Active Network Intelligence 24.40.02 (LTS) Release Notes

05-00496-D03

Revision: 1.0
2023-2-16

Comments

If you have any comments, questions, or ideas in relation to the content in this documentation, we welcome your feedback. Please send your feedback to Sandvine via email at docs@sandvine.com.

Contacting Sandvine

To view the latest Sandvine documentation please visit: https://docs.support.sandvine.com. A valid Sandvine portal account is required to be able to access this site, so if you require an account please register at https://www.sandvine.com/support by clicking on: Sign up now!. For a list of the Sandvine Sales and Support Offices, please access this link: http://www.sandvine.com/about_us/contact.asp.

Table of Contents

1. Release Notes: Active Network Intelligence 24.40.02

1.1. Release Train—Long Term Support

This is a **Long Term Support** train release.

Release train	Description
Long Term Support	The Long Term Support (LTS) train is intended for customers wanting a baseline of functionality without introducing features in subsequent patches. Sandvine will support these releases with Maintenance Release (MR) patches that contain only defect fixes.
Technical Release	The Technical Release (TR) train is intended for customers wanting early access to new functionality. Sandvine provides support for these releases with subsequent TRs that may contain additional features and defect fixes. • A new TR will obsolete the prior release on that stream. For example, 22.02.00 will obsolete 22.01.00. • A new LTS release will obsolete all prior TR. For example, a 22.20.00 LTS release will obsolete 22.01.00, 22.02.00, and all other prior TR releases. • If an issue is observed in the current TR, the resolution will be available in a later TRs on that stream or the next LTS release for that stream.

1.2. Related documents

Related documentation is available from the Sandvine Customer Support website.

Document	Document Number
ActiveLogic Product Guide	05-00499
ActiveLogic Installation and Initial Configuration Guide **Note** Content of this guide is taken from the [ActiveLogic Product Guide]. This guide describes the installation, the initial configuration, and the upgrade of ActiveLogic.	05-00476
Active Network Intelligence CLI Reference Guide	05-00396
PIC Product Guide	05-00433
ActiveLogic SNMP Guide **Note** This guide is introduced in ActiveLogic 24.20.00 LTS. A new chapter for Alarms is introduced in this guide for all platform-related alarms. This new chapter contains information such as impact and troubleshooting steps.	05-00518

Document	Document Number
iQ31020 Hardware Platform Guide	05-00456
iQ42080 Hardware Platform Guide	05-00530
iQ42300 Hardware Installation Guide	05-00434
iQ52600 Hardware Platform Guide	05-00455
iQ52600 Quick Start Guide	05-00459
[Virtual KVM Platform Guide]	05-00388
Virtual vSphere Platform Guide	05-00470

1.3. New features

No new features are introduced in this release.

1.4. Enhancements

This section describes the enhancements made in this release.

1.4.1. High Traffic Rate for Maestro Security Engine

Issue ID:	PRE-25509
Description:	The performance of PacketLogic Daemon (PLD) and web LiveView daemon (PLHTTPD) is improved to support a high traffic rate for Maestro Security Engine.

1.5. Resolved issues

The following issues are resolved in this release:

Description	Identified in	Issue
Title: PLSD Unnecessarily Sends Kafka Request for Topics **Description**: Even if you disable topics like traffic records, score records, and flow records in the system configuration, PacketLogic Statistics Daemon (PLSD) still sends Kafka requests for these topics.	ActiveLogic 23.20.00	PIC-8379
Title: Traffic Passes as Unknown **Description**: ActiveLogic runs traffic classification modules in a secondary execution context with a configurable timeout (PLOS_CONTEXT_TIMEOUT). The secondary execution context experiences a false timeout if the engine's process pauses for some reason and causes traffic to pass as unknown.	ActiveLogic 23.40.04	PRE-25245
Title: ActiveLogic Fails to Save the **Delayed Ack** ConfigurationValues Correctly **Description**: In ActiveLogic Client, when you configure the values in the **Delayed Ack** tab for any AccelerateObject item and save, ActiveLogic fails to save the values correctly. Due to incorrectly saved values, the acceleration traffic stalls in the engine.	ActiveLogic 24.40.00	PRE-25700

1.6. Caveats

The following caveats apply to this release:

Channel-Role is Not Set when Using channel-bind-mode	
Issue:	DIST-4446
Identified in:	PacketLogic 21.60.02
Description:	When using `channel-bind-mode`, the role is not set in the channel-editor.
Impact:	You have to manually set the channel-role after changing it in `channel-bind-mode`.
Workaround:	Set the role manually either in the channel configuration through ActiveLogic Client or through ActiveLogic python-API.

