(config)# no fw gtp insertion-mode monitor
```

The monitor mode can be configured for the following sub policies:

- Validation Policy
- Filtering Policy
- Rate Limiting Policy
- General Policy – Supported for Maximum Message Length only

You can also configure the GTP firewall to skip state checks. When skip state checks is configured, the GTP packets without a state in an existing network are forwarded. This option is useful when a new GTP firewall is deployed in an existing network with traffic flowing through preexisting GTP tunnels and the GTP firewall does not have the necessary state to accurately track those transactions. As a result, the packets may be dropped due to the lack of state information. To prevent such drops for an existing session, you can configure **skip-state-checks** to forward packets without a state while configuring the GTP firewall for new tunnels.

Use the following command to deploy GTP in the insertion mode and enable **skip-state-checks**:

ACOS(config)# **`fw gtp insertion-mode skip-state-checks`**

The `GTP Stateless Forward` counter is incremented each time a packet is forwarded without a state. This configuration must be disabled once the Stateless Forward counter reduces to a reasonable number and the GTP firewall has a state for most of the ongoing GTP tunnels.

For more information, see 'GTP Firewall' in the *Firewall Configuration Guide*.

Support for GTP Rate Limiting Logs

You can enable logs to be generated when the packets are dropped due to GTP rate limiting at the APN-Prefix or Network Element (SGW/PGW) level. The logs are generated for the following message types:

- `gtp-v0-c-aggregated-message-type-rate`
- `gtp-v1-c-aggregated-message-type-rate`
- `gtp-v2-c-aggregated-message-type-rate`
- `gtp-v1-c-create-pdp-request-rate`
- `gtp-v1-c-update-pdp-request-rate`
- `gtp-v2-c-create-session-request-rate`
- `gtp-v2-c-modify-bearer-request-rate`

To enable logging, you must configure the log periodicity. The log periodicity can be set from 1 to 30 minutes. The following example displays how to enable log periodicity for GTP rate limiting:

```
fw gtp network-element-list-v4  myv4list log-periodicity <1-30> mins
fw gtp apn-prefix-list prefix1 log-periodicity <1-30> mins
```

The Log Event GTP Rate Limit Periodic counter is incremented every time a log is generated for GTP rate limiting. To view the GTP firewall logging counters, use the show counters fw logging gtp command.

The `custom-record gtp-rate-limit-periodic template rate-limit` command is added to configure NetFlow monitors for exporting GTP rate limiting.

The following information elements are used to configure a NetFlow template that monitors GTP rate limiting:

- information-element rate-limit-key
- information-element rate-limit-type
- information-element rate-limit-drop-count

For more information, see 'GTP Firewall' in the *Firewall Configuration Guide*.

GTP-U Inner IP Filtering

A service provider may want to prevent a subscriber from accessing some specific destinations that are forbidden due to malicious behavior or compromised equipment. Such access may expose subscribers and service provider infrastructure to security threats. Using the Threat Intel capability, the GTP firewall can block unauthorized access by dropping the packets coming from or going to such malicious destinations.

The GTP firewall leverages the Threat Intelligence module (or Threat Intel for short) that provides data about malicious IP addresses on the internet. The IP addresses of the threat actors and the forbidden destinations are collected to create a class-list. A collection of such class-lists can be used to create a Threat List. In addition, you can create a class-list with a list of malicious IPs and bind it to the threat-list.

When an IP threat list is configured, the GTP firewall matches the inner IP address of the GTP-U tunnel with the source or the destination IP addresses listed on the threat list. If the IP addresses match, the GTP firewall drops the traffic and prevents the subscriber from connecting to a malware IP address.

For more information about Threat Intel and for configuring an IP Threat List, see 'GTP Firewall' in the *Firewall Configuration Guide*.

Secure Sockets Layer Insight

ACOS 5.2.1-P1 introduces the following new features and enhancements for Secure Sockets Layer Insight (SSLi):

NOTE: For SSLi configuration steps, refer *SSL Insight Configuration Guide*. Similarly, for SSLi specific CLI commands, refer *Command Line Reference for ADC Guide*.

The following topics are covered:

Custom CA Support

When ACOS starts SSL connection with the remote server, it utilizes SCV (Server Certificate Verification) function to verify the remote server's certificate through OCSP response and CRL. SCV works effectively when the remote server's certificate is issued by the public CA. This function is now extended for custom CA as well.

ECDSA Certificates Support over Nitrox V (N5) Platform

SSLi supports both RSA and ECDSA certificates based on OpenSSL 1.1.1 over 'QAT' and 'software-tls1.3' module modes. This feature is extended to support ECDSA on the 'N5-old' platform using OpenSSL 0.9.7. Therefore, only TLS 1.2 and earlier versions are supported.

CLI Configuration

There is no new CLI added. However, the existing CLI commands have extended to configure both RSA and ECDSA certificates.

```
ACOS(config)#slb common
ACOS(config-common)#ssl-module
ACOS(config-common)#ssl-module N5-old
ACOS(config-common)#exit
```

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# forward-proxy-ca-cert ecdsa_l3v
ACOS(config-client ssl)# forward-proxy-ca-key ecdsa_l3v
ACOS(config-client ssl)# forward-proxy-alt-sign cert ecdsa_l3v key
ecdsa_l3v
ACOS(config-client ssl)# forward-proxy-verify-cert-fail-action continue
ACOS(config-client ssl)# forward-proxy-enable
ACOS(config-client ssl)# exit
```

Platform

ACOS 5.2.1-P1 introduces the following new feature and enhancement for ACOS Platforms:

Hardware Platform Support

Thunder 7655(S) has been introduced as the newly-supported hardware platform in the ACOS 5.2.1-P1 release. For more information on the complete list of supported hardware Platforms,refer *Hardware Platforms Support* in *Release Notes*.

Enhancements in ACOS 5.2.1

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.1 release:

The following topics are covered:

aFlex

ACOS 5.2.1 introduces the following new features and enhancements for aFlex.

NOTE: For more information, refer *aFleX Scripting Language Reference*.

The following topics are covered:

aFlex Header Command Supports SIP Virtual Port

The IP, UDP, and TCP aFleX command now supports SIP virtual port functionality. With this feature, ADC uses an IP gateway for SIP security and overcomes fraud issues from VoIP service.

The following aFleX commands and events are provided:

IP commands:

- IP::addr
- IP::client_addr
- IP::local_addr
- IP::protocol
- IP::remote_addr
- IP::server_addr
- IP::stats
- IP::tos
- IP::ttl
- IP::version

TCP Commands:

- TCP::client_port
- TCP::close
- TCP::collect
- TCP::local_port
- TCP::mss
- TCP::offset
- TCP::option
- TCP::payload
- TCP::remote_port
- TCP::respond
- TCP::rtt
- TCP::server_port

UDP Commands:

- UDP::client_port
- UDP::local_port
- UDP::payload
- UDP::remote_port
- UDP::respond
- UDP::server_port

IP, TCP, and UDP Events:

- CLIENT_ACCEPTED
- CLIENT_CLOSED
- CLIENT_DATA
- SERVER_CLOSED
- SERVER_CONNECTED
- SERVER_DATA

lwnode Command Support in TCP Proxy Virtual Port

The existing 'lwnode' aFlex functionality is now implemented in CLIENT_DATA under TCP proxy virtual port. This feature will then utilize the RESOLVE::Lookup command and enable Server Name Indication (SNI) to perform 'A' lookups.

Application Access Management

ACOS 5.2.1 introduces the following new features and enhancements for Application Access Management (AAM):

NOTE: For AAM specific configuration steps, refer *Application Access Management Guide*.

The following topics are covered:

AAM Support Cookie Attributes

To enhance the cookie attributes security, three new attributes are added under AAM authentication template. You can configure this feature using both CLI and GUI.

- Cookie Secure - The secure cookie can only be transmitted over an encrypted connection.
- Cookie Http only - The http-only cookie cannot be accessed by client-side APIs, such as Javascript.

- Cookie Samesite - The samsite cookie mitigates cross-site request forgery (XSRF) attacks.

CLI Configuration

```
ACOS(config)# aam authentication template <name>
ACOS(config-auth template:a1)# cookie-secure-enable
ACOS(config-auth template:a1)# cookie-httponly-enable
ACOS(config-auth template:a1)# cookie-samesite <strict / lax / none>
```

GUI Configuration

To enable cookie attributes, go to **AAM > Polices and Templates > Authentication Template**.

AAM User ID information in the SSLi logs

With this release, the SSLi logs will include AAM user ID information. It will provide details about the users, which was not available previously as SSLi logs were not correlated with AAM access.

Allow Authentication Method Fallback Chain

An enhancement is implemented to try multiple authentication methods if the preferred authentication method fails while creating an authentication profile. This feature provides a higher authentication success rate and eases policy configuration. The authentication methods chaining for fallback is beneficial on networks with multiple client operating systems.

CLI Configuration

```
ACOS(config)# aam authentication template <template-name>
ACOS(config-auth template:template-name)# logon <logon-name>
ACOS(config-auth template:template-name)# chain server <server-name>
priority <1-5>
ACOS(config-auth template:template-name)# chain service-group <sg-name>
priority <1-5>
```

GUI Configuration

To enable this feature, go to **AAM > Policies and Templates > Authentication**

Templates.

Authentication Session Resource Limit Enhancement

The maximum authentication session limit's default value is currently set to 102400 per partition regardless of system memory. This value can now be set based on the available system memory to optimize system resource usage.

CLI Configuration

```
ACOS(config)# aam resource-usage auth-session-count <6400-12800>
```

GUI Configuration

To enable this feature, go to **System > Setting > Resource Usage**.

OAuth 2.0 and OpenID Connect Support

With this release, AAM supports Open ID connect identity layer along with OAuth 2.0 protocol for user authentication and authorization. It extracts user information or forwards the authorization token to the backend server to identify the users and the authorization parameters.

The following functionalities are provided:

- OpenID Connect works as an OpenID Connect Relying Party with OpenID Providers and the OAuth 2.0 works as an OAuth client.
- OpenID Connect and OAuth 2.0 supports the following authorization grant types:
  - Authorization Code
  - Implicit
  - Hybrid

CLI Configuration

```
ACOS(config)# aam authentication oauth authorization-server <NAME>
ACOS(config)# aam authentication oauth client <NAME>
ACOS(config)# aam authentication relay oauth <NAME>
ACOS(config)# show aam authentication statistics oauth
ACOS(config)# show aam authentication statistics oauth-relay
```

GUI Configuration

To enable this feature, go to:

- **AAM > Authentication Client > OAUTH > Authorization Server**
- **AAM > Authentication Client > OAUTH > Client**
- **AAM > Authentication Relay > OAUTH**
- **AAM > Global Stats > OAUTH Stats**

reCAPTCHA Challenge Authentication Support

AAM now supports the reCAPTCHA challenge service from Google to improve security and protect against brute force password hacks. It also supports Google's reCAPTCHA web service and AAM flexible advanced customization to add challenges in the form-based logon and works with the authentication and authorization methods supported by AAM.

The CAPTCHA challenge blocks the automated password guessing attacks, followed by temporary account lockout after several authentication failures.

CLI Configuration

```
ACOS(config)# aam authentication captcha <name>
ACOS(config)# captcha-variable <captcha_var_name>
ACOS(config)# aam authentication captcha <name>
ACOS(config)# captcha <captcha_profile>
ACOS(config)# attribute {1..32} <attr_name> attr-type number {equal |
not-equal | less-than | more-than | less-than-equal-to | more-than-
equal-to} <num>
ACOS(config)# captcha-authz-policy <authz_policy>
```

GUI Configuration

To enable this feature, go to:

- **AAM > Auth Clients > Portal > Logon**
- **AAM > Auth Clients > Logon Form**
- **AAM > Authentication > Templates**

- **AAM > Authorization Policies > Update > Attributes**
- **AAM > AAA Policies > Update > Rule 1**

Re-authentication Support for Browser

When the cookie max-age is set to '0' the authentication session is valid till the browser is closed or the authentication session on ACOS is removed or timeout. Hence, you must re-authenticate to access the ACOS again. The Cookie Max-Age can now be configured from ‘0-2592000’.

SAML Bad Request Redirect URL

From this release, the SAML service providers can configure the Bad Request Redirect URL. This feature will redirect the users to the 'Bad Request' page instead of displaying a '403 Error' page.

This URL can be configured using both CLI and GUI.

CLI Configuration

```
ACOS(config)#aam authentication saml service-provider sp1
ACOS(config-SAML service provider:sp1)#bad-request-redirect-uri Specify
URL to redirect
```

GUI Configuration

To configure the URL, go to **AAM > Auth Clients > SAML Service Providers**.

Application Delivery Controller

ACOS 5.2.1 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for ADC specific CLI commands, refer *Command Line Reference for ADC Guide*.

The following topics are covered:

aFlex Table Synchronization Support by VRRP-A

The aFlex table maintains more than 1000 entries in a hash table for the ACOS system. In the VRRP-A cluster scenario, this table may get deleted during the upgrade, reboot, or failure. Therefore, to avoid creating this table manually, the aFlex table synchronization method is implemented through VRRP-A. This feature sends the table information to the standby ACOS device in real-time and can easily be retrieved.

You can enable this feature using both CLI and GUI.

CLI Configuration

Following new commands are available under SLB common:

```
ACOS(config)# slb common
ACOS(config-common)# aflex-table-entry-aging-interval <1-3600>
ACOS(config-common)# aflex-table-entry-sync enable
ACOS(config-common-aflex-table-entry-sync)# max-key-len 50
ACOS(config-common-aflex-table-entry-sync)# max-value-len 100
ACOS(config-common-aflex-table-entry-sync)# min-lifetime 3600
```

Following new commands are available under Virtual Port:

```
ACOS(config)# slb virtual-server vslb1
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# aflex-table-entry-sync enable
```

Following show commands are updated to include the new feature information:

```
ACOS(config-web-category)#show vrrp-a statistics
ACOS (config)# show aflex debug table
```

GUI Configuration

To enable aFlex Table Synchronization feature, go to:

- **ADC > SLB > Global**
- **ADC > SLB > Virtual Servers > Virtual Ports**

ADC supports ACK Flood DDoS Attack Protection

This feature enhances ACK flood DDos attack prevention for ADC.

ADC supports Proxy Protocol

Proxy Protocol is an internet protocol that conveniently transmits client information such as protocol, source IP, destination IP, source port, destination port, etc. by adding a small header into the TCP. ADC solution now supports the proxy protocol feature, which helps you identify the client's IP address when the load balancer uses TCP for back-end connections.

This protocol supports two header formats:

- Version 1 - a human-readable (ASCII string) format
- Version 2 - a binary format

CLI Configuration

To enable the proxy protocol option, use **`proxy-header insert`**.

```
ACOS(config)# slb template tcp-proxy TP
ACOS(config-tcp proxy)# proxy-header insert {v1 | v2}
```

Attack Detection and Prevention using ZBAR

The ADC has combined multiple infrastructural capabilities to create an enhanced solution that identifies volumetric and IOT DDoS attacks on the SLB virtual port. It employs mitigation policies to provide excellent application responsiveness for the good sources. The bad sources are dropped or rate-limited based on their computed threat score. The 'attack-detection' command needs to be set to enable this feature.

This solution employs the following infrastructure capabilities:

- Analytics infrastructure – It adaptively baselines multiple traffic metrics and derives attack thresholds..
- ZBAR (Zero Day source behavior Attack Recognition) infrastructure - It infers and classifies the type of attack from source behavior. It identifies the bad sources based on multiple metrics to profile source behavior anomalies.
- • Packet capture infrastructure – It automatically captures a few packets from the deemed attackers and stores them as evidence, for signature extraction and further analysis.

Known Issues

- Increases CPU utilization
- Increases memory utilization
- Reduces session capacity

CLI Configuration

- To enable this feature, refer the following configuration:

```
ACOS (config)# slb virtual-server vip1 12.12.12.203
ACOS (config-slb vserver)# port 80 tcp
ACOS (config-slb vserver-vport)# attack-detection
```

- To view the ZBAR information, refer the following show commands:
  - `show visibility zbar dest`
  - `show visibility zbar dest bad-sources`

Built-in Solution for Health Monitor DNS Method

ACOS supports various health monitor methods. One of which is the DNS method to monitor the DNS services running status accurately. This method is currently executed using an external shell script, which often causes higher memory and CPU consumption.

As a solution, a build-in mechanism is implemented to monitor the DNS services and support IPv4, IPv6, and FQDN expectations. This feature also captures debug and error messages for better debugging.

Known Limitations

- DNS truncated is not supported
- DNS response length limit for TCP is 65535 bytes and for UDP is 4096 bytes (EDNS)
- SOA and TXT record type is not supported hence will be ignored

CLI Configuration

Following new **expect** parameters are available under **method dns domain**:

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)# method dns domain <domain-name> expect
{ipv4-addr <ipv4 address> | ipv6-addr <ipv6 address> | FQDN <fqdn>}
```

Following new **expect** parameter is available under **method dns ipaddress**:

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)# method dns ipaddress {ipv4 address | ipv6
address} expect FQDN <fqdn>
```

GUI Configuration

To enable expect option, go to **ADC > Health Monitors > Method Type > DNS**.

Clone Option for ADC Components

This feature was implemented in ACOS 4.1.4-GR1-P3 and is now implemented in this release.

The following ADC components supports clone option to duplicate the instance or clone the component.

NOTE: This feature is supported only on GUI and not in CLI or aXAPI.

- Virtual Server
- Virtual Service
- Service Group
- Server

DNS with Response Policy Zone support

The DNS Response Policy Zone (RPZ) feature is introduced to block malicious hosts, sites, domain names, IP addresses, and mitigate the malformed DNS queries. You can build a DNS firewall using DNS Response Policy Zones (RPZ).

The DNS RPZ acts like a DNS zone and uses a customized policy with firewall rules in the DNS servers. Each rule is stored in a DNS resource record set (RRset) or resource records (RRs) and consists of a trigger and a corresponding action. The response behaviour can be controlled like an error reply, a Walled Garden IP, or dropped packets to protect the backend and the client.

ACOS can import customized RPZ and supports all its policy, including five triggers and six actions. ACOS applies the RPZ policy rules when DNS transactions occur at the virtual port.

CLI Configuration

To import the RPZ file, use the following command:

```
ACOS(config)# import rpz A10.rpz use-mgmt-port
scp://root@192.168.93.182/root/A10.rpz
```

To bind the RPZ to the DNS template, use the following command:

```
ACOS(config)# slb template dns dns_template1
ACOS(config-dns)# rpz 1 A10.rpz
ACOS(config-dns-rpz)# logging enable
ACOS(config-dns-rpz-logging:enable)# rpz-action drop
```

```
ACOS(config-dns-rpz-logging:enable)# rpz-action tcp-only
```

Additionally, the following show commands are introduced to display RPZ configurations and statistics:

- **show rpz <file>**
- **show dns statistics**
- **show slb virtual-server <vip-name> <port_number> dns-udp/dns-tcp application-statistics**

DNS over TLS Support on Layer 7

The existing DNS over TLS (DoT) ADC feature is enhanced to support the Layer 7 DNS Application Protocol for better security and encryption. The following features are available:

- Extensions Mechanisms for DNS (EDNS(0)) Padding - This allows DNS clients and servers to artificially increase the DNS message size by a variable number of bytes. You can define the maximum message length to limit the EDNS(0) options space along with the Block-length and Random-Block-length padding.
- Client Subnet in DNS Queries - This allows recursive resolvers to forward original network information from which a query is sent when interacting with the other nameservers.
- Bind UDP service group - This allows binding UDP service group, if the virtual port is DNS-TCP. Previously, only TCP service group binding was supported.

CLI Configuration

The following new commands are available under DNS Template:

- add-padding-to-client - To add the EDNS(0) padding to the client if the client-SSL is configured.
- remove-padding-to-server - To remove the EDNS(0) padding to the server.
- remove-edns-csubnet-to-server - To remove the EDNS(0) client subnet from the client queries.
- udp-retransmit - To re-transmit the UDP packet if the server didn’t come back after the specified time i.e. when the client is TCP and the backend is UDP.

NOTE: These options are for DNS-TCP and/or DNS-UDP ports only. UDP ports are not supported.

Example:

```
ACOS (config-dns)#add-padding-to-client {block-length | random-block-length}
ACOS (config-dns)# remove-edns-csubnet-to-server
ACOS (config-dns)# remove-padding-to-server
ACOS(config-dns)# udp-retransmit {max-trials | retry-interval}
```

The following new commands are available under Virtual Server:

```
ACOS (config)# slb virtual-server VIP1 1.2.3.4
ACOS (config-slb vserver-vport)# port 853 dns-tcp
ACOS (config-slb vserver-vport)# extended-stats
ACOS (config-slb vserver-vport)# source-nat pool nat1
ACOS (config-slb vserver-vport)# service-group DoT <backend is TCP>
ACOS (config-slb vserver-vport)# template dnsDNS_Test
ACOS (config-slb vserver-vport)# template client-sslSSLInsight_ClientSide
ACOS (config-slb vserver-vport)# template server-sslSSLInsight_ServerSide
```

GUI Configuration

- Under **ADC > SLB > Virtual Server > Virtual Port > Protocol > DNS-TCP**:
  - Bind TCP Service Group
  - Bind **Template Client-SSL** and **Template Server-SSL**
- Under **ADC > L7 Protocols > DNS Templates**:
  - Remove EDNS(0) Padding To Server
  - Add EDNS(0) Padding To Client > Block-Length and Random-Block-Length
  - Remove EDNS(0) Client Subnet From Client Queries
  - UPD Retransmit Policy
  - Retry Interval Value
  - Max Trial Value

ECMP Support

This feature was implemented in ACOS 4.1.4-GR1-P3 and is now implemented in this release.

ECMP (Equal-cost multi-path routing) protocol is a routing strategy where next-hop packet forwarding to a single destination can occur over multiple best paths, which tie for top place in the routing table.

This feature allows connection information (source IP, source port, destination port from the forward tuple, and real server IP) hashing. The routes would be more balanced as the number of unique hashes would increase significantly.

CLI Configuration

```
ACOS(config)# slb common
ACOS(config-common)# ecmp-hash [system-default | connection-based]
```

GUI Configuration

To enable **ECMP** option go to **ADC > SLB > Global**.

Low Latency Support

The low latency feature is already available in the ACOS legacy releases. This feature is now implemented in this version, along with the following enhancements:

- Support fast-path, basic TCP, and FIX IPv4 traffic
- Support hardware forwarding for established sessions
- Support physical platforms with Ternary content-addressable memory (TCAM) hardware

The 'low-latency' command is available under SLB common configuration mode commands.

CAUTION: This configuration is allowed only in the shared partition as it affects the entire system. Hence, you must reboot the ACOS device after configuration.

CLI Configuration

```
ACOS(config)# slb common
ACOS(config-common)# low-latency
```

GUI Configuration

To enable **Low Latency** option, go to **ADC > SLB > Global**.

Next-Hop Pool Support

This feature was implemented in ACOS 4.1.4-GR1-P3 and is now implemented in this release.

ADC will support alternative next-hop IP address when one of the firewall or router devices fail. The next-hop pool contains the list of valid next-hop firewall or router IP addresses for ADC.

This feature also validates the return of next-hop (MAC address) if it is defined in the 'use-rcv-hop-resp' next-hop pool. The health check will monitor the firewall or router paths heath and learn all the MAC addresses of the next-hop firewall or routers.

The 'server-group' option is available under a virtual port to enable this feature. And it is configured along with the 'use-rcv-hop-resp' option.

CLI Configuration

```
ACOS(config)#slb virtual-server to-vpn
ACOS(config-slb vserver)#port 0 tcp
ACOS(config-slb vserver-vport)#service-group to-vpn-tcp
ACOS(config-slb vserver-vport)#use-rcv-hop-for-resp
ACOS(config-slb vserver-vport)#server-group to-vpn
ACOS(config-slb vserver-vport)#no-dest-nat
```

GUI Configuration

To enable **Next Hoppool** option go to **ADC > SLB > Virtual Servers**.

'no-dest-nat' Feature Enhancement

This feature was implemented in ACOS 4.1.4-GR1-P3 and is now implemented in this release.

The 'no-dest-nat' existing feature under virtual-server checks whether the same service-group is bound to another virtual-server and prevents the user from configuring this feature. However, in some cases, the user may want to bind one service-group under multiple virtual-server with 'no-dest-nat' feature enabled. To accommodate such requirement, a new 'service-group-on-no-dest-nat-vport' option is implemented in CLI, aXAPI, and GUI.

Known Limitations

Health check operating in DSR mode is incompatible if a user enables 'dsr-health-check-enable' and binds same service-group on multiple 'no-dest-nat' virtual ports.

NOTE: If you are upgrading from 4.1.1-P11 or older release, and already have this configuration then contact A10 support prior to upgrade. To avoid impact, it is recommended to schedule downtime during the upgrade from legacy versions. And, this configuration must be updated after the upgrade.

CLI Configuration

```
ACOS (config)# slb common
ACOS (config-common)# service-group-on-no-dest-nat-vports [allow-same | enforce different]
```

GUI Configuration

To enable **Service Group Binding on no-dest-nat Vports**option go to **ADC > SLB > Global**.

Recursive DNS Lookup Support

ACOS supports recursive DNS lookup function with limited DNS request types. This feature is extended to support the data plane and all the DNS request types. The enhancement adds data plane functionality to the existing local-dns-resolution feature. It helps to rapidly provide the response to the client without communicating with any other DNS servers.

This feature will be used in the following two scenarios:

- If there are no servers available to respond to client's DNS query (servers down due to health check)

- If the DNS server in the service-group bound to the virtual port responds to client's query without a matching record.

NOTE:

- When this feature is enabled on a DNS template and is bound to the virtual port, then the virtual port is marked functional up, even if there are no servers up due to health check in the service-group.
- This feature is supported only on 'dns-udp' and 'dns-tcp' type virtual server ports.

You can enable this feature from the DNS template using both CLI and GUI.

CLI Configuration

To enable the recursive DNS resolver, use **recursive-dns-resolution**

```
ACOS(config)# slb template dns dns1
ACOS(config-dns)# recursive-dns-resolution [hostnames | ipv4-nat-pool |
ipv6-nat-pool]
```

GUI Configuration

To enable the recursive DNS resolver, go to **ADC > Templates > L7 Protocols > DNS**.

Reuse NAT IP Port with Unique 4-tuple Flow

This feature was implemented in ACOS 4.1.4-GR1-P3 and is now implemented in this release.

ACOS supports the utilization of IP NAT pool with Smart NAT (SNAT) for more than 65535 concurrent connections and functions like a Smart NAT (SNAT) for high capacity usage of NAT port resources.

Known Limitation

Only one 4-tuple NAT pool can be active per remote port.

CLI Configuration

- To configure unique 4-Tuple, configure the NAT to NAT IP in SNAT-Pool flow using

the ip nat pool command and bind it to the virtual port.

```
ACOS(config)# ip nat pool pool2 121.116.10.99 121.116.10.99
121.116.10.99 netmask /24 port-overload
ACOS (config)# slb virtual-server NAT1 60.1.1.62
ACOS (config-slb vserver-vport)# port 1 udp
ACOS (config-slb vserver-vport)# source-nat pool 121.116.10.99
ACOS (config-slb vserver-vport)# service-group sg1-udp
```

- To view IP NAT related statistics, use 'show slb server rs ip-nat-stats' command

GUI Configuration

- To enable **IPv6 NAT Pool** option go to **ADC > IP Source NAT > IPv6 Pools**
- To enable **IPv4 NAT Pool** option go to **ADC > IP Source NAT >IPv4 Pools**.

NOTE: You cannot edit both the IPv4 and IPv6 pools on GUI.

Carrier Grade NAT

ACOS 5.2.1 introduces the following new features and enhancements for Carrier Grade NAT (CGN or CGNAT):

The following topics are covered:

DDoS Protection Logging Enhancement

Event logging for DDoS Protection has been enhanced to send the logs to the logging servers as follows:

- Local—Logs are sent to the local buffer and can be viewed using the show log command.

- Remote—Logs are sent to the remote syslog server and IPFIX collectors.
- Both—Logs are sent to both local buffer and remote servers.

The log protocols supported are Syslog and NetFlow. Both CEF and ASCII formats are supported for Syslog. The ‘show counters cgnv6 logging’ and ‘show cgnv6 logging statistics’ commands include additional iDDoS (L3 and L4) Entry Creation and Deletion counters and statistics respectively.

For more information, refer:

- 'Enabling Logging for DDoS Protection’ in *IPv4-to-IPv6 Transition Solutions Guide*, to enable the DDoS Protection logging feature
- Traffic Logging Guide, to view the log samples
- Command Line Reference for CGN, to view logging statistics and counters

Reduce Minimum Value on Rule Port-mapping Interim Update

The interim update interval for the rule port-mappings interim-update parameter is changed from 30-120 minutes to 15-120 minutes. The minimum value is reduced to send the interim log messages every 15 minutes.

GUI Configuration

The supported value for the Log Interim Update Interval of NAT Mappings is changed from 30-120 minutes to 15-120 minutes.

For more information, refer *Command Line Interface Reference for CGN* and *Online Help*.

VRID and User-Group level Statistics

For VRRP-A and ScaleOut cluster, the global T1 level statistics currently display per technology per partition. The granularity of these statistics is now extended to include per VRID (VRRP-A) and per User-group (ScaleOut) levels information by introducing the following show commands:

- show counters cgnv6 fixed-nat per-instance
- show counters cgnv6 lsn per-instance

These show commands support the following CGN technologies,

- Fixed NAT 44
- Fixed NAT 64
- Fixed NAT DS-Lite
- LSN NAT 44
- LSN NAT 64
- LSN NAT DS-Lite

NOTE:

- The existing T1 level statistics are unchanged.
- The first instance i.e., instance 0 is allocated by default once a Fixed-NAT or an LSN pool is configured even if it is tied to a VRID/User-group that is greater than 0.

Gi or SGi Firewall

ACOS 5.2.1 introduces the following new features and enhancements for Gi or SGi Firewall:

NOTE: For more information, refer *Firewall Configuration Guide*.

The following topics are covered:

DDoS Protection Logging Enhancement

Event logging for DDoS Protection has been enhanced to send the logs to the logging servers as follows:

- Local—Logs are sent to the local buffer and can be viewed using the show log command.
- Remote—Logs are sent to the remote syslog server and IPFIX collectors.
- Both—Logs are sent to both local buffer and remote servers.

The log protocols supported are Syslog and NetFlow. Both CEF and ASCII formats are supported for Syslog. To support DDoS (L3 and L4) Entry Creation and Deletion in NetFlow, the following new custom templates have been added:

- cgn-ddos-l3-entry-creation
- cgn-ddos-l3-entry-deletion
- cgn-ddos-l4-entry-creation
- cgn-ddos-l4-entry-deletion
- fw-ddos-entry-creation
- fw-ddos-entry-deletion
- fw-session-limit-exceeded

The 'show counters netflow monitor test' is enhanced to include the additional custom NAT iDDoS Entry Records counters. The show commands such as ‘show counters cgnv6 logging’ and ‘show cgnv6 logging statistics’ include additional iDDoS (L3 and L4) Entry Creation and Deletion counters and statistics respectively.