Admin or AUX Connectivity is Lost on OpenStack Deployments with Engine Mode Set to PLOS	
Issue:	DIST-5737
Identified in:	ActiveLogic 22.08.00
Description:	When core services restart on OpenStack deployments with PacketLogic Operating System (PLOS) engine mode, admin/aux connectivity is lost.
Impact:	Admin or AUX interface is unable to send out the packets from the virtual ActiveLogic.
Workaround:	Set the role manually either in the channel configuration through ActiveLogic Client or through ActiveLogic python-API.

Disable Restore of the Configuration Backup from Pre 14.1.2.8 Systems onto 15.0 and Later Systems	
Issue:	DIST-6071
Identified in:	ActiveLogic 24.20.00
Description:	The SNMP Severity level is not available in PythonAPI.
Impact:	Unable to use PythonAPI to extract SNMP Severity level.
Workaround:	None

SNMP Response Time is Increased	
Issue:	DIST-6103
Identified in:	ActiveLogic 23.20.00
Description:	In ActiveLogic, the Net-SNMP daemon stalls while populating networking information (such as IP address, network interface, open TCP socket, and routing) in its MIB values.
Impact:	A network-monitoring tool, which does not receive a steady flow of data from Net-SNMP, can cause the network-monitoring tool to consider ActiveLogic as offline.
Workaround:	None

Line Sharing - Device Detection	
Issue:	DRDL-681
Identified in:	ActiveLogic 23.40.00

Line Sharing - Device Detection	
Description:	Encrypted flows do not show device information from the unencrypted flows from the same device.
Impact:	Encrypted flows do not contain device infomation when unencrypted flows from the same device exists.
Workaround:	None.

[PL15000] Shaping with Limit on PPS/CPS is Not Working Correctly	
Issue:	PRE-5964
Identified in:	PacketLogic 20.30.02
Description:	ShapingObjects with limits for packets per second (PPS) or connections per second (CPS) are not properly synchronized among Flow Processors (FP). This causes every FP to use the full limit for such ShapingObjects. This limitation only affects PL15000.
Workaround:	None.

[E10K] ActiveLogic Crash Loop After Enabling Channel	
Issue:	PRE-6831
Identified in:	PacketLogic 21.43.00
Description:	When using an Intel e10K NIC driver and after enabling another channel in PLOS, the system might enter a diagnostic loop.
Workaround:	A full chassis restart is required to perform a reset of the Ethernet controller.

Optics Monitoring Works Only with NVM Version 6.01 (and above) on NMC with i40e Driver	
Issue:	PRE-8816
Identified in:	PacketLogic 21.64.00
Description:	The NICs with Intel i40e driver must have NVM version 6.01 or above. The transceivers fail to generate optics monitoring data if NICs with Intel i40e driver has an NVM version lower than 6.01.
Workaround:	The NICs with Intel i40e driver must be upgraded to NVM version 6.01 or above.

i40e Virtual Function Restarts Repeatedly	
Issue:	PRE-18520
Identified in:	ActiveLogic 22.20.05
Description:	When the i40e-based cards are used in traffic mode and a channel is enabled, the PLOS engine restarts repeatedly.
Impact:	ActiveLogic does not process any traffic.
Workaround:	Reboot the ActiveLogic instance.

Link State Events are Not Received from i40e Driver (x710 NICs) on Virtual ActiveLogic	
Issue:	PRE-20061
Identified in:	ActiveLogic 23.40.00

Link State Events are Not Received from i40e Driver (x710 NICs) on Virtual ActiveLogic	
Description:	In DPDK mode, virtual ActiveLogic does not receive link state updates (link going down or coming back up) from the PF driver of i40e/x710 NIC.
Impact:	For virtual ActiveLogic in DPDK mode with x710 based NIC: • Link state propagation (LSP) does not work. • Protected channel (with Niagara bypass) remains unchanged when link state changes.
Workaround:	None.

Enabling QUEUESYNC_SCALING_ENABLED with Split by Shapers Greater than 1.1Gbps Cause Over Shaping	
Issue:	PRE-23369
Identified in:	ActiveLogic 23.20.00
Description:	Input traffic can lead to over shaping in a configuration that meets the following conditions: • The QUEUESYNC_SCALING_ENABLED configuration is enabled in a multi NUMA node ActiveLogic device such as iQ42300, iQ52600, or virtual ActiveLogic. • Shapers greater than 1.1Gbps are split by any option other than `none`. Therefore, it is recommended that you avoid this configuration.
Impact:	This affects the shaping accuracy.
Workaround:	Disable the QUEUESYNC_SCALING_ENABLED configuration.

[PythonAPI] System Diagnostic Support for Float Numbers	
Issue:	PY-326
Identified in:	PacketLogic 21.64.00
Description:	The Python API gets raw values for the following float types: • Transmit bias current • Transmit power • Transceiver temperature • Receiver voltage • Receiver power The raw values are received from the transceiver and are not converted into proper units.
Impact:	Python API does not support float type.
Workaround:	None.

Performance Degrades in X710 After Upgrading to Ubuntu 20.04	
Issue:	FEA-829
Identified in:	ActiveLogic 24.20.00
Description:	When you upgrade the KVM hypervisor from older version to Ubuntu 20.04 and use i40e pf driver 2.1413, ActiveLogic has a higher steal time.
Impact:	ActiveLogic performance reduces in terms of traffic throughput.
Workaround:	None

1.7. Limitations

The following limitations apply to this release:

PL1800	
Identified in:	PL1800
Description:	The H750P RAID controller in PL1840, PL1860, PL1880, and iQ1881 hardware platforms requires the PERC CLI management tool for configuration. Due to this, you cannot have another RAID controller internally or externally that requires a Mega CLI management tool. This will affect the SN1201/SN1204 Storage Node that connects to an external RAID controller.

iQ31020	
Identified in:	iQ31020

Description:	• With PLOS engine mode, iQ31020 platform does not support `Auto-Negotiation` on 10Gb links.
	• Link partners should be set to a fixed speed, if the platform fails to bring the link up.
	• When ActiveLogic transitions from bypass state to active state, a delay of:
	  • up to 2 seconds is observed for X710 channels to be detected as up in PLOS engine mode.
	  • 1 second is observed for X710 channels to be detected as up in DPDK engine mode
	During this brief period, the traffic forwarded from bypass device is dropped.

iQ42300	
Identified in:	iQ42300

Description:	• iQ42300 does not support hot swappable NIC interfaces. The chassis requires a restart to support the newly added NICs.
	• During engine restart, a delay of up to 5 seconds is observed for Mellanox NICs (CX5 and CX6) to be detected as up and running because of inherent nature of the cards, and not the limitations in engine to detect the cards. During this brief delay, any traffic forwarded by the Bypass card is dropped.
	• Currently, the `mii-bonding` of AUX interfaces is not supported on iQ42300 platform. The workaround is to use ARP-bonding. For more details, see *Generic LACP (802.3ad + VLAN Tags) support for system interfaces* section in *Active Network Intelligence 23.40.00 (LTS) Release Notes*.
	• While migrating from PLOS engine-mode to DPDK engine-mode on iQ42300 platform, BALANCER_NODE is set to 1, even if PLOS_BALANCER_LOCAL_NODE is false. This causes the traffic to be handled only within the local node. BALANCER_NODE should be manually set to 2, to avoid this.
	• When ActiveLogic transitions from external bypass state to active state, a delay of:
	  • up to 2 seconds is observed for X710 channels to be detected as up in PLOS engine mode.
	  • 1 second is observed for X710 channels to be detected as up in DPDK engine mode
	During this brief period, the traffic forwarded from bypass device is dropped.

iQ52600	
Issue ID:	DIST-4826
Identified in:	ActiveLogic 22.26.00

iQ52600	
Description:	**PERC H345 RAID controller** RAID monitoring using `snmp` is **not** supported on iQ52600. Refer to the storage status in Dell iDRAC. **PERC H355 RAID controller** RAID monitoring using `snmp` is supported on iQ52600.

PL15000	
Identified in:	PL15000
Description:	• 40G pluggable network modules (PNMs) are not supported. • Shelf Management Mezzanine (ShMM) is only accessible using the left RJ45 Ethernet port. • Multiple Divert VLANs are not supported on the same channel. • When using legacy style NetObject tree provisioning, dynitem operations in triggers are not natively supported. Trigger scripts must be modified. • The `request system diagnostics` CLI command is not applicable for PL15000 platform.

ActiveLogic with NMC Model P/N:PL-09102	
Identified in:	ActiveLogic with NMC model P/N:PL-09102
Description:	Hot swap of SFPs on the PL-09102 are not registered. The old value is kept.