You can configure the radius attributes for rate limiting to be included in the logs under the firewall template logging configuration.

- For enabling the DDoS Protection logging, configuring the radius attributes for rate limiting, and viewing the log samples, see ‘Firewall Logging’ in the *Firewall Configuration Guide*.
- For NetFlow changes, see *Traffic Logging Guide*.

DSCP Match Rule

The firewall rules are configured to match traffic based on source IP, destination IP, source port, destination port, and protocol. This feature is enhanced to support rules that match traffic based on the Differentiated Services Code Point (DSCP) value in the IP header.

The IP header (IPv4 and IPv6) six DSCP bits contain packet classification information used in the firewall rule as a match criterion. When a session matches this new rule, all the session packets are treated the same way. Additionally, the existing actions such as Deny, Permit, Reset, and Log apply to this rule as well.

CLI Configuration

The following example demonstrates multiple DSCP configurations to match traffic with the DSCP value in IPv4 header:

```
rule-set dscp
rule 1
action permit
source ipv4-address any
source zone any
dest ipv4-address any
dest zone any
service any
dscp af23
dscp cs6
dscp range 30 40
dscp range 10 20
application any
!
```

GUI Configuration

To configure a rule to match DSCP values, go to **Security > Firewall > Rulesets > Rule > DSCP List**.

Enhanced Action Group CLI

A new “action-group” CLI command has been introduced for configuring complex action behaviors on the matching traffic. In addition to configuring all the actions that can be done using the action CLI command, the action-group CLI command enables you to bind a rate limiting policy to a rule and configure a respond-to-user-mac action.

The action and the action-group CLI commands are mutually exclusive. You can either configure an action or an action-group for a rule.

Firewall Log Enhancement for Threat-Intel

The existing Firewall logging feature is enhanced with the threat category fields to track suspicious traffic detected by Threat-Intel. This feature is available in the Firewall logs and GUI.

The following fields are added to the Syslog, ACOS event log, and Application Firewall local log:

- Source Threat List
- Destination Threat List
- Source Threat Category
- Destination Threat Category

GUI Configuration

The following chart options are available in the **Security > Firewall > Dashboard**:

- Top 10 Destination Threat Categories - Bytes
- Top 10 Destination Threat Categories - Connections

Rate Limiting Enhancement

The Rate Limiting feature has been enhanced to support the following:

- Rate Limiting can be applied to the traffic coming from certain application protocols and categories. Rate limiting is applied only after the application is classified.
- Rate limiting features such as Packets-Per-Second (PPS), Throughput, and Connections-Per-Second (CPS) are supported on Gi firewall and transparent firewall sessions for both IPv4 and IPv6 traffic.
- Rate Limiting can now be applied to the traffic at the rule level. For example, if you have configured PPS total as the rate-limiting policy, the PPS rate limiting is applied to the aggregate traffic matching the rule.

Global License Manager

ACOS 5.2.1 introduces the following new feature and enhancement for Global License Manager (GLM):

For more information, refer *GLM Perpetual Licensing Guide*.

Quick Trial License

A10 Networks offers a trial license for a number of its appliances. An ACOS user can easily request licenses, using a new or existing GLM account. If the Unique User ID is available on a GLM organization, ACOS provides a license or trial for that organization. Users from a different organization can also request a license. A new user is created for the username and organization along with a trial license ID.

Request Add on Licenses from ACOS

ACOS has 3rd party add on licenses which offer 90 day trial periods. It is possible to request a trial or permanent license and can be initiated from the ACOS CLI or management GUI.

User can request a license by clicking a Request Trial button on GUI. The license will be issued immediately, and installed so that trial can begin right away

This quick trial license is valid for ACOS Thunder Hardware, VM-vThunder and Container Thunder.

However, the IPSEC VPN license is provided only after approval by system administrator.

The 90 day trial license is available for:

- Web URL Classification and Reputation License
- IP Threat Intelligence License
- Application Visibility License

Web URL Classification and Reputation License

Web URL Classification and Reputation enables web traffic to be classified into one or more web categories and given a reputation index. Security policies based on web classification and reputation may be defined to deny, decrypt, inspect, proxy, steer, or log. Example web categories include financial services, health and medicine, bot-nets, and malware. Reputation index indicates whether the URL is trustworthy, low risk, medium risk, suspicious or high risk.

IP Threat Intelligence License

IP Threat Intelligence enhances firewall capabilities by blocking incoming and outgoing connections to known malicious sites. It may also be used to identify compromised hosts within the network. Malicious IP addresses are categorized by attack type and are dynamically updated to adapt to a changing threat environment.

Application Visibility License

Application Visibility enables traffic to be classified by a combination of deep packet inspection and behavior analysis. Application security policies provide control over individual or groups of similar applications permitted to use the network. Applications are identified and categorized into groups such as peer-to-peer, multimedia, social networking, and anonymizers. Periodic updates allow evolving and new applications to be identified.

The following functions are available when license is enabled:

- Trial licenses can be requested and immediately obtained only if they have never been issued before for the used device.
- Trial license requests can be initiated from Thunder CLI, GUI or ACT GUI
- For vThunder or cThunder, a trial can be requested.

- Trial license request can be initiated from Harmony to Thunder.
- Thunder license request does not require Thunder administrator to login to the GLM.

ACOS records the unique device ID/Serial number, model, that is requesting the license, the IP address, GLM account, time of license request, time of license issue, type of request (initiated by Thunder), type of license, and then provides the trial license.

- Thunder administrator can create a GLM account if one doesn't exist already only from Thunder hardware device.
- Thunder administrator can create a GLM account from Thunder and make a license request so GLM GUI need not be accessed.
- Thunder administrator can use an existing GLM account as well.

Request IPsec VPN License from Thunder

Customers can request and obtain trial licenses from the ACOS device directly from Thunder ACOS CFW. Customers can request the trial license for IPSEC VPN, but it must be approved by A10 Sales and Purchase. The IPsec VPN license must be requested before it can be used and is available for vThunder and cThunder trial licenses.

To get an IPSEC VPN license:

- The user must submit a request to A10 SOA or approver be processed.
- License must be approved by A10 before it can be issued to user.
- IPsec VPN license requests must be sent to approvers.
- Once IPsec VPN license is approved and issued, the device will automatically update and download the license if it is connected to the internet.

GUI Configuration

There is a new **License Type** option under the **Request a License** pop-up, added to the **ACOS > System > Admin > Licensing** page as part of the “Quick Trial License” feature. User can request a license by clicking a **Request Trial** button on GUI. The license will be issued immediately and installed so that trial can begin right away.

The following sub-options are provided related to this functionality:

- When user tries to **Request Quick Trial License**, any of the following License Status messages are displayed:
  - “GLM connection failed”
  - ”Account not found for this ACOS device”
  - “Found GLM account”
- If license status is **GLM connection failed**, user can click **Settings** button, perform change in settings and click Retry button.
- If license status is **Account Not Found**, user can click **Create New Account** to create one new account and request license or Account Lookup button to search for existing account.
- If license status is **Found GLM account**, user can click **Use This Account** to get the trial license or **Use a Different Account**.

Global Server Load Balancing

ACOS 5.2.1 introduces the following new feature and enhancement for Global Server Load Balancing (GSLB).

NOTE: For more information, refer *Global Server Load Balancing Guide*.

FQDN Partial Matching Support

Currently, a wildcard FQDN works when the exact octet DNS query matches. Now, the FQDN partial match support is built for cloud applications. This feature provides better resolution for the domain names and avoids aflex rules creation, which are hard to maintain and extend as a service.

The supported functions are:

- Starts-with
- Ends-with
- Contains

Harmony Controller Integration

ACOS 5.2.1 introduces the following new features and enhancements for Harmony Controller (HC) Integration:

NOTE: For more information, refer *Harmony Controller Integration Guide*.

The following topics are covered:

DNS/GSLB Analytics on Harmony Controller (HC)

This feature is an enhancement to collect display DNS logs and provide analytic display for DNS type Virtual port and GSLB functions. This display is now provided on HC as well. The client must be registered to HC for this feature to function correctly. For more information, refer Harmony Controller Documentation Site.

The following information is exchanged for interaction between ACOS and HC DNS App, The DNS collection metrics have the protocol support for DNS-TCP and DNS-UDP. The following information is collected:

- Logging and Debugging statistics
- Messages for statistics and logging
- Show command information for tech-support
- Support for system and network management (for example, CLI, Web UI, SNMP, aXAPI)

ACOS Thunder device sends out the log and metrics to HC to analyze the application data. The ACOS application log contains the connection information and sends the following action logs:

- Response return
- Query drops

- Query time-out
- Response from cache or GSLB

DNS query information is sent out to HC as logs and analytics display for DNS type virtual port, in the following situations:

- DNS request time out
- DNS response incoming
- DNS response by the cache
- DNS response by GSLB

When the client registers HC successfully, Thunder device or ACOS sends out telemetry (logs/metrics) for HC and DNS app. HC can be used to:

- analyze the server traffic flow
- to deploy the DNS service
- Check server request type and class
- Check how the server returns information to the client

The following commands in ACOS have been enhanced to display additional information when extended-statistics are configured under globally or under virtual port.

- show dns stats
- show slb virtual-server <server_name> <port_number> [dns-udp/dns-tcp] application-statistics

The following analysis charts or reports are displayed on HC from the collected DNS/GSLB statistics:

- QPS with Query Types
- List of top clients sending DNS Requests for various filters
- List of the top Query Domains

High Availability Active Standby and Scaleout Handover Support

The high availability of active-standby and new Scaleout statistics is implemented by CGN group to correctly export it into Harmony 5.2.

IPsec Virtual Private Network

ACOS 5.2.1 introduces the following new features and enhancements for IPsec Virtual Private Network (VPN):

NOTE: For IPsec specific configuration steps, refer *Configuring IPsec VPN* .

The following topics are covered:

GCM Ciphers Supports IKEv2

The Galois/Counter mode (GCM) is currently supported in IPsec. In this release, it will support IKEv2 Gateway encryption algorithm along with the pseudo-random function for better performance and security.

The following GCM cipher options are available:

- AES-GCM-128
- AES-GCM-192
- AES-GCM-256

IPsec Packet Distribution using VMAC

Currently, the Thunder 7650 chassis platform distributes the packet between the Primary and the Blade using one of the packet distribution rules, the VMAC rule. This

rule uses the MAC address of the floating IP with an even or odd virtual router identifier (VRID) in the following ways:

- The packet is sent to Master if the destination IP is a floating IP with even VRID.
- The packet is sent to Blade if the destination IP is a floating IP with an odd VRID.

VMAC now distributes IPsec inbound packet to the Master or Blade. To use this feature, you must configure the VRID and floating IP with VRID and use the floating IP as VPN IKE gateway's local IP.

IKE Acceleration with QAT Support

ACOS provides QAT support for accelerating IKE operations and enhances the performance of the tunnel establishment.

The following algorithms are supported:

- Diffie-hellman (DH) groups 1,2,5,14,15 and 16
- Rivest–Shamir–Adleman (RSA) certificates of 2048-bit or 4096-bit.
- Elliptic-curve Diffie–Hellman (ECDH) groups 19 (256-bit elliptic curve) and 20 (384-bit elliptic curve)
- Elliptic Curve Digital Signature Algorithm (ECDSA) 256-bit, 384-bit, and 521-bit curves

NOTE: Only new ACOS Thunder series platform models support QAT. To check the QAT support, use the 'show hardware' command.

Scaleout Support in IPsec

Scaleout support is now available for IPsec with improved efficiency in IKE/IPsec negotiations. When multiple devices work in a single cluster for IPsec the aggregate throughput increases significantly.

NOTE: The function works under IPsec stateless mode only.

Management Access and Security

ACOS 5.2.1 introduces the following new features and enhancements for Management Access and Security (MAS):

The following topics are covered:

Multi-domain LDAP Support

The LDAP feature is enhanced to support multi-domain admin authentication and authorization. You can configure the host without specifying the common name (cnattribute) or domain name.

CLI Configuration

```
ACOS(config)#authentication type ldap local
ACOS(config)#authentication mode multiple
ACOS(config)#ldap-server host 10.16.11.127 port 3268
```

GUI Configuration

To configure new 'None' option, go to **System > Admin > External Authentication > LDAP**.

Multiple Factor Authentication (MFA) for Management Plane

With this release,when the MFA is configured another authentication layer is added as a second factor, which takes client SSL certificate as input and validates it against CA root certificate which is configured in ACOS. The user can provide second factor authentication in the following ways for CLI and GUI access.

CLI Configuration

1. Enabling MFA for management plane.

```
!
system mfa-management enable
!
```

2. Configuring CA root certificate.

```
!
system mfa-validation-type
CERT CA.pem
!
```

3. For importing CA certificate CLI command is already available in ACOS and CA certificate will be stored under standard path. Command to import CA is as follows:

```
ACOS(config)# import ca-cert ?
NAME<length:1-245> CA Cert File(enter bulk when import an archive
file)
```

4. Configure Client certificate store:

```
!
system mfa-cert-store
cert-host 1.1.1.1
protocol scp
cert-store-path /here/is/cert/store
username testuser password encrypted
10AtKRhH1NQ8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
!
```

GUI Configuration

To configure MFA, go to **System > Settings > MFA**

Pre-Login Message

Starting with ACOS 5.2.1, you can set the pre-login message and display it before the user logins to ACOS GUI. To set the pre-login message, go to **System > Settings > Web**.

NOTE: String limit is 1985 characters.

For more information, refer *Online Help*.

RBA Support in GUI

The Role-Based Access (RBA) feature is now introduced in GUI. This configuration can be enabled and disabled through RBA Setting.

The feature supports the following functionality:

- Create, view, edit, and delete the users, roles and groups
- Hide and show the GUI menu based on the GUI privilege
- Show lineage dynamically, which is received from the CM object lineage list
- Canned role configuration
- RBA customization

GUI Configuration

- To configure system access, go to **System > Admin > RBA > System**.
- To configure roles, go to **System > Admin > RBA > Roles**.
- To configure user access, go to **System > Admin > RBA > Users**.
- to configure group access, go to **System > Admin > RBA > Groups**.

Network Configuration

ACOS 5.2.1 introduces the following new features and enhancements for Network Configuration:

NOTE: For more information, refer *Network Configuration Guide*.

The following topics are covered:

BGP Restart Neighbor Session After Max-Prefix Limit Reached

When the number of network prefixes that are received from a neighbor reaches the maximum configured limit, the ACOS device brings down the BGP session with the peer. Starting with ACOS 5.2.1, you can configure the restart interval to reestablish the BGP session automatically after the configured time interval.

CLI Configuration

To set the restart interval:

```
maximum-prefix NUM [ threshold ] [ restart restart-interval]
restart <1-1440>
Range is 1 - 1440 in minutes.
```

BGP, RIB, and FIB Capacity Increased for IPv4 and IPv6 on Platforms with 128G+ Memory

The IPv4 and IPv6 BGP, RIB and FIB route capacity has been upgraded for platforms with 128G and higher memory. When running the system in deployment scenarios require substantially higher route limits as follows:

- A minimum of four Control CPUs are required
- 128 GB+ platforms supported

Unnumbered IPv6 ACL Support

ACOS allows users to configure an Access List (ACL) to control the source IPv6 addresses for the control packets. IPv6 ACL’s permit action allows the source IPv6 address to pass through without any NAT action. When the source IPv6 address is not permitted, ACOS will NAT using the source IPv6 address specified under 'use-source-ipv6'.

Overlay Networks

ACOS 5.2.1 introduces the following new feature and enhancement for Overlay Networks:

NOTE: For more information, refer *Configuring Overlay Networks Guide*.