[E1K] PLOS Does Not Bring i350 Fiber Interfaces in a Virtual Environment	
Issue:	PRE-3487
Identified in:	PacketLogic 17.2.0
Description:	i350-based 1Gbps network adapters with fiber interface are not supported in this release. Do not search ethernet controller chipsets to determine speeds affected.

Line Sharing - Device Detection	
Identified in:	ActiveLogic 23.40.00
Description:	Latency in syncing the device information for new connections appear as unsupported traffic. • For Liveview, this latency is observed for a brief period of time. • The connections without synced device information appear as unsupported in statistics reporting.

Line sharing - Device Detection (Limitations Based on Subscriber Device)	
Applies to:	As per the subscriber device.

Description:	• ActiveLogic does not have the capability to identify devices when the client scrambles the TCP timestamp.
	
	  • Subscriber devices based on Linux kernel version 4.9 (and above), scrambles the timestamp field in TCP options.
	  • Mac and iOS devices scramble the TCP timestamp.
	
	• Windows devices are capable of randomizing source ports for TCP connections. Hence, in such scenarios, the device detection is not possible.
	
	  • ActiveLogic detects the usage of randomized ports, and stops associating device ID to the connection.
	  • Randomized port usage is detected independently on each ActiveLogic node in a cluster.

1.8. Behavior changes

This section lists the behavior changes observed when upgrading to this release.

> **Note**
>
> ActiveLogic 24.40.00 is the last release in which Python2 API is updated. After this release, Python2 API will be available but it will not be updated to support any new features. It is recommended that you migrate to Python3 API.

1.8.1. Channel configuration in DPDK engine-mode for virtual ActiveLogic

Description:	The channel configuration is done manually in DPDK engine-mode for virtual deployments of ActiveLogic. When resetting engine-mode, manual channel configuration is needed. For more details, see virtual guides (*Virtual KVM Platform Guide* / *Virtual vSphere Platform Guide*) to configure channels. • When upgrading from older releases, a migration script moves the configured channels. • When migrating from PLOS, a migration script moves the configured channels.
Applicable when upgrading from:	ActiveLogic version 23.20.00 and onwards.

1.8.2. License check

Description:	When upgrading, a license check is performed to determine whether subscriber-identifying values are obfuscated. The following four separate license modules control the functionality:
	
	• Statssubsensitive: Controls whether data written to StatsFS is obfuscated.
	• insightssubsensitive: Controls whether data sent to Insights Data Storage is obfuscated.
	• Ipfixsubsensitive: Controls whether flow records exported by IPFIX are obfuscated.
	• Obfuscate HTTP Inject License:
	
	   • Allows the operator to selectively create HTTP inject responses without the VIA marker.
	   • When the Obfuscate HTTP Inject license does not exist, the system generates HTTP Inject responses which include a VIA HTTP Header to clearly indicate the response was generated by a middlebox and not the origin server.
	   • The obfuscate license only controls whether the operator is allowed to disable the insertion of the VIA header or not. A system configuration setting is used to enable or disable the obfuscation.
	
	If the license modules are present, there is no change in behavior upon upgrading. If the license modules are *not* present, subscriber identifying values will be obfuscated regardless of the configuration.

Applicable when upgrading from:	Applicable to all versions.

1.8.3. Upgrading ActiveLogic and PIC

Description:	When upgrading ActiveLogic systems and PIC control nodes, make sure that both platforms are upgraded at the same time.
Applicable when upgrading from:	Applicable to all versions.

1.8.4. Load balancing traffic

Description:	When upgrading from 19.0 or earlier versions to 20.30 or later, all traffic will be load balanced locally.
	This means that the CPU load might behave differently depending on how the NMCs are set up on the system. If, for example, you have only NMCs/interfaces on one NUMA-node, packets will only be received locally.
	When upgrading, you need to have the same amount of NMCs/traffic interfaces on both NUMA nodes, to make them receive the same amount of traffic. Configure the NUMA node as specified in the table.

NUMA node	Slot
0	1/3, 1/4, 2/3, and 2/4
1	1/1, 1/2, 2/1, and 2/2

> **Note**
>
> These slot numbers are applicable only to the following platforms:
>
> - PL8840v1 and v3
> - PL8960v1 and v3
> - PL9420v1, v2, v3, and v4

Applicable when upgrading from:	PacketLogic version 19.0 or earlier to PacketLogic version 20.30 and onwards.