The following topics are covered:

IPv4 GRE Tunneling

ACOS GRE tunneling feature is enhanced to support IPv4 GRE tunneling with IPv4 and IPv6 payload. The GRE KeepAlive feature is also introduced to continuously monitor GRE tunnel endpoints' health and bring down the corresponding logical interface (LIF) upon failure.

The following features are provided:

- Send Syslog and SNMP trap alerts when the GRE tunnel is up or down
- View the GRE tunnel status using CLI and aXAPI
- Distribute routes based on GRE tunnel status

Known Limitations

The following functionalities are not supported in this release:

- Fragmentation for ISIS packets
- IPv6 GRE tunnels
- GRE supported for non-FTA models only

CLI Configuration

```
ACOS(config)# encap [vxlan| nvgre | gre | ip-encap]
```

GUI Configuration

To enable this feature, go to:

- **Network > Interfaces > LIFs**
- **Network > Overlay > Overlay Tunnel Vtep**
- **Network > Overlay > Overlay Tunnel Global**

IP Encap (IPinIP) Tunneling

With this release, IP encap provides support for IPinIP, IPinIPv6, IPv6inIP and IPv6inIPv6 encapsulations. Payloads of IPv4 and IPv6 can be transported atop IPv4 or IPv6 encapsulation headers. This is configured through the `ip-encap` VTEP encap.

CLI Configuration

```
ACOS(config)# encap [vxlan| nvgre | gre | ip-encap]
```

Platforms

ACOS 5.2.1 introduces the following new features and enhancements for ACOS Platforms:

The following topics are covered:

Open topic with navigation

You are here:

Hardware Platform Support

Thunder 7655(S) has been introduced as the newly-supported hardware platform in the ACOS 5.2.1 release.

NOTE: For more information on the complete list of supported hardware Platforms, refer Hardware Platforms Support.

Automated Packet Capture Enhancements

This feature was introduced in ACOS 5.2.0. In this release, it is enhanced to automatically merge pcapng files. Additionally, the advanced configuration capabilities were added to capture packets in a more detailed and efficient way.

For more information, refer *Command Line Reference Guide*.

Automated Service Discovery Support

Automated service discovery feature automates the addition of backend servers into the pool in real-time, as traffic flow increases or decreases. Also, the services are moved by the scheduler as per the resource demands.

This feature is extended to the following platforms:

- Consul
- Oracle Cloud
- Kubernetes
- VMware Center

Disk Expansion Support on Azure

Starting this release, the vThunder disk can be expanded on Azure without re-installing. It can be expanded up to 2048 GB.

Known Limitations

Disk shrink is not supported.

For more information, refer *Installing vThunder on Microsoft Azure*.

Dynamic Interface Attachment and Detachment

In virtualization and cloud platforms, dynamic interface attachment or detachment is required to make the vThunder deployment easier. ACOS supports interface attachment and detachment when the VM is running state and does not require a reboot.

NOTE: This feature is supported only on Openstack, AWS, and OCI platforms.

For more information, refer *Installing vThunder on OpenStack*, *Installing vThunder on Amazon Web Services (AWS)*, and *Installing vThunder on Oracle Cloud*.

CLI Configuration

To detect the attached or detached interface, use:

```
system probe-network-devices
```

GUI Configuration

To detect dynamically added interfaces in the vThunder, go to **System > Settings > Action**.

Extended 96 CPUs Support

Currently, FTA platform supports 96 CPUs' to achieve higher level of performance. Now, this feature is extended to support the following platforms and provide a larger form factor:

- Non-FTA
- cThunder
- Baremetal
- vThunder

Non-Dedicated Management Interface Support

In non-dedicated management port mode, there is no interface dedicated for management traffic:

- If vThunder is deployed with one vmxnet3 interface, vThunder operates in non-dedicated management mode by default.
- If vThunder is deployed with more than one vmxnet3 interface, vThunder operates in dedicated management mode by default. The first interface is the management interface, and the rest of the interfaces operate as data interfaces

Known Limitation

It is supported only on the ESXi platform.

CLI Configuration

- To display the current management interface mode:

```
#show system management-interface-mode
```

- To switch to dedicated mode:

```
# system management-interface-mode dedicated
```

- To switch to non-dedicated mode:

```
# system management-interface-mode non-dedicated
```

System Table Integrity Check Support

The system table integrity support is already available in the ACOS 4.1.4-GR1-P5. This feature is now implemented in this version. This feature checks the table integrity of the below entries:

- Address Resolution Protocol (ARP)
- Neighbor Discovery (ND6)
- IPv4 forwarding information base (FIB) address
- IPv6 address
- Media Access Control (MAC address)

Additionally, the error logs are generated for each table when the discrepancies are detected between the Master and Blade tables. For more information, refer *Command Line Reference Guide*.

SYN Cookies Support at Hardware Level

Currently, the hardware-based SYN cookies work on application levels where the partitions are deployed. The SYN cookies do not work if networks are present below the application delivery controller. This feature now supports SYN cookies at the hardware level, which will add a layer of security on boxes.

CLI Configuration

```
ACOS(config-if:ethernet:1)#ip tcp syn-cookie
ACOS(config-if:ethernet:1)#
```

Known Limitations

The following platforms are not supported in this release:

- CGN
- Firewall

Scaleout

ACOS 5.2.1 introduces the following new features and enhancements for Scaleout:

NOTE: For Scaleout specific configuration steps, refer *Scaleout Configuration Guide*.

The following topics are covered:

Minimum Nodes Number in a Cluster

Starting this release, you can configure the minimum nodes number in the cluster. When the number of active nodes is less than the minimum-nodes configuration, then the cluster stays in the waiting state. Even after reaching the minimum node requirement, the cluster may not come up if it does not match the quorum number requirement that is N/2 + 1, where N is the total number of nodes.

Scaleout Statistics

Starting this release, the counters for the show scaleout statistics are changed. The changes are as follows:

- New counters are added
- Few counters are removed
- Few counters are renamed

The old Scaleout counters were valid till ACOS 5.2.0-P1 release.

Secure Sockets Layer Insight

ACOS 5.2.1 introduces the following new features and enhancements for Secure Sockets Layer Insight (SSLi):

NOTE: For SSLi configuration steps, refer *SSL Insight Configuration Guide*. Similarly, for SSLi specific CLI commands, refer *Command Line Reference for ADC Guide*.

The following topics are covered:

Automatically Update CA Bundle File

Previously, the CA certificate was manually packaged with the ACOS device. The device administrators can use the 'automatic-update' feature to update the pre-loaded CA certificate for shared partition and maintain the up-to-date CA certificate package on the GLM server.

NOTE: To use this feature, ensure that the device is registered with the Global License Manager (GLM). For more information, refer *Global License Manager User Guide*.

CLI Configuration

- The following are the automatic-update commands:
  - `ACOS(config)#` **`automatic-update check-now`** - To immediately update the CA bundle and application firewall protocol bundle.
  - `ACOS(config)#` **`automatic-update proxy-server`** - To connect through proxy server
  - `ACOS(config)#` **`automatic-update revert`** - To manually revert to the previous version.
  - `ACOS(config)#` **`automatic-update app-fw`** - To schedule the application firewall protocol bundle automatic update.
  - `ACOS(config)#` **`automatic-update ca-bundle`** - To schedule the CA bundle automatic update.
  - `ACOS(config)#` **`automatic-update use-mgmt-port`** - To connect through management port.
- The following is the automatic-update show command:

```
ACOS(config)# show automatic-update
```

- The following command binds the CA bundle with the Client-SSL Template:

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS(config-client ssl)# ca-cert a10_autoupdate_ca partition shared
ACOS(config-client ssl)# forward-proxy-trusted-ca a10_autoupdate_ca
partition shared
```

GUI Configuration

To enable the automatic-update options, go to **Security > Firewall > Configure> Application Protocol Update**.

Certificate Pinning Candidate List Support

Certificate Pinning is a method used by certain apps to secure traffic and defend against man-in-the-middle (MITM) attacks. In this case, an app stores or pins a copy of the original certificate within its code, and if it sees a modified version of that certificate, the app rejects it and terminates the connection immediately.

Hence, SSLi provides a certificate pinning candidate list feature to support such apps. This feature maintains a list of known domain names that may use certificate pinning on their client apps.

The following new CLI command and GUI page are available to view the certificate pinning candidate list:

CLI Configuration

```
ACOS(config)# show slb ssl-cert-pinning-candidate-list
SNI Counter TTL
-----------------------
youtube.com 10 1440
gmail.com 6 1440
```

GUI Configuration

A new **SSL Cert Pinning** page is available under **ADC > SSL Management**.

Client and Server-side TLS 1.3 Support on Intel QAT and Software SSL

The SSLi client and server-side supports the latest TLS 1.3 protocol on the Intel QuickAssist Technology (QAT) and Software SSL modules. Additionally, all the latest TLS 1.3 cipher suites are supported. This feature ensures benefit from all the enhanced security features and high performance that come with these modules.

The following configurations are available for this feature:

- SSLi uses the existing 'forward-proxy-ssl-version' command to enable TLS 1.3 in the client-SSL template.

  Additionally, a new 'forward-proxy-esni-action' command is introduced to bypass or drop the encrypted server name indication (ESNI) extension.

- SSLi uses the existing 'version' command to enable TLS 1.3 in the server-SSL template.

CLI Configuration

Cipher Configuration:

```
ACOS (config)# slb template cipher cipher_tls13
ACOS (config-cipher)# TLS_CHACHA20_POLY1305_SHA256 priority 5
ACOS (config)# exit
```

Server- SSL Configuration:

```
ACOS (config)# slb template server-ssl SSLInsight_TLS13
ACOS (config-server ssl)# forward-proxy-enable
ACOS (config-server ssl)# version 34 33
ACOS (config-server ssl)# template cipher cipher_tls13
```

Client- SSL Configuration:

```
ACOS (config)# slb template client-ssl SSLInsight_TLS13
ACOS (config-server ssl)# forward-proxy-ssl-version 34
ACOS (config-server ssl)# forward-proxy-esni-action bypass
```

GUI Configuration

To enable TLS 1.3 in the client-SSL Template, go to:

- **ADC > Templates > SSL > Client-SSL > Forward Proxy SSL Version**
- **Security > SSLi > Templates > Client-SSL > Advanced > Forward Proxy SSL Version**

Enhanced Web Category Filtering

The Web Category feature is enhanced to filter and block Child Abuse Material (CAM) only using the Web Category filters. As per Internet Watch Foundation (IWF) Classification, this filter can be classified by joining two web categories:

- 'Illegal' and 'Adult and Pornographic'
- 'Entertainment and Arts' and 'Nudity'

This feature can be enabled using 'illegal-pornography' and 'nudity-artistic' categories available under Web Category and Client-SSL template. Then you can bind with the Policy template.

CLI Configuration

- Under Client-SSL Template

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS-(config-client ssl)# forward-proxy-bypass web-category illegal-pornography
ACOS-(config-client ssl)# forward-proxy-bypass web-category nudity-artistic
```

- Under Web Category

```
ACOS(config)# web-category enable
ACOS(config-web-category)# category-list illegal-pornography
ACOS(config-web-category)# category-list nudity-artistic
```

GUI Configuration

To enable the 'illegal-pornography' and 'nudity-artistic' options, go to:

- **ADC > Templates > SSL > Client-SSL > Forward Proxy Bypass > Web Category**
- **ADC > Templates > SSL > Client-SSL > Forward Proxy Bypass > Exception Web Category**
- **Security > Web Categories > Category List**

Extended End-to-End HTTP/2 Support with Hardware Modules

In ACOS 5.2.0 release, the end-to-end HTTP/2 protocol support is available with the Software SSL module in these three SSLi scenarios:

- Static port SSLi without forward-policy
- Static port SSLi with forward-policy (Explicit Proxy/ Transparent Proxy/ Proxy-chaining)
- Dynamic port SSLi

With the growing adoption of HTTP/2 protocol and dedicated hardware accelerators to improve the CPU performance and utilization, we have extended the end-to-end HTTP/2 support with the following modules:

- Nitrox V (N5) hardware acceleration SSL module
- Inter QuickAssist Technology (QAT) SSL module in both TLS 1.2 and TLS 1.3
- Software SSL module in both TLS 1.2 and 1.3

FTPS Support

This feature was implemented in ACOS 4.1.4-GR1-P5 and is now implemented in this release.

The File Transfer Protocol over SSL (FTPS) support is provided in SSLi to ensure that the data exchanged between the client and the server is encrypted and secured. Currently, this feature is supported in FTP passive mode and for:

- Explicit FTPS (RFC 4217) - Client starts connection as normal FTP and request to use TLS before login.
- Implicit FTPS (no RFC) - Client starts connection as TLS at the beginning, just like HTTPS.

The configuration shall be available only if the SSLi License is enabled.

CLI Configuration

Under SLB Template SSLi:

```
ACOS(config)# slb template ssli ssli-tmp1
```

```
ACOS(config-ssli)# type ftp
```

Under Client-SSL and Server-SSL Template:

```
ACOS(config)# slb template client-ssl clientssl
ACOS(config-client ssl)# enable-ssli-ftp-alg port-number <1-65535>
ACOS(config)# slb template server-ssl serverssl
ACOS(config-server ssl)# enable-ssli-ftp-alg port-number <1-65535>
```

GUI Configuration

- To configure the Type option: **Security > SSLi > Templates**
- To configure the **Enable SSLi FTP ALG** option:
  - **Security > SSLi > Templates > Client SSL**
  - **Security > SSLi > Templates > Server SSL**
  - **ADC > Templates > SSL > Client SSL**
  - **ADC > Templates > SSL > Server SSL**

LDAPS Support

This feature was implemented in ACOS 4.1.4-GR1-P5 and is now implemented in this release.

The Lightweight Directory Access Protocol over SSL (LDAPS) support is provided in SSLi for making the connection secure thus protecting the sensitive data from the malicious eavesdropping attack. Currently, two LDAPS modes are available:

- LDAP over SSL - supported by dynamic port SSLi
- LDAP STARTTLS - supported by LDAP service in SSLi Template

CLI Configuration

```
ACOS(config)# slb template ssli ssli-tmp1
ACOS(config-ssli)# type ldap
```

GUI Configuration

To configure the Type option: **Security > SSLi > Templates**

Match SNI to Prevent SSLi Bypass

This feature was implemented in ACOS 4.1.4-GR1-P3 and is now implemented in this release.

Currently, ClientHello message is sent as plain text, which makes it possible to spoof with the SNI information and bypass a non-bypass site. Hence, a new option called forward-proxy-require-sni-cert-matched is introduced under client-SSL template to prevent the SSLi bypass.

When this option is enabled, the SNI in the ClientHello message must match with one of the server certificate (subject CN or DNS fields in SAN). If not matched, the action could be inspected or dropped, as selected.

CLI Configuration

```
ACOS(config)# slb template client-ssl SSLInsight_ClientSide
ACOS(config-client ssl)# forward-proxy-require-sni-cert-matched
{nomatch-
action-drop | no-match-action-inspect}
```

GUI Configuration

To configure **Forward Proxy Require SNI Cert Match option** go to **Security > SSLI Templates > Clients SSL**.

SNI Bypass Support based on Certificate Status

In inbound SSLi visibility scenarios, it is possible to control which traffic to send to the SSL visibility device in the network (IP) layer. However, it may be challenging to have control when the same IP (or VIP) has multiple websites in a single IP having its own certificate and key. Hence, it becomes critical to choose which web sites subject to SSL visibility and which web sites are not.