1.8.5. CPU on each NUMA node

Description:	When upgrading from 19.0 or earlier versions to 20.30 or later, there will be a CPU on each NUMA node.
	CPU0 is a central part of PLOS and handles NIC-RX drops, LB-drops, and other PLOS-related tasks. With NUMA, there will be one more CPU per NUMA node handling similar tasks. Communication with user-space and other daemons will still be handled by CPU0.

Applicable when upgrading from:	PacketLogic version 19.0 or earlier to PacketLogic version 20.30 or later.

1.8.6. Proxy configuration

Description:	The **Resource Manager** proxy configuration is improperly migrated during upgrades to firmware version 19.0.
	As a result, the system fails to load the configuration and boots with settings restored to defaults.
	The workaround is to disable the proxy setting before upgrading the system. If *File Server* is proxied, then it is recommended that you manually upload the package through ActiveLogic Client, and perform a local upgrade.
Applicable when upgrading from:	Earlier PacketLogic versions to 19.0.

1.8.7. Resource copy

Description:	In general, resource copy is supported between release X.Y.* unless otherwise stated.
	SSHD: The default set of ciphers and MACs has been altered to remove unsafe algorithms. In particular, CBC ciphers and arcfour* are disabled by default.
	In OpenSSH version 7 and later, DSA key support is disabled by default due to its inherit weakness. Because of this, the DSA key will be replaced by an RSA key when ActiveLogic is upgraded to version 17.0 and later.
	During the ActiveLogic upgrade, a migration is executed where the old DSA key will be replace by an RSA key. Both old and new public key will be shown during this stage to let you see what DSA key you were using and what the new RSA key will be.
	It will only be possible to use RSA keys going forward. The compatibility option in ssh_config has been removed as well as the possibility to offer DSA keys.
	During the ActiveLogic upgrade, a migration is executed where the old DSA key will be replace by an RSA key. Both old and new public key will be shown during this stage to let you see what DSA key you were using and what the new RSA key will be.
	It will only be possible to use RSA keys going forward. The compatibility option in ssh_config has been removed as well as the possibility to offer DSA keys.
Applicable when upgrading from:	PacketLogic version 17.0 and onwards.

1.8.8. Migrator scripts

Description:	The migrator scripts which migrate TUI configurations to ConfD during firmware upgrade have been improved. When a firmware upgrade is started, the scripts will validate the configurations before migrating them from TUI to ConfD, and for a better user experience will display all configuration issues. The process is as follows:
	
	1. Firmware upgrade is started through CLI.
	2. Before the actual firmware upgrade starts TUI configurations are validated to check if they are compatible with ConfD.
	3. If there are any issues with the TUI configurations, the incompatible TUI configurations will be listed and the firmware upgrade is aborted.
	4. The user is prompted to correct any invalid configurations.
	5. The user corrects issues and restarts firmware upgrade and validation is started once more.
	
	Logs will be generated when TUI configurations are validated and during the firmware upgrade which will let the user know if the migration of the TUI configurations passed/failed.
	
	This is a sample output of configuration issues when upgrading the firmware:
	
	<pre>Downloading ftp://1.2.3.4/builds/latest-xeon-plos_64.tar.gz.gpg
	
	% Total % Received % Xferd Average Speed Time Time Time
	 Current
	                                Dload Upload Total Spent
	 Left Speed
	100 256M 100 256M 0 0 41.2M 0 0:00:06 0:00:06 --:--:--
	 41.9M
	Decrypting image
	Extracting image
	Running install.sh
	One or more admin/aux interfaces have the same IP address.
	 Please ensure each admin/aux interface has a unique IP
	 address.
	
	Above issues will cause migration of TUI configurations to
	 fail. Please fix above issues and retry firmware upgrade.
	
	firmware-install: Installation aborted
	Firmware upgrade failed</pre>
	
	ⓘ Important
	
	For upgrades using Deployer tool
	Incompatible TUI configuration messages during firmware upgrade cannot be viewed (in the Deployer) when upgrading the system using Deployer.

Applicable when upgrading from:	PacketLogic version 18.x and onwards.

1.8.9. Upgrading from a TUI firmware to a ConfD firmware

Description:	When a system is upgraded from a TUI based firmware (<= 18.1) to a ConfD based firmware (>= 19.0), the configurations are migrated from TUI to ConfD. In earlier releases, if migration of configuration failed, then the connectivity to the system was lost. Now, during upgrade to a ConfD based firmware the connectivity of the system is maintained even if migration fails. You should be able to access the system through a temporary SSH using the IPv4 address of the system. You can SSH to the system as a `recovery` user using port 42043. When logging in as a `recovery` user, a **recovery menu** is displayed using which you should be able to fix the migration failure.

```
ssh recovery@<system-IP-address> -p 42043
recovery@<system-IP-address>'s password:
Last login: Mon Dec 7 04:15:18 2020 from 1.2.3.4

Recovery
========================================

V) View logs relevant to ConfD startup failure or TUI
 configurations migration failure
L) View recent logs related to ConfD
E) Edit configurations migration files
R) Restart ConfD and load the edited migration files
O) Reboot the system
C) Create support bundle
S) Secure copy support bundle to remote host
X) Exit
```

Description: (continued)

> **Note**
>
> The **recovery menu** is accessible through the console as well (if you are upgrading the system through serial console).

> **Note**
>
> If the password of `pladmin` user is customized, then the password for `recovery` user is same as `pladmin` user. If `pladmin` user has the default password, then the password of `recovery` user is set to `password`.

You can do the following using the recovery menu:

- View the logs to determine the cause for migration failure.
- Edit migration files and restart ConfD to fix the migration failure.
- Create support bundles, and securely copy the bundles to remote systems. The support bundles can be used as input for Sandvine Customer Support for recovering from the migration failure.
- Reboot the system.

> **Important**
>
> - Ensure that the system is rebooted after fixing the migration failure. This is required to ensure proper working of the system.
> - Ensure that the ConfD is restarted to replace the old incorrect configurations with the new correct configurations.
> - After fixing the migration failure, the temporary SSH connectivity is lost when the system is rebooted. After reboot, the system becomes accessible through the usual admin SSH.
> - If the admin SSH port is set to 42043, then the recovery SSH is available through port 42044.

Description: (continued)	**Note** The temporary SSH connectivity is not setup if the system has only an IPv6 address and does not have a working IPv4 address. **Important** Fix all the ConfD migration errors before proceeding to reboot the system. The system might end up in a bad state, if the errors are not fixed and rebooted.
Applicable when upgrading from:	PacketLogic TUI based firmware (<= 18.1) to PacketLogic ConfD based firmware (>= 19.0)

1.8.10. TTL tracking

Description:	The following system configuration values for TTL tracking are removed: • TTL_TRACKING_SERVICE_OBJECT_PATH • TTL_TRACKING_CLEAR_ON_DYNCHANGE The legacy TTL count tracking is replaced by the new HopLimitObject.
Applicable when upgrading from:	PacketLogic version 20.30.0 and onwards

1.8.11. Flow priming improvements

Description:	The flow priming improvements (FEA-304) can have an impact on Thread 0 CPU load. If the system is running above 80% load on Thread 0 CPU, then certain trade-offs between CPU, memory, and classification might be required. The tuning guidelines are described in *Tuning DRDL key-value store* section in *ActiveLogic Product Guide*. Please consult your Sandvine representative to review the DRDL key-value store configuration before upgrading.
Applicable when upgrading from:	ActiveLogic version 22.24.00 and onwards.

1.8.12. Increase in memory usage

Description:	To support some of the functionality added in release 21.35.00, the amount of memory used by the system has increased. When deploying ActiveLogic systems on a hardware with 8 GB RAM, the following configuration parameter has to be adjusted to not exceed the recommended value: MAX_CONNECTION: maximum value 250000
Applicable when upgrading from:	PacketLogic version 21.35.00 and onwards.

1.8.13. Flow priming memory usage

Description:	To support flow priming improvements the amount of memory used by the system has increased from 22.25.00 TR release.
	When deploying ActiveLogic systems with lesser memory the following configuration parameters should be reduced and adjusted:
	• MAX_CONNECTIONS • DRDL_KVSTORE_POOLSIZE_0 • DRDL_KVSTORE_POOLSIZE_64 • DRDL_KVSTORE_POOLSIZE_255
	The tuning guidelines are described in *Tuning DRDL key-value store* section in *ActiveLogic Product Guide*.
Applicable when upgrading from:	ActiveLogic version 22.25.00 and onwards.

1.8.14. External authentication

Description:	In previous releases (**version 18 and earlier**), for external authentication feature, the SSH login local fallback cannot be disabled through the configuration that was used to disable local fallback. The local fallback was **always** enabled irrespective of the configuration. From **version 19 and above**, the SSH login local fallback is also disabled through the configuration that is used to disable local fallback, like other login such as ActiveLogic Client.
Applicable when upgrading from:	PacketLogic version 19 and onwards.