To overcome this challenge, SSLi provides a way to bypass the connection of such websites based on the following scenarios:

- Certificate and key pair is not present in the VIP
- Certificate is expired
- SNI configured

To enable this feature, the following new CLI and GUI options are available under client-SSL template:

CLI Configuration

```
ACOS(config)# slb template client-ssl CLIENT_SSL
ACOS(config-client ssl)# server-name-bypass missing-cert
ACOS(config-client ssl)# server-name-bypass expired-cert
ACOS(config-client ssl)# server-name-bypass class-list sni_bypass
ACOS(config-client ssl)# server-name-bypass enable-log
```

NOTE: These new commands are available only if the 'server-name', 'server-name-auto-map', and 'server-name-regex' commands are configured.

GUI Configuration

Go to **ADC > Template > SSL > Client SSL**:

- SNI Bypass when Missing Cert/Key
- SNI Bypass when Certificate Expired
- SNI Enable Logging when Bypass Event Happens
- SNI Bypass when Matched Explicit Bypass Class-List

SSL Certificate Management for Shared Partition

This feature was implemented in ACOS 4.1.4-GR1-P3 and is now implemented in this release.

Several data centers host many devices and services and give rise to the necessity of large-scale SSL deployment in multi-tenant environments. It becomes practically challenging to generate CSR from each private partition, sign into the CSR digitally, and import the partition. Further challenges arise in binding it to the clients-SSL template and managing each certificate.

To simplify the SSL certificate or key management task, a new parameter partition shared is introduced in the existing commands under client and server SSL templates and is configurable using both CLI and GUI. This will generate the CSR in each device shared partition with the non-exportable private key feature and have the ability to bind that Cert/Key (stored) from Private partition (tenant).

CLI Configuration

The 'partition-shared' parameter is available in the following commands:

- forward-proxy-ca-cert
- forward-proxy-ca-key
- forward-proxy-alt-sign
- forward-proxy-trusted-ca
- client-certificate-Request-CA
- cert-alternate
- key-alternate
- CRL

Example:

```
ACOS[partition1](config)# slb template client-ssl clientssl
ACOS[partition1](config-client ssl)# forward-proxy-ca-key myCAkey
partition shared
```

GUI Configuration

- The following new options are available under **ADC > Templates > SSL > Client SSL.**
  - Forward Proxy CA Cert From Shared Partition
  - Forward Proxy CA Private Key From Shared Partition
  - Forward Proxy Alternate Signing CA Cert/Key From Shared Partition
  - Client Certificate Request CA From Shared Partition
  - Forward Proxy Trust CA List From Shared Partition
  - Alternate Server Certificate From Shared Partition
  - Alternate Server Private Key From Shared Partition
- The following new options are available under **Security > SSL > Templates > Client SSL**.
  - CA Cert From Shared Partition
  - Key From Shared Partition

- Cert /key From Shared Partition
- Forward Proxy Trust CA List From Shared Partition

- The **CRL Files From Shared Partition** option is available under **Security > SSL > Templates > Server SSL**.
- The **Cert-Revocation List From Shared Partition** option is available under **ADC > Templates > SSL > Server SSL**.

Zero RTT Support on New N5 Module

In ACOS 5.1.0 release, 0-RTT (early data) feature was supported on QAT module and Software SSL TLS 1.3. In this release, this feature is supported on new Nitrox V (N5) module as well using the existing ‘early-data’ CLI command.

VRRP-A High Availability

ACOS 5.2.1 introduces the following new feature and enhancement for VRRP-A High Availability:

Display Configure Sync Status on Header Bar

Previously, the 'Configure Sync Status' icon was unavailable on the GUI header. The sync icon displays Running, and Startup configures information and links to the 'Sync Configure' when the cursor hovers over it. In this release, this icon will be visible when the VRRP-A is enabled.

Web Application Firewall

ACOS 5.2.1 introduces the following new features and enhancements for Web Application Firewall (WAF):

NOTE: For WAF specific configuration steps, refer *Web Application Firewall Guide*.

The following topics are covered:

Customizable WAF Deny Page

The Web Application Firewall (WAF) is enhanced with a customizable WAF Deny page that displays the relevant message to the end user when a request is denied. You can also add extra information such as the WAF event or violation ID, request details, reasons for denial and even the highlighted violation payload.

The new aFleX command, **`WAF::response_body`** is introduced to aggregate the information displayed when the violation occurs.

NOTE: Binding the WAF Deny page per WAF Template is not supported since the aFleX is bound to the virtual port.

Mask Sensitive Data in Logs

The query value masking feature is introduced in the WAF template to prevent sensitive information disclosure in the violation logs. The new **`violation-mask-log`** command is implemented to mask the query parameter value during logging.

The following features are available:

- The symbol 'x' is used to mask the sensitive data.
- The mask length is generated randomly to prevent guessing the content length.
- The mask is applied only while generating the logs; the real servers continue to receive the original unmasked values.

CLI Configuration

The following command masks the query parameters *`username`* and *`password`* during logging,

```
ACOS(config)# waf template waf1
ACOS(config-waf)# violation-log-mask
ACOS(config-waf-violation-log-mask)# query-param-name equals "username password"
```

GUI Configuration

To configure the query parameter names to be masked, go to **Security** > **WAF** > **WAF Templates** > **Add/Edit WAF Template** > **Violation Log Mask Query Parameter Name**

NOTE: Currently, the Harmony Controller log and Syslog support this feature. However, the debug logs display unmasked values.

Query Parameter Enhancement in HTTP Policy

The HTTP Policy is enhanced with the following new condition types to match a single-match-rule and the multi-match-rule query string, along with the existing match options:

- **query-param-name**
- **query-param-value**

Known Limitations

- The match for these condition types works only if the query string is included in the URL and not in the request body.
- In case of query names with special characters, the match requires url-encoded version of these characters. For example, to match a space (" "), you must specify "%20".

CLI Configuration

The following example demonstrates **query-param-name** condition type usage:

```
ACOS(config)# slb template http-policy http-policy4.2.6
ACOS(config-http-policy)# query-param-name contains fname template waf http-policy-waf-A
ACOS(config-http-policy)# query-param-name equals [no-name] template waf http-policy-waf-B
```

The command **query-param-name equals [no-name]** is considered as a condition that matches a query with an empty name.

The following example demonstrates **query-param-value** condition type usage:

```
ACOS(config)# slb template http-policy http-policy4.2.6
ACOS(config-http-policy)# query-param-value ends-with fname service-group http-policy-sg-A
ACOS(config-http-policy)# query-param-value equals [no-value] service-group http-policy-sg-B
```

The command **query-param-value equals [no-value]** is considered as a condition that matches a query with and empty value.

WAF Template Count Enhancement

The new **waf-template-count** command is introduced under **system resource-usage** command. It allows you to specify the number of configurable WAF templates in the system. The default value is 128. The minimum and maximum configurable values are platform specific.

The corresponding show command is also introduced under **show system resource-usage** command. It displays the total number of configurable WAF templates currently available in the system.

CLI Configuration

The following command sets the number of configurable WAF templates to 120:

```
ACOS(config)# system resource-usage waf-template-count 120
```

GUI Configuration

To configure the WAF template count, go to **System** > **Settings** > **Resource Usage** > **System Resource Usage** > **WAF Template Count**

WAF Template Inheritance Support

The WAF (Web Application Firewall) template configuration has many fields and hence defining the complete template at all levels is time consuming. Therefore, a new method is introduced that inherits the entire configuration from one WAF

template (parent) to another (child). The child template inherits all the features of the parent template and overrides only the specific features that need changes.

A new **`parent template waf`** command is implemented under the WAF template.

Known Limitations

- The child template can inherit the configuration from one parent only; multiple inheritance is prohibited.
- The inheritance is supported at one level only; the parent template cannot inherit the configurations from another template.
- After downgrading, the inheritance configuration will be removed, and the child template will lose its true configuration. You will have to reconfigure the child template.
- The following configurations will not be inherited,
  - Logging template
  - Deploy mode
  - Deny action
  - Cookie security
  - PCRE mask
  - Referer check
  - **`xml-content-validation`**
  - **`redirect-whitelist`**
  - **`url-learned-list`**
  - **`log-succ-reqs`**

CLI Configuration

Consider an existing WAF template **`waf-temp-parent`**. Use the following commands to create another template **`waf-temp-child`** that inherits the features of this template,

```
ACOS(config)# waf template waf-temp-child
ACOS(config-waf)# parent template waf waf-temp-parent
```

Enhancements in ACOS 5.2.0-P1

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.0-P1 release:

The following topics are covered:

aFlex

ACOS 5.2.0-P1 introduces the following new feature and enhancement for aFlex.

NOTE: For more information, refer *aFleX Scripting Language Reference*.

aFleX Support for TLS 1.3

With this release, the aFleX events and commands related to SSL can be executed on the TLSv1.3.

Network Configuration

ACOS 5.2.0-P1 introduces the following new feature and enhancement for Network Configuration:

NOTE: For more information, refer *Network Configuration Guide*.

Unnumbered IPv4 Interfaces Support in BGP

ACOS supports enabling unnumbered IPv4 interfaces in BGP. As per RFC 5549, ACOS BGP supports exchanging IPv4 routes over an unnumbered IPv4 interface. This is achieved by BGP neighbor communication over IPv6 Link Local addresses and requires enabling IPv6 on the interface.

Platforms

ACOS 5.2.0-P1 introduces the following new feature and enhancement for Platforms:

N5 Hardware Supports TLS 1.2 ChaCha Poly Ciphers

From ACOS 5.2.0, Nitrox V (N5) crypto accelerator now supports three additional TLS 1.2 ChaCha Poly Ciphers. The following has more details about Cipher names and ID.

Table 3 : TLS 1.2 ChaCha Poly Ciphers Support List

Cipher Name	Cipher ID
TLS1_DHE_RSA_CHACHA20_POLY1305_SHA256	0xCC, 0xAA
TLS1_ECDHE_RSA_CHACHA20_POLY1305_SHA256	0xCC, 0xA8
TLS1_ECDHE_ECDSA_CHACHA20_POLY1305_SHA256	0xCC, 0xA9

NOTE: Additionally, for the N5 new module, there are significant architecture changes in 5.2.0-P1. If you are using the N5 new module, then kindly upgrade to ACOS 5.2.0-P1.

Enhancements in ACOS 5.2.0

This topic provides a brief overview of the new features and enhancements added in the ACOS 5.2.0 release:

The following topics are covered:

aFleX

ACOS 5.2.0 introduces the following new features and enhancements for aFleX:

NOTE: For more information, refer *aFleX Scripting Language Reference*.

The following topics are covered:

aFleX New Proxy Support

The following is a new set of the commands which now supports the new proxy:

- HTTP::disable
- HTTP::retry
- SSL::respond
- COMPRESS::enable
- COMPRESS::gzip
- COMPRESS::disable
- CACHE::hits
- CACHE::expire
- CACHE::enable
- CACHE::disable

SMTP Commands

The following is a new set of the commands which now supports the SMTP:

- **SMTP::greet** - Set EHLO OK messages.
- **SMTP::ehlo** - Retrieve client's ehlo or Helo message.
- **SMTP::mail** - Retrieves MAIL command parameter (reverse-path).

SMTP Events

The following is a new set of the commands which now supports the SMTP events:

- **SMTP_EHLO** - Triggered when EHLO command arrives.
- **SMTP_MAIL** - Triggers upon receiving MAIL FROM command from client.

URL Command

The following is a new command which now supports the URL:

URL::reputation

Gets the URL reputation values.

Application Access Management

ACOS 5.2.0 introduces the following new features and enhancements for Application Access Management (AAM):

NOTE: For AAM specific configuration steps, refer *Application Access Management Guide*.

The following topics are covered:

Application Access Management (AAM) SAML Relay

The AAM enhancement extends the support for Security Assertion Markup Language (SAML) Relay to the backend servers while performing SAML authentication. It provides additional information about the authenticated user. Additionally, SAML re-authentication of Application Server is not required since the first Service Provider (SP) can relay the SAML response token to the Application Server. Statistics fields, such as Failures, Requests, Successes, and Error are added to provide more information.

CLI Configuration

```
ACOS(config)#aam authentication relay saml saml
ACOS(config-saml auth relay:saml)#relay-acs-uri /adfs/ls/
ACOS(config-saml auth relay:saml)#idp-auth-uri https://idp.a10-
tplab.com/adfs/ls/
```

```
ACOS(config-saml auth relay:saml)#server-login-uri equals /start
ACOS(config-saml auth relay:saml)#server-cookie-name auth-relay
ACOS(config-saml auth relay:saml)#relay-state value test
ACOS(config-saml auth relay:saml)#retry-number 3
```

GUI Configuration

To configure Application Access Management (AAM) SAML relay, go to **AAM > Auth Relays > SAML**.

L3V Partition DNS Server Support

Currently, Application Access Management (AAM) supports the configuration of **IP DNS** in the L3V partition. But, in the previous release, the AAM daemon a10authd and IPsec daemon Charon, were using the DNS in a shared partition.

With this enhancement, the AAM daemon a10authd and IPsec daemon Charon can use the L3V partition DNS for L3V partition operations. The L3V partition DNS can resolve the domain name and hostname in a10authd and Charon and it also extends its support for Kernel VRF implementation for v4 and v6 L3V.

SP-initiated Single Log Out (SLO)

With this release, the SP-initiated Single Log Out (SLO) provides an enhanced secure session when authenticated through ACOS via SAML. The service provider can initiate a logout from the ACOS in the SAML SP-initiated SLO endpoint. Both the Service Provider (SP) and Identity providers (IdP) can log out and clear the sessions, which allows logout from all the authenticated sessions simultaneously.

However, server re-authentication is required to initialize the session again. Statistics field SP-initiated SLO requests, Global Logout successes, Local Logout successes, and Partial Logout successes are added to provide additional information.

CLI Configuration

The following is a set of commands used for configuring SP-initiated SLO:

```
ACOS(config)#aam authentication saml service-provider test
ACOS (config-SAML service provider:test)#SP-initiated-single-logout-
service location
```

```
/Logout2 asynchronous
ACOS(config-SAML service provider:test)#SP-initiated-single-logout-
service location
/Logout3
```

GUI Configuration

To configure SP initiated single log out, go to **AAM > Authentication Client > SAML Service Provider**.

Application Delivery Controller

ACOS 5.2.0 introduces the following new features and enhancements for Application Delivery Controller (ADC):

NOTE: For ADC specific configuration steps, refer *Application Delivery Controller Guide*. Similarly, for ADC specific CLI commands, refer *Command Line Reference for ADC Guide*.

The following topics are covered:

DNS Template Caching Support

The DNS cache template includes a round-robin policy that allows each service to set its own policy. This feature is implemented in both CLI and GUI. The **cache-record-serving-policy** option is available to set one of the following condition:

- **round-robin** - To enable the service level round-robin policy.
- **no-change** - To disable the service-level round-robin policy.

- **global** - To enable the global-level round-robin policy.

CLI Configuration

```
ACOS(config)# slb template dns dns1
ACOS(config-dns)# cache-record-serving-policy {round-robin | no-change |
global}
```

GUI Configuration

To configure ***DNS Cache Record Response Policy*** option, **ADC > Templates > L7 Protocols > DNS**.

DNS Over HTTPS Template Enhancements

The DNS over HTTPS (DoH) template is enhanced with the capability to forward the traffic to another VIP on the same partition and port number. This feature allows the existing DNS VIP on the same ACOS device and L3v partition to handle the DNS query extracted from a DOH query.

Additionally, the decapsulated DNS query can be forwarded to an external IP address (IPv4 or IPv6) without the need to configure the SLB server and service-group. The configuration is available in both CLI and GUI.

NOTE: The capability to load balance using this feature is done internally to a single IP and not for a group of IPs. For internal IPs, you still need to use the existing Server Load Balancing (SLB) server or service-group configuration to bind to the DoH template.