1.8.15. Removal of legacy shaping counter functionality

Description:	In previous releases, shaping counters were used in conjunction with volume-based shaping and quota management. The shaping counters are legacy functionality, and were only kept for backwards compatibility.
	Legacy shaping counter functionality is hidden since 21.60.00 LTS release, and will be removed in 23.40.00 LTS release.
	SessionContext counters have replaced this functionality.
	For systems that are using shaping counters functionality, and migrating to 23.40.00 LTS release, **must** migrate to **provisioning** using SessionContext before upgrading.
Applicable when upgrading from:	ActiveLogic version 23.40.00 and onwards.

1.8.16. Enhanced security to IFeeds service on ActiveLogic nodes

Description:	The following command **must** be run on an ActiveLogic node configured as a **relay** server in a deployment:
	`set service intelligence-feeds relay <enabled/disabled>`
	This is to provide enhanced security to IFeeds service on ActiveLogic nodes.

Applicable when upgrading from:	ActiveLogic version 23.22.00 and onwards

1.8.17. Consistency in licensing terminology and behavior

Description:	After upgrade, the following behaviors are observed:
	
	• After Support-End Expiry
	
	  • any new firmware installations or upgrades are blocked.
	  • any new psf installations are blocked.
	  • any new DRDL signature upgrades are blocked.
	  • any new Intelligence Feeds updates are blocked.
	• License-End Expiry results in:
	
	  • Traffic shunting in ActiveLogic.
	  • Services which require license stops working.
	  • An incident is generated.
	• The output of `show system license` CLI command, displays the information based on the licensing models used (for example, License Manager 1.0, License Manager 2.0).

Applicable when upgrading from:	ActiveLogic version 23.40.00 and onwards

1.8.18. Higher increase in memory footprint

Description:	Memory footprint increases on upgrading to ActiveLogic version 24.20.00 On the ActiveLogic the memory increases by 32 bytes for every connection. The MAX_CONNECTIONS system configuration influences the increase of memory use in ActiveLogic version 24.20.00. For example, if MAX_CONNECTIONS = 5 million, then, Memory increase = 5 million x 32 bytes = 150MB Hence, 1 GB of memory decrease in packet-processing memory is observed.
Applicable when upgrading from:	ActiveLogic version 24.20.00 and onwards

1.8.19. Licensing of DRDL

Description:	Signature-bundles are not included in the ActiveLogic firmware. You must download the signature bundle manually.
Applicable when installing or upgrading from:	New installations or when upgrading from ActiveLogic 23.20.00 or earlier versions to 24.40.00 or later

1.9. Compatibility Matrix

The ActiveLogic interoperates within a Sandvine deployment based on this system compatibility table. Interoperability is dependent on a variety of factors such as:

- Product—This column identifies the products that ActiveLogic interoperates with.

- Minimum Supported Release—This column identifies the minimum supported software version that this ActiveLogic release can successfully interoperate with.

- Platform—This column identifies the Sandvine element required to host the specific software listed.

> **Note**
>
> Unless indicated otherwise, the recommended release for all compatible products is the latest LTS release (xx.yy.zz) for which the `Major.Minor` part (xx.yy) matches across all deployed and interoperating products.

Product	Minimum Supported Release	Platform
PIC firmware	23.20.00	Virtual, Appliance
Maestro Policy Engine	23.20.00	Virtual, Appliance
ActiveLogic Client	23.20.00	Windows, Mac, Ubuntu
Python API 3.8	23.20.00	N/A
Insights Data Storage	23.20.00	PIC
Elements	24.20.00	PIC, Maestro Policy Engine (Virtual, Appliance)
Deep Insights	23.20.00	Virtual, Appliance
Maestro Security Engine	24.40.01	Virtual

> **Important**
>
> The 32-bit ActiveLogic Client will be deprecated. This will be the last release that Sandvine will offer the windows 32-bit compatible ActiveLogic Client. It is recommended to use the 64-bit version.

1.9.1. Hardware compatibility

The following tables describe the hardware support for this release:

Table 1.1 ActiveLogic

Platform	Supported	Comment
PL8840	Yes	Initial support 15.1.5.12-MR3. V3 hardware support added in 17.2.2.3.
PL8960	Yes	Initial support 14.1.2.28-MR1. V3 hardware support added in 17.2.2.3.
PL9420	Yes	Initial support 15.0.7. V2 hardware support added in 15.0.11.3. V3 hardware support added in 17.2.2.3. V4 hardware support added in 19.0.0.31.
PL15000	Yes	Initial support 16.2.0.3.
Virtual Platforms	Yes	KVM and vSphere v6.7.
iQ31020	Yes	Initial support 22.40.
iQ42080	Yes	Initial support 24.40.
iQ42300	Yes	Initial support 21.60.