CLI Configuration

```
ACOS(config)# slb template doh doh2
ACOS(config-doh)# forwarder
ACOS(config-doh-forwarder)# forwarding-ipv4 40.40.40.101 internal port
53 protocol tcp
```

Enhanced DNS Cache Filters

Currently, our system supports deleting the entire DNS cache entry per partition at once. There is no mechanism to delete or display a certain DNS cache entry for a

particular domain or record. The `clear` or `show` commands are now enhanced by the addition of multiple filters to delete or display DNS cache based on DNS class, DNS type, domain name, and Fully Qualified Domain Names (FQDN).

The commands now support the following:

- Clear or show system DNS cache based on DNS class, DNS type, domain name and FQDN
- Clear or show global DNS cache based on DNS class, DNS type, domain name and FQDN
- Clear or show per vport DNS cache based on DNS class, DNS type, domain name and FQDN

CLI Configuration

The following commands have new options in ACOS 5.2.0:

NOTE: Multiple filters can be specified in one command. For example, you can specify `domain-name` and `dns-type` in one command.

Clear or Show System DNS Cache

```
ACOS(config)# clear dns cache entry domain-name fqdn_domain foo.com
ACOS(config)# clear dns cache entry domain-name dns_domain_name foo.com
ACOS(config)# clear dns cache entry dns-type TXT
ACOS(config)# clear dns cache entry dns-class 66

ACOS(config)# show dns cache entry domain-name fqdn_domain foo.com
ACOS(config)# show dns cache entry domain-name dns_domain_name foo.com
ACOS(config)# show dns cache entry dns-type 55
ACOS(config)# show dns cache entry dns-class IN
```

Clear or Show Global DNS Cache

```
ACOS(config)# clear dns cache global domain-name fqdn_domain temp.com
ACOS(config)# clear dns cache global domain-name dns_domain_name
temp.com
ACOS(config)# clear dns cache global dns-type CNAME
ACOS(config)# clear dns cache global dns-class CS
```

```
ACOS(config)# show dns cache global domain-name fqdn_domain foo.com
ACOS(config)# show dns cache global domain-name dns_domain_name foo.com
ACOS(config)# show dns cache global dns-type 77
ACOS(config)# show dns cache global dns-class HS
```

Clear or Show per vPort DNS Cache

```
ACOS(config)# clear slb virtual-server vip1 20053 dns-udp dns-cache
entry domain-name fqdn_domain foo.com
ACOS(config)# clear slb virtual-server vip1 53 dns-tcp dns-cache entry
domain-name dns_domain_name foo.com
ACOS(config)# clear slb virtual-server vip1 20053 dns-udp dns-cache
entry dns-type CNAME
ACOS(config)# clear slb virtual-server vip1 53 dns-tcp dns-cache entry
dns-class 44

ACOS(config)# show slb virtual-server vip1 20053 dns-udp dns-cache entry
domain-name fqdn_domain foo.com
ACOS(config)# show slb virtual-server vip1 53 dns-tcp dns-cache entry
domain-name dns_domain_name foo.com
ACOS(config)# show slb virtual-server vip1 53 dns-tcp dns-cache entry
dns-type TXT
ACOS(config)# show slb virtual-server vip1 20053 dns-udp dns-cache entry
dns-class CS
```

Link-cost Load Balancing

In the existing **`bw-rate-limit`** feature, if the link utilization exceeds the pre-configured bandwidth limit, new sessions are not sent to that link and the existing sessions are limited by the limited rate of the bandwidth.

Additionally, in case of a link failure, the incoming traffic is dropped. To overcome this, the link-cost load balancing method is introduced. In this method, link usage is prioritized based on the cost of the bandwidth for the connection. If the link utilization exceeds the pre-configured bandwidth, the excess traffic is sent to the link operating at the lowest overage cost. Also, in case of a link failure, traffic is sent to the next available link.

This feature is available as an **slb template link-cost** object that can be applied under an **slb server** object. Additionally, **link-cost-load-balance** option is introduced under the **method** command of **slb service-group**.

CLI Configuration

The following example configures a link-cost template:

```
ACOS(config)# slb template link-cost ln1
ACOS(config-rserver)# bandwidth-interval 10
ACOS(config-rserver)# prepaid-bandwidth 10
ACOS(config-rserver)# overage-bandwidth 5
```

This load balancing mechanism also provides statistics to understand and estimate the cost incurred by the customers for their data usage each month. A new option **link-cost-statistics** is added to **show slb service-group** command to display these statistics.

```
ACOS(config)# show slb service-group <group-name> link-cost-statistics
<start_date> <end_date>
```

Query Type and Query Class Filter for DNS Template

Currently, **slb template dns** has no provision to allow or drop a DNS query based on its type or class. New commands **query-type-filter** and **query-class-filter** are introduced to provide this mechanism. Using these filters you can create a list of DNS query types and or or query classes that need to be allowed or dropped. The DNS packets in the list that is allowed are forwarded while the others are blocked. By default, all query types and classes are allowed.

CLI Configuration

Configure DNS query types to be allowed:

```
ACOS(config)# slb template dns dns1
ACOS(config-dns)# query-type-filter allow
ACOS(config-dns-query-type-filter:allow)# query-type ANY
ACOS(config-dns-query-type-filter:allow)# query-type 7
```

Configure DNS class types to be denied:

```
ACOS(config)# slb template dns dns1
```

```
ACOS(config-dns)# query-class-filter deny
ACOS(config-dns-query-class-filter:deny)# query-class ANY
ACOS(config-dns-query-class-filter:deny)# query-class 5
```

To disable this feature:

```
ACOS(config-dns)# no query-type-filter allow
ACOS(config-dns)# no query-class-filter allow
```

NOTE: You cannot configure more than 16 query-type items and 8 query-class items.

Smart NAT Enhancements to Support Range Over 64K Ports

The existing Smart NAT Auto feature is enhanced to support multiple interface or floating IPs to reach more than 64K. This will facilitate to add more interface or floating IPs when it reaches 41K each IP.

By default, this feature is enabled when the source-nat auto feature is configured. However, if VRRP-A is enabled then the floating IPs will be used and if disabled then interface IPs will be used. Additionally, a flag named **ip-rr** is introduced in both CLI and GUI, which will enable the IP address round-robin method on the configured NAT pool.

This option rotates through the floating IPs for every request to balance the traffic across all the available floating IPs. It will automatically create NAT mappings using the ACOS interface connected to the real server.

This feature supports all the platforms that include the Source NAT auto functionality.

CLI Configuration

To configure IP round-robin:

```
ACOS(config)# slb virtual-server vip1 160.160.160.150
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# source-nat auto ip-rr
```

To view source NAT statistics:

```
ACOS(config)# show slb server rs auto-nat-stats
```

```
Total Number of Services configured on Server rs: 21
Service          HA/VR ID    IP_RR Nat Address    Port Usage   Total Used
  Total Freed  Failed
-------------------------------------------------------------------------
-------------------
rs:80/tcp        1           Yes 10.212.1.225   64           660469
660405       0
                                        10.212.1.226   64           660470       6604
rs:8080/tcp      1           Yes 10.212.1.225   0            0
0            0
                                        10.212.1.226   0            0            0
```

GUI Configuration

To configure **IP-RR** option, go to **ADC > SLB > Virtual Server > Virtual Port**.

Application Delivery Partition

ACOS 5.2.0 introduces the following new feature and enhancement for Application Delivery Partition (ADP):

NOTE: For ADP specific configuration steps, refer *Application Delivery Partitions Guide*. Similarly, for specific CLI commands, refer *Command Line Reference Guide*.

Overlapping or Duplicate Addresses Across Multiple L3V Partitions for IPv6

Overlapping or duplicate addresses across multiple L3V partitions are now supported for IPv6. Two IPv6 addresses can be configured within the same subnet in two separate partitions.

The following configuration with overlapping IPv4 and IPV6 addresses is now feasible:

```
Shared partition:
interface ethernet 1
ip address 1.1.1.1 255.255.255.0
ipv6 address 2002::1:1:1:1/112
```

```
L3V partition:
interface ethernet 2
ip address 1.1.1.1 255.255.255.0
ipv6 address 2002::1:1:1:1/112
```

Capacity FlexPool License Add-ons Support

ACOS 5.2.0 introduces the following new feature and enhancement for Capacity FlexPool License Support:

NOTE: For more information, refer *Capacity FlexPool License and Enterprise License Management License Guide*.

Web Category v2 Webroot License Support

The Web Category v2 Webroot License support is added to enhance the Capacity FlexPool License Add-ons. Upon the purchase of CFW Capacity FlexPool license box, the following ACOS features are available:

- Webroot
- Webroot TI
- IPsec Add-ons

NOTE: The earlier version of Web Category, Webroot License Support feature was already available with a web category license 1.0. It is now enhanced with the newly introduced additional options such as read, delete and import, in the updated 1.5 license version.

The Web Category v2 Webroot is enhanced so that it now performs the following:

Read

This option reads v1.5 Webroot license: A flow is added to extract the token from v 1.5 Webroot license file. After the license is decoded, token is generated.

Allow

This option allows import of v1.5 license file via **`import glm-license`** command.

Show

This option shows installed v2 license information with **`show web-category license`** command.

```
vThunder#show web-category license
Module Status                    : Enabled
License Status                   : License is valid
License Type                     : show license-info for webroot type
License Expiry                   : show license-info for expiration
Remaining Period                 : show license-info for expiration
Grace Period Status              : show license-info for grace period
Grace Period                     : show license-info for grace period
UUID/SN                          :
vThunderFDAD1486FEDB7B09158855EECE02EEB1DF87C5F2
```

Delete

This option deletes only the **GLM Webroot CLI**.

Running the **`delete glm-license`** command removes all licenses including the Webroot license.

```
vThunder(config)#delete glm-license ?
 cylance      only remove Cylance license
 ipsec-vpn    only remove IPSEC VPN license
 qosmos       only remove QOSMOS license
 threatstop   only remove ThreatSTOP license
 webroot      only remove Webroot license <<<<<<<
 webroot-ti   only remove Webroot Threat Intel license
 <cr>
```

Add

This option adds **Bright Cloud Honoring Serial Controlled Motor Driver (SCMD) Bit** feature.

This feature validates one of the spare bits in **`bc4_web_cat_license_detail`** as **`scm_bit_set`**, to detect the previous value of the **`scmd bit`**.

For Example

When `(config-web-category)#enable`, then a v2 license is used to enable the library as:

```
[WEB-CATEGORY]:BrightCloud license activated
```

When a v2 license has previously enabled Bright Cloud, the license is no longer valid, after a check, and there is no v1.5 license. In that case, the library is disabled as:

```
[WEB-CATEGORY]:BrightCloud license deactivated
```

Validate

This option validates the **v2 bit/web_cat_check_scm_license**.

If V2 license is valid, then the v1 check is skipped. Otherwise, it falls through to v1 logic.

Display

This option displays Webroot license type (Webroot or NFR or Trial) and notes filed for a Webroot license with `show license -info` command.

For Example

```
vThunder#show license-info
Host ID         : FDAD1486FEDB7B09158855EECE02EEB1DF87C5F2
USB ID          : Not Available
Billing Serials: vThe444a86bc0000, vTh69bf4386e0000
Token           : Not Available
Product         : CFW
Platform        : vThunder
Burst           : Disabled
GLM Ping Interval In Hours : 1
------------------------------------------------------------------------
------------
Enabled Licenses          Expiry Date (UTC)                Notes
------------------------------------------------------------------------
------------
SLB                       None
CGN                       None
```

```
GSLB                          None
RC                            None
DAF                           None
WAF                           None
SSLI                          None
DCFW                          None
GIFW                          None
URLF                          None
AAM                           None
FP                            None
WEBROOT                       07-June-2020      License Type: webroot
THREATSTOP                    N/A               Requires an additional
ThreatSTOP license.
QOSMOS                        N/A               Requires an additional QOSMOS
license.
WEBROOT_TI                    N/A               Requires an additional
Webroot Threat Intel license.
CYLANCE                       N/A               Requires an additional
Cylance license.
IPSEC_VPN                     N/A               Requires an additional IPsec
VPN license.
100 Mbps Bandwidth            None
```

Carrier Grade NAT

ACOS 5.2.0 introduces the following new features and enhancements for Carrier Grade Network Address Translation (CGN or CGNAT):

The following topics are covered:

Rate Limit Resets for Unknown Sessions

ACOS will send a TCP reset packet to the client if the client's non-SYN TCP packet does not match any existing session. It is possible under certain failover situations for the CPU to reach a very high utilization due to flooding of TCP reset packets.

Beginning with ACOS 5.2.0, you can avoid the possibility of high CPU utilization due to TCP reset flooding.

Use the **reset-unknown-conn** command to limit the rate of TCP resets sent out by ACOS.

Known Issues and Limitations

The System TCP Rate Limit Resets Unknown Sessions is supported only on Carrier Grade NAT L3V partitions for CGNv6 or Firewall TCP **reset-on-error** configuration.

CLI Configuration

The following command configures the rate limit for TCP **reset-on-error**:

```
system tcp rate-limit-reset-unknown-conn {pkt-rate <num> |[log]}
```

Show Commands

A new counter, **Rate Drop reset** is added to the **show counters cgnv6 l4** and **show cgnv6 l4** commands.

- Use the following command to view the statistics for the TCP reset packet rate limits:

```
show system tcp rate-limit-reset-unknown-conn
```

- Use the following command to clear the TCP reset packet rate limit statistics:

```
clear system tcp rate-limit-reset-unknown-conn
```

GUI Configuration

The following GUI updates are made on ACOS GUI:

- **System > Settings > General** includes the following two new fields:
  - **Rate Limit Reset Unknown Conn Pkt Rate**
  - **Rate Limit Reset Unknown Conn Log**
- **System > Monitoring** includes a new page called **TCP Rate Limit Reset Unknown Conn** to view the statistics for TCP rate limit reset unknown connection.
- **CGN > LSN > Stats > NAT L4** includes a new field called Rate Drop reset.

Support for Displaying Fixed-NAT Port Usage Histogram

A new show command named **`show cgnv6 fixed-nat histogram port usage {inside-user | nat ip}`** is introduced to display a histogram of active TCP or UDP users using ports in specific port ranges to which the inside user or the NAT IP belongs.

For more information, refer *IPv4-to-IPv6 Transition Solutions Guide* and *Command Line Reference for CGN*.

Show Commands

```
GIFW-SI-DUT-A-Active#show cgnv6 fixed-nat histogram ?
  port-usage  port Usage Histogram for TCP and UDP
GIFW-SI-DUT-A-Active#show cgnv6 fixed-nat histogram port-usage ?
  inside-user  Inside User
  nat-ip       NAT Address
GIFW-SI-DUT-A-Active#show cgnv6 fixed-nat histogram port-usage
```

Viewing Port Overload Statistics at NAT Pool Level

Starting with ACOS 5.2.0, the NAT pool statistics can be used to view the total number of TCP and UDP ports overloaded.

For more information, refer *IPv4-to-IPv6 Transition Solutions Guide* and *Command Line Reference for CGN*.

Show Commands

The following show command for NAT pool statistics has been enhanced to display the total number of TCP and UDP ports overloaded:

```
ACOS#:show cgnv6 nat pool statistics
```

The following show counter for NAT pool has also been enhanced to display the number of times a port on a NAT address was assigned to a new client while another client was still using the mapping, the number of times a session on an overloaded port was created, and the number of times a session created on an overloaded TCP port was freed:

```
ACOS#:show counters cgnv6 nat pool
```

GUI Configuration

The following ACOS GUI information is added under **CGN > LSN > LSN Pools**:

- TCP Overload
- Overloaded—Total number of TCP ports overloaded
- Create—Total number of TCP port overloading sessions created
- Free—Total number of TCP port overloading sessions Freed
- UDP Overload
- Overloaded—Total number of UDP ports overloaded
- Create—Total number of UDP port overloading sessions created
- Free—Total number of UDP port overloading sessions Freed

Gi or SGi Firewall

ACOS 5.2.0 introduces the following new feature and enhancement for Gi or SGi Firewall:

DDoS Protection for Gi or SGi Firewall

ACOS provides security protection to help mitigate against some forms of Distributed Denial of Service (DDoS) attacks on subscriber IPs and subnets. During the DDoS attack, the subscriber may get temporarily disconnected because the traffic may not be delivered to the subscriber. Rate limiting and DDoS protection helps to ensure the firewall operation is not interrupted.

The following rate limiting features and IP blacklisting limits the volume of the traffic overcoming attacks that consume resources.

For more information, refer *Firewall Configuration Guide*.

Packets Per Second (PPS) Rate Limiting

This option configures the maximum number of packets allowed per second. When the number of packets-per-second crosses the configured threshold, the excessive traffic is dropped.

Throughput Rate Limiting

This option configures the maximum mega bits allowed per second. When the rate of traffic sent to a subscriber IP or a subnet per second crosses the configured threshold, the excessive traffic is dropped.

Connections Per Second Rate Limiting

This option configures the maximum number of connections you can initiate per second, per subscriber IP or subnet. When the number of connections per second rate limit exceeds the configured threshold, no new connections will be made on the subscriber IP or the subnet.

IP Blacklisting

This option blocks individual IP addresses or a subnet on DDoS attack. When a DDoS attack targeted towards a specific IP address is detected, then ACOS adds that IP address to the blocked list. The ACOS blocked list can contain up to 1024 IP addresses at any given moment.

The above rate limit entries are created for an inside subscriber or client IP only. It is highly recommended to configure an inside or inbound interface using the **`ip client`** command and an outside or outbound interface using the `ip server` command before configuring the rate limits. This configuration helps to identify if the session is an inbound session or an outbound session.

After configuring the above rate limits, you must define the firewall rule-set and bind the template lid to the rule-set.

The logs are generated by default when the firewall DDoS protection entries are added and removed. The logs support only the Syslog format.

IPsec Virtual Private Network

ACOS 5.2.0 introduces the following new features and enhancements for IPsec Virtual Private Network (VPN):

NOTE: For IPsec specific configuration steps, refer *Configuring IPsec VPN* .

The following topics are covered:

IKE Negotiation and Acceleration Phase 2 Support

Currently, IPsec supports management traffic on the management interface using the IPsec tunnel setup. This configuration must be performed manually to allow secured communication when sending the management traffic. Occasionally, however the manual configuration dependency may result in failure or lack of protection over management traffic.

The current behavior is now enhanced to eliminate the manual configuration and automate the process with traffic driven IKE negotiation. With this feature, when the management traffic is sent to IPsec tunnel, IKE negotiation is triggered to securely send the management traffic even if the IPsec tunnel is not configured.

Additionally, IPsec tunnel setup rate is enhanced to increase the performance by 300%-1600% based on CPU consumption level. This establishes the tunnels a faster, which in effect speeds up the dynamic sessions configuration.

IPsec Support for A10 Thunder Series 7650 (Chassis)

From this release, A10 Thunder Series 7650 supports IPsec feature to ensure end-to-end security and data flow protection.

IPsec Support for Intel QAT

Intel Quick Assist Technology (QAT) provides a software-enabled foundation for security, authentication, and compression. It significantly increases the standard Platforms solutions performance and efficiency. When the server load balancer uses ssl-module QAT configuration, IPsec is enforced to use the QAT hardware mode and enhances the IPsec data path performance simultaneously.

NOTE: In the ACOS Thunder series platforms, only some new Platforms models support QAT. To check the support, use `show hardware` command.

Network Configuration

ACOS 5.2.0 introduces the following new features and enhancements for Network Configuration:

NOTE: For more information, refer *Network Configuration Guide*.

The following topics are covered:

L2 Protocols: STP or RSTP and MSTP

Starting with ACOS 5.2.0, the L2 protocols STP or RSTP and MSTP are supported on the ACOS Platforms. The xSTP protocols help avoiding loops in L2 topologies.

CLI Configuration

The following commands configure the spanning-tree mode as STP:

```
ACOS(config)# spanning-tree mode stp
ACOS(config-stp)# enable
ACOS(config-stp)# priority 4096
```

The following command configures the VLAN in STP mode:

```
ACOS(config-stp)# vlan 100
```

The following commands configure the spanning-tree mode as RSTP:

```
ACOS(config)# spanning-tree mode rstp
ACOS(config-rstp)# enable
ACOS(config-rstp)# priority 4096
ACOS(config-rstp)# vlan 200
```

The following commands configure the spanning-tree mode as MSTP:

```
ACOS(config)# spanning-tree mode mstp
ACOS(config-mstp)# enable
ACOS(config-mstp)# revision 1 name tree
ACOS(config-mstp)# priority 4096
ACOS(config-mstp)# instance 1
ACOS(config-mstp)# priority 4096
ACOS(config-mstp)# vlan 300
```

Static Route BFD Using Resource Tracking Template

The Resource Tracking Template option has been added to the static route BFD config for IPv4 or IPv6 static routes. In addition, the Resource Tracking Template has been enhanced to track Scaleout status.

For example, the resource tracking can track the Scaleout status and bring down the BFD sessions associated with the static routes. As a result, any routing protocol inadvertently sharing the static route BFD sessions, also goes down.

Virtual Wire Interface Support

This release supports virtual wire interface configuration for IP-less deployments and interface servers that enhances load balancing. Additionally, the virtual wire endpoint is used at the server side to continue server validation. The explicit proxy configuration will enable forwarding the traffic of certificate fetching. When you want to use virtual wire, then ACOS must be configured in management interface only.

To use this feature, you must first enable Ethernet as a virtual wire interface. And then, configure the virtual wire endpoints as Ethernet, trunk, or virtual wire Ethernet group.

CLI Configuration

To enable virtual wire interface and configure endpoints:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# virtual-wire
ACOS(config-if:ethernet:1)# interface ethernet 2
ACOS(config-if:ethernet:2)# virtual-wire
ACOS(config-if:ethernet:2)# virtual-wire 1
ACOS(config-virtual-wire:1)# ethernet 1 ethernet 2
```

To enable the server certificate to fetch the traffic and forward it through the explicit proxy:

```
ACOS(config)# slb template policy Explicit_Proxy
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# action act_8080
ACOS(config-policy-forward-policy-action)# forward-to-proxy ep8080
support-cert-fetch
ACOS(config-policy-forward-policy-action)# log
ACOS(config-policy-forward-policy-action)# exit
ACOS(config-policy-forward-policy)# exit
ACOS(config-policy)# exit
```

Platforms

ACOS 5.2.0 introduces the following new features and enhancements for Platforms:

The following topics are covered:

Hardware Platforms Support

The following is a list of newly-supported hardware platforms for ACOS 5.2.0:

- TH3350-E
- TH3350 (Also supported from ACOS 5.1.0-Px patch release)
- TH3350S
- TH5650S
- TH7650 (Also supported from ACOS 5.1.0-Px patch release)

NOTE: For more information on the complete list of supported hardware Platforms, refer Hardware Platforms Support.

Automated Packet Capture

Currently, the ACOS debugging (axdebug) feature captures packets-based on the manually configured filters. This new feature provides the capability to capture the packet that increments a counter or when the counter increment rate is anomalous. If configured, it also captures the entire session related to that packet or multiple sessions from the same source. ACOS can capture multiple packets in parallel and capture multiple packets for different events configured.

Broadcom NIC Support

Installing vThunder (Virtual Thunder) on Oracle Cloud shapes that belong to 2x Series are enhanced to use Broadcom NIC (SRIOV Virtual Functions) for network traffic.

For more information on OCI shapes, refer *Installing vThunder on Oracle Cloud for A10 vThunder Series Guide*.

Cloud Initialization Using ACOS Cloud Services Support

ACOS cloud services are enhanced to provide a way of auto-configuring vThunder (Virtual Thunder) using a standard user interface and cloud initialization. Valid ACOS CLI commands are provided as user data in either `json` or `yaml` formats during instance launch time. vThunder (Virtual Thunder) gets auto-configured after complete boot up of the device.

Cloud initialization using ACOS cloud services is supported on the following platforms:

- OpenStack
- OCI
- AWS
- Azure

The cloud platforms, including OpenStack, OCI, and AWS, support user data input through their GUI. Azure does not support user data input through GUI; however, it can be provided through Azure CLI.

NOTE: ACOS cloud services do not support auto configuration of commands, which need user input to complete their operation.

CLI Configuration

The following are the available auto-configuration options:

- Reset the system using the `#system-reset` command. The following is an example:

```
vThunder(config)(NOLICENSE)#system-reset System reset requires reboot,
do you want to continue?[yes or no]:
```

- Erase the configuration for the following:
  - **preserve-accounts**
  - **reserve-management**
  - **reload**
- Enter the `#erase preserve-management preserve-accounts reload` command to erase the startup configuration.

```
vThunder(config)(NOLICENSE)#erase preserve-management preserve-
accounts reload
Please confirm: Erase startup configuration (Y or N)?:
```

- Create the aFleX script. The following is an example:

```
vThunder(config)(NOLICENSE)#aflex create af1
```

- Enter and Run the aFleX script.

  (Type on a line by itself when done)

NOTE: The **User Data** is supported in **`json`** and **`yaml`** input formats.

User Data Input Configurations in json and yaml Formats

The following is an ACOS sample configuration for **`json`** and **`yaml`** format:

```
!Current configuration: 384 bytes
!Configuration last updated at 15:52:43 IST Tue Jun 2 2020
!Configuration last saved at 15:52:43 IST Tue Jun 2 2020
!64-bit Advanced Core OS (ACOS) version 5.2.0, build 7 (Feb-12-
2020,23:41)
!
hostname vThunder-01
!
interface management
ip address dhcp
!
interface ethernet 1
enable
!
end
!Current config commit point for partition 0 is 0 & config mode is
classical-mode
```

User Data in yaml Format

```
a10_blob:
hostname vThunder-01
interface management
ip address dhcp
enable
```

```
interface ethernet 1
enable
end
```

User Data in json Format

```
#cloud-config-archive
- type: text/json
content: |
{
"a10_blob": "hostname vThunder-01\ninterface management\nip address
dhcp\nenable\nin                terface ethernet 1\nenable\nend"
}
```

Update Admin Password

Upon launching vThunder, use the following commands to update the default admin passwords in YAML and JSON formats. The ACOS cloud-init services enable the user to update the default admin password in place of **<password>** in the following format during vThunder launch service.

User Data in yaml Format

```
admin_chpasswd: <password>
```

User Data in json Format

```
#cloud-config-archive
- type: text/json
content: |
{
"admin_chpasswd": "<password>",
}
```

Counter Infra and Debugging Enhancements

The existing counter infra and debugging capability have been enhanced to manage the triggers, categorize, and display the related data for effortless troubleshooting.

The new counter and drop-counter tags are implemented to manage the count and statistics. These tags trigger the tracking and counting of packet errors and drops.

This feature enhances the usability and debugging ability across our various technologies such as Application Access Management (AAM), IP Security and Virtual Private Network (VPN), Application Delivery Controller (ADC), and Web Application Firewall.

Let's Encrypt and ACME Protocol Support

This release provides both the Let's Encrypt and Automatic Certificate Management Environment (ACME) protocol support for CA certificate management in Secure Sockets Layer Insight (SSLi). This protocol is based on passing JSON-formatted messages over HTTPS and was designed by the Internet Security Research Group (ISRG) in RFC 8555 for their Let's Encrypt service. This feature can be configured using both CLI and GUI.

You can set up an HTTPS server and automatically obtain a browser-trusted certificate. The domain verification is done using challenge HTTP-01 for provisioning an HTTP resource under a well-known URI. Additionally, the domain's IP address must be mapped to ACOS's virtual IP address and **reply-acme-challenge** option must be enabled.

NOTE: Currently, A10 supports only HTTP-01 challenge type.

CLI Configuration

To enable `reply-acme-challenge` under Server Load Balancing (SLB) Virtual Server Port:

```
ACOS (config)# slb virtual-server VIP1 192.168.22.22
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# reply-acme-challenge
```

To configure ACME certificate:

```
ACOS(config)# pki acme-cert test
ACOS(config-acme cert:test)# account-email test@url.com
ACOS(config-acme cert:test)# cert-type rsa
ACOS(config-acme cert:test)# domain test.com
```

```
ACOS(config-acme cert:test)# san-domain testing.com
ACOS(config-acme cert:test)# enroll
ACOS(config-acme cert:test)# run-with-staging-server
ACOS(config-acme cert:test)# renew-every hour 8
ACOS(config-acme cert:test)# exit
```

To view the log, debug, or status of the ACME certificate information:

```
ACOS(config)# show pki acme-cert [log | status]
```

GUI Configuration

The following are the GUI options:

- To configure ACME: **ADC > SSL Management > ACME Certificates**.
- To view ACME status: **Security > SSLi > Reports > PKI > ACME Certs**.

Official 128 GB Memory Support for vThunder (Virtual Thunder)

vThunder allows a high number of users and their throughput in a virtualized environment. vThunder (Virtual Thunder) devices support 128 GB memory and provision the resources to match the same.

For provisioning, the resources of both NUMAs inside the compute host are used, so that memory allocation is 64 GB from NUMA0 and 64 GB from NUMA1.

NOTE: This feature supports all platforms with 2 NUMA, 128GB memory, and 35 virtual CPUs. The memory allocation limits change according to available memory.

For more information, refer *vThunder Installation Guides*.

Shared Polling Mode Support

ACOS is enhanced from 5.2.0 release onwards to support shared polling mode for deployments that have CPUs greater than four.

When shared polling mode is enabled, both I/O and data processing are performed by all the vCPUs except the control CPU. If there is no I/O and data processing task in

the queue, then the system automatically switches the CPU to idle mode to conserve CPU cycles. Users can enable or disable the shared poll mode.

NOTE: This mode is only preferred when performance or latency is not the key criteria for the success and the user wants to maximize host CPU utilization due to multiple VMs running on it.

For more information, refer *vThunder Installation Guides*.

TLS 1.3 Support for Management Plane

For ensuring better security and protection, TLS (Transport Layer Security) 1.3 support is provided for encryption over the ACOS management plane. This capability can be configured using the CLI command.

CLI Configuration

To enable or disable TLS (Transport Layer Security) 1.3:

```
ACOS (config)# system tls-1-3-mgmt enable
ACOS (config)# no system tls-1-3-mgmt enable
```

Scaleout

ACOS 5.2.0 introduces the following new features and enhancements for Scaleout:

NOTE: For Scaleout specific configuration steps, refer *Scaleout Configuration Guide*.

The following topics are covered:

ADC Scaleout in Transparent Cache Switching Mode

Transparent Cache Switching (TCS) is supported in Server Load Balancing (SLB) Scaleout. TCS improves server response time by redirecting client requests for content to cache servers containing the content.

When a client sends a request for content that is hosted by the content server, the ACOS redirects the client's request to the cache server. If the cache server has the requested content, the cache server sends the content to the ACOS device, which sends the content to the client. Similarly, when a traffic packet is sent to the real server, the global traffic map is used to ensure that the return traffic always reaches the node that owns that traffic set.

For more information, refer *Application Delivery Controller Guide*.

NOTE: Source NAT pool is not used.

Known Limitations

The following are the limitations:

- Only L3 redirect is supported.
- L2 redirect is not supported.
- It is recommended to enable the **jumbo** option in the L3 redirected mode to avoid fragmentation on an additional VXLAN overhead of 50 bytes.

GUI Configuration

A new field Scale Out Traffic Map is added under **ADC > SLB > Global**.

Distributed Forwarding

To improve the performance of packet handling, ACOS 5.2.0 offers the ability to reduce the number of packet redirections in Firewall Scaleout

CLI Configuration

The following command enables the distributed forwarding:

```
scaleout distributed-forwarding fw
```

Known Limitations

The following are the known issues and limitations of the Distributed Forwarding option:

- It is applicable for TCP and UDP sessions.
- It is applicable for redirected packets on L3 Scaleout mode and dedicated L2 Scaleout mode.
- Distributed Forwarding in L2 Scaleout mode is not supported when there is no dedicated redirection interface.
- It does not apply to DNS-UDP (port 53) and ICMP.
- TCP Window Check (currently enabled by default) is not supported along with distributed forwarding.
- Firewall Rate Limiting is not supported with Distributed Forwarding.

Radius Message Distribution in a Cluster

A RADIUS message can be received on any node in the cluster. Starting from ACOS 5.2.0, this message is redirected to a node that is active for the subscriber IP in this message. The same RADIUS entry is then synchronized to the standby node for that subscriber.

To distribute the RADIUS traffic equally among all the nodes in the cluster, you must configure the loopback interface with the same IP address on all the nodes. The RADIUS messages must be sent to the loopback IP. You must configure the routing protocols such as OSPF or BGP between the router and the ACOS device so that the client-side router allows the RADIUS message to reach any node in the cluster.

To ensure the radius message distribution works properly, you must exclude the loopback IP address from the IP routing table. To exclude the loopback IP address, use the exclude-interfaces CLI command while configuring the local device in the Scaleout cluster.

The RADIUS message distribution in a cluster is applicable for both Carrier Grade NAT and Firewall devices.It supports L2 and L3 redirection.

Scaleout for DS-Lite

Starting with ACOS 5.2.0, the Scaleout for DS-Lite is supported on all platforms including Dual-Blade Chassis or Thunder 7650.

Known Issues and Limitations

The following are the limitations:

- Carrier Grade NAT (CGN) Scaleout supports only the following:
- LSN (NAT 44, NAT 64)
- Fixed NAT (NAT44 and NAT64)
- DS-Lite
- The following Carrier Grade NAT (CGN) IPv6 technologies are not supported:
- Static-NAT or range list
- One-to-One NAT
- Stateless technologies such as MAP-E, MAP-T, and Lightweight 4over6 IPv6 transition.
- The following technologies are also not supported in Scaleout for DS-Lite:
- DS-Lite with Gi Firewall in Scaleout mode
- DS-Lite Hairpinning
- Port Reservation with Prefix Quota for DS-Lite
- L3 Redirection for DS-Lite

NOTE: For the L2 redirection to work properly, the sender and the receiver CGNAT Scaleout device must be in the same Layer 2 network with unique IP and MAC addresses.

Scaleout Support Extended for up to 16 Virtual Instances

ACOS 5.2.0 onwards support a a maximum of 16 vThunder (Virtual Thunder) ACOS instances in a Scaleout cluster, to increase the aggregate throughput capacity of the cluster.

Secure Sockets Layer Insight

ACOS 5.2.0 introduces the following new features and enhancements for Secure Sockets Layer Insight (SSLi):

NOTE: For SSLi configuration steps, refer *SSL Insight Configuration Guide*. Similarly, for SSLi specific CLI commands, refer *Command Line Reference for ADC Guide*.

The following topics are covered:

End-to-End HTTP/2 Support

ACOS SSLi now supports end-to-end HTTP/2 standard, which means that the HTTP/2 is an extension of the current HTTP standard and the application semantics remain the same. The full support enables efficient use of network resources and reduce latency.

The implementation is available for static-port SSLi with forward-proxy, static-port SSLi without forward-proxy, and dynamic-port SSLi. However, it is not supported for STARTTLS SSLi.

Extended Master Secret RFC 7627 Support

This release onwards the Extended Master Secret (EMS) RFC 7627 supports the previous versions of software SSL and Nitrox V (N5) hardware. This ensures better security and protection against man-in-the-middle (MITM) attacks even for old software and hardware.

SSLi Support for Intel QAT

This release provides SSLi support for Intel QuickAssist Technology (QAT). That includes symmetric encryption and authentication, asymmetric encryption, digital signatures, RSA, DH, and ECC, and lossless data compression. This capability improves the overall performance across the applications and the platforms.

For SSLi, Intel QAT offloads the crypto operation for the TLS security protocol. Asynchronized operation is used in such a way that the SSL application delivers a callback function to the Intel QAT API. Control returns to the SSL application once the request has been sent to the hardware accelerator, and the callback is invoked when the engine completes the operation. Additionally, both the RSA and ECDSA cryptography standard in the CA certificate or Private key are supported for QAT.

This capability can be configured using the **ssl-module** command with the **QAT** option, which enables the SSLi support.

NOTE: Only a few ACOS Thunder platforms support QAT. To check the support, use **show hardware** command.

Known Limitation

The following features are not supported for Intel QAT:

- Explicit and Transparent Proxy
- Static Port type STARTTLS
- STARTTLS Interception
- TLS (Transport Layer Security) 1.3
- AAM
- aFleX

Web Reputation for SSLi Bypass

The SSLi bypass decision-making process now supports the Web Reputation capability that boosts the URL security and limits the risk of inappropriate or malicious web content. As per the standards, the Web Reputation scores range from (1-100) with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious, High

Risk and customized scores. Based on this score, the SSLi decides to intercept or bypass the URL and forward policy decides to redirect, forward, or drop. Additionally, this feature is also supported on aFlex.

The configuration is available in both CLI and GUI under the Client-SSL and Forward Policy templates along with aFlex.

CLI Configuration

- Under Web-Category

  `reputation-scope` - When this is set, you can bind this setting to the forward policy template for destination rule.

```
ACOS(config)# web-category
ACOS(config-web-category)# reputation-scope scope_1
```

- Under Forward Policy Template

  `web-reputation` - When the web-reputation score is greater than or equal to the setting level or customized score, then trigger the corresponding action setting.

```
ACOS(config)# slb template policy BLUE
ACOS(config-policy)# forward-policy
ACOS(config-policy-forward-policy)# require-web-category
ACOS(config-policy-forward-policy)# action A1
ACOS(config-policy-forward-policy-action)# source S1
ACOS(config-policy-forward-policy-source)# destination web-reputation-scope scope_1 action A1 url priority 120
```

- Under Client-SSL Template

  - `web-reputation` - When the web-reputation score is greater than or equal to the setting level or customized score, the request would be bypassed.

```
ACOS(config)# slb template client-ssl SSL_webreputation
ACOS-(config-client ssl)# forward-proxy-bypass web-reputation
{trustworthy | low-risk | moderate-risk | suspicious | malicious | <1-100>}
```

  - `exception-web-reputation` - When the web-reputation score is less than or equal to the setting level or customized score, the request would be

intercepted.

```
ACOS(config)# slb template client-ssl SSL_webreputationexception
ACOS-(config-client ssl)# forward-proxy-bypass exception-web-
reputation {trustworthy | low-risk | moderate-risk | suspicious |
malicious | <1-100>}
```

- `exception-web-category` - When the web category matches the exception category list, the request would be intercepted.

```
ACOS(config)# slb template client-ssl SSL_webrcategoryexception
ACOS-(config-client ssl)# forward-proxy-bypass exception-webcategory
sports
```

- Under Show commands
  - `url-stats` - Shows the statistics of the web-reputation hits in client-ssl template.

```
ACOS(config)# show slb template client-ssl ssl-test url-stats
```

  - `web-reputation bypassed-urls/intercepted-urls` – Shows the URLs which are bypassed or intercepted by web-reputation rules along with URL reputation score.

```
ACOS(config)# show web-reputation bypassed-urls
ACOS(config)# show web-reputation intercepted-urls
ACOS(config)# show web-reputation url-reputation www.google.com
```

GUI Configuration

To configure web-reputation and exception-web-reputation options, go to **ADC > Templates > SSL > Client-SSL**.

aFleX Configuration

To get the URL reputation value:

```
URL::reputation <host> <require-web-category>
```

System Configuration and Administration

ACOS 5.2.0 introduces the following new feature and enhancement for System Configuration and Administration (SAG):

NOTE: For details and Prometheus configuration options, see *System Configuration and Administration Guide* (More generic name of this document is SAG).

Visibility and Analytics Monitoring

ACOS users with critical infrastructure can monitor network resources through visibility and analytics. ACOS supports a logging system to monitor resources like system interface statistics, virtual server, remote server, and virtual port.

All ACOS 5.2.0 platforms have native support for Prometheus. A Prometheus server can query various analytics as specified in its configuration. Users and systems can now use the following functionalities:

- Create and view dashboards to communicate with the Prometheus server using a Visualization and Analytics tool, like Grafana.
- Query any API statistics configured in the Prometheus server's YAML file.
- View the default metrics logged, when no filters are specified:
- All Interface Metrics
- CPU Usage
- Memory Usage

Thunder Container (cThunder)

ACOS 5.2.0 introduces the following new features and enhancements for Thunder Container (cThunder):

Thunder Container or cThunder is a containerized ACOS image that is deployed by using Docker on a host operating system. You can configure ACOS to operate as an

ACOS Series Server Load Balancer (SLB) or Carrier Grade Networking (CGN) device. Thunder Container (cThunder) supports many of the same features as the Thunder hardware-based models, but the exact set of supported features varies based on whether Thunder Container (cThunder) is running an Server Load Balancing (SLB) or a CGN.

NOTE: For more information, refer *Installing Thunder Container on Docker Guide*. For more information and details on related aXAPI statistics and counters, refer *Thunder Container Kubernetes Guide*.

The following topics are covered:

Container Support with Docker

Docker is a tool that enables you to create, deploy, and run applications by using containers. A container enables applications to run in isolation on top of a host operating system, such as Linux or Windows.

Containers enable the developer to package an application with all the required components, such as libraries and dependencies. This package is called a container image. When you run a container image in an isolated environment on top of the operating system, it is referred to as a container instance. The Docker Engine interfaces between the host operating system and a container.

Increased CGNAT and Gi Firewall Resources

The virtual CGNAT solution provides high-performance, highly transparent network address and protocol translation that provides:

- Extension of IPv4 network connectivity for service providers.
- Transition to IPv6 standards simultaneously.
- Security for subscriber services and infrastructure.

Thunder Container (cThunder) provides increased support to deploy the A10 Networks Virtual Carrier Grade NAT (vCGNAT) solution for mobile and residential networks.

Thunder Container (cThunder) a Virtualized Appliance

A10 Thunder Container (cThunder) software provides a flexible, easy-to-deploy, high-performance, and secure application services that runs on any choice of Hypervisors, or in the Cloud, for maximum speed and efficiency.

FlexPool Licensing Model

Capacity pooling provides consumption flexibility, to distribute A10 secure application services, where and when they are needed. A scalable capacity pool uses the cloud consumption model to dynamically allocate services and eliminate over provisioning of resources.

Scaleout Technology Support

Scaleout solution allows multiple Thunder Containers to form a cluster and provide the same set of services as a single infrastructure. Scaleout technology enables CGN, Gi or SGi Firewall, and standalone Firewall services to be provided across multiple devices for load distribution and better scalability.

Combined CGNAT and Gi Firewall Functionality Support

This solution provides a combined CGNAT and Gi Firewall functionality inside the single Thunder Container (cThunder) solution to decrease latency as a consolidated and integrated layer.

Memory Support

To accommodate a high number of users, and their throughput in a virtualized environment, Thunder Container (cThunder) supports 128 GB memory to provision utility resources.

For provisioning the resources, both NUMAs inside the compute host are used. Memory allocation is 64 GB for NUMA0 and 64 GB for NUMA1.

NOTE: This feature supports all platforms with 2 NUMA, 128 GB memory, and 35 virtual CPUs. The memory allocation limit changes according to the available memory.

Web Application Firewall

ACOS 5.2.0 introduces the following new features and enhancements for Web Application Firewall (WAF):

NOTE: For WAF specific configuration steps, refer *Web Application Firewall Guide*.

The following topics are covered:

Enhanced Violation Detection and Reporting

Until now, the Web Application Firewall (WAF) would detect a violation and perform the responsive action immediately to mitigate the attack.

It would not process further checks to uncover more violations after the first one. Violation detection mechanism is now enhanced so that WAF does not stop after the first violation; instead it continues to process and detect a maximum of 6 violations.

In case of a violation, the WAF performs one of the following actions:

- Allow
- Deny
- Redirect
- Sanitize
- Mask

After the 6th violation is detected, the WAF performs a responsive action immediately (except for **Mask** action). The responsive action is based on the severity and priority of the violations detected. All the detected violations are logged in the WAF reports.

HTTP Policy Enhancements

Currently, rules can be configured in an HTTP policy template to match the host, URLs, or cookie names.

Based on the rule that matches, the service group or WAF template is assigned. To improve the granularity of these rules, a new command named **multi-match-rule** is introduced to bind multiple conditions with a given rule. The **multi-match-rule** objects are matched according to the sequence number specified.

For example, if the incoming HTTP request satisfies two rules, the rule with the smaller sequence number is selected. The Web Application Firewall (WAF) template associated with this rule is used.

CLI Configuration

The following example demonstrates the usage of **multi-match-rule**:

```
ACOS(config)# slb template http-policy http-policy4.2.6
ACOS(config-http-policy)# multi-match-rule A 1024
ACOS(config-http-policy-multi-match-rule)# host starts-with A1
ACOS(config-http-policy-multi-match-rule)# url contains exampledomain
ACOS(config-http-policy-multi-match-rule)# cookie-name contains F1
ACOS(config-http-policy-multi-match-rule)# template-waf http-policy-waf-
A
```

Additionally, two new condition types are introduced in the HTTP policy template: **header-name** and **header-value**. These conditions also support the match options **equals**, **starts-with**, **contains**, and **ends-with**.

Introduced Samesite Attribute and Non-SSL Cookie Prefix Check

When a browser sends a request to a website, the browser checks and sends matching cookies that belong to that website (first-party). This behavior is also

repeated for requests made by third-party websites through the browser. However, this may result in Cross-Site Request Forgery (CSRF) attacks.

To mitigate these attacks, the **samesite** cookie attribute is introduced. Using this attribute, you can specify whether your cookie is restricted to a first-party or third-party context. The attribute can be set to **strict** or **lax** or **none**, **lax** being default. The command **add-samesite** adds the **samesite** attribute to the set-cookie header if it is not already added by the server.

Similarly, Non-SSL cookie prefix check is introduced to check if the cookie names in the client's HTTP request are prefixed with **__Secure-** or **__Host-** and if the cookies have a secure origin (for example, client HTTP request coming in to SSL or TLS-enabled vPorts). Cookies from non-secure origins (for example, client HTTP request coming in to non-SSL enabled vPorts) are considered as violations.

CLI Configuration

The following example demonstrates the usage of **add-samesite** command:

```
ACOS(config)# waf template waf-prefix-samesite
ACOS(config-waf)# cookie-security
ACOS(config-waf-cookie-security)# set-cookie-policy sto allow add-http-only add-secure add-samesite strict
```

After configuring the command **non-ssl-cookie-prefix**, Web Application Firewall (WAF) allows **__Secure-** or **__Host-** cookie name prefixes on SSL (Secure Sockets Layer) or TLS (Transport Layer Security) enabled vPorts.

```
ACOS(config)# waf template waf1
ACOS(config-waf)# http-protocol-check
ACOS(config-waf-http-protocol-check)# non-ssl-cookie-prefix
```

NOTE: This check is case sensitive.

Contact Us