Platform	Supported	Comment
iQ52600	Yes	Initial support 22.40.

> **Note**
>
> In AL.23.20.00 release, the following platforms support DPDK engine mode:
>
> - Virtual ActiveLogic
> - iQ52600
> - iQ42300

> **Note**
>
> With engine mode DPDK, ActiveLogic versions 24.20 and later support the iQ31020 hardware platform. The FEA-601 introduces this support.

Table 1.2 PIC

Platform	Supported	Comment
PL1840	Yes	Supported from 16.2.10.2, 17.1.7.1, 17.2.7.12, 18.1.3.13, 19.0.0.31, 20.30.0.20. Replacing PL1620 and PL1640.
PL1860	Yes	Supported from 16.2.10.2, 17.1.7.1, 17.2.7.12, 18.1.3.13, 19.0.0.31, 20.30.0.20. Replacing PL1650.
PL1880	Yes	Supported from 16.2.10.2, 17.1.7.1, 17.2.7.12, 18.1.3.13, 19.0.0.31, 20.30.0.20. Dedicated to Insights Data Storage.
Virtual Platforms	Yes	KVM, vSphere v6.7, and vSphere v7.0.

1.10. Integrated Open Source Software

Sandvine integrates multiple open source products to ensure delivering the best of breed product to the market. Upon customer request Sandvine can furnish the list of open source software utilized within its products and platforms.

1.11. Upgrade Notes

1.11.1. Performance impact

1.11.1.1. CPU utilization

When upgrading between major software releases, there may be a performance impact on ActiveLogic packet-processing CPU utilization when a similar configuration, feature set, and traffic load is used. This impact is due to enhanced or new functionality as well as changes to default system configuration settings. The increase in CPU utilization may be more noticeable when upgrading across multiple major releases. There may also be a larger impact on certain platforms.

The actual impact depends on the traffic mix, load, and platform configuration complexity. If the platform to be upgraded is currently operating in excess of 60% CPU utilization, contact Sandvine Customer Technical Support (CTS) or your solution/resident engineer before performing an upgrade.

1.11.1.2. Intelligence feeds

- **Distributed server redundancy**. In contrast to the hard-coded address list that prevents servers from being added for ContentLogic databases, the distributed server address list supported with the more robust and extensible Intelligence feeds functionality allows download from multiple servers—so, if one becomes unavailable the download the system simply connects to another server on the list. New servers can be added to the list at any time.

- **Self-repair**. The distributed Intelligence feeds database incorporates a self-repair mechanism that detects invalid data and circumvents outages to in customer data sets.

- **Reduced disk overhead**. As URL categories often change, the Intelligence feeds database regularly updates the URL with the latest information, and deletes obsolete files to significantly reduce the disk overhead normally associated with accumulated delta files in ContentLogic databases.

- **Memory requirements**. Additional memory is required to enable the new Intelligence feeds functionality delivered in this release. The following table shows the additional system memory and disk storage requirements for each database type. Additional packet processing memory is also utilized.

Database	System memory required	Packet processing memory required	Disk storage required
Cyber Threat Intelligence	2.6 GB	600 MB	8 GB
DeviceLogic	571.8 MB	0 GB	Negligible
GeoLogic	10.4032 GB	1.74 GB	12.6732 GB
Internet Advertising Database (IAD)	15.5266 GiB	5.54 GB	19.0005 GB
Internet Filtering Database (IFD)	12 GB	8.4 GB	60 GB
IFD_Lite	3.2 GB	2.3 GB	12 GB
Internet Watch Foundation (IWF)	289.2 MB	0.15 GB	Negligible
OTT Microsoft	867.6 MB	0 GB	Negligible

1.11.1.3. Memory usage

DRDL ABI18 signature bundle needs extra 256 MB of memory in packet-processing zone. Ensure about the extra memory before upgrading to this version.

> **Note**
> As part of FEA-784, PLD stores more strings in the string cache, which can have performance impact if the cache size is not enough. For this reason consider increasing STRING_CACHE_SIZE.

1.11.2. SSH hardening within Sandvine products

> 🖋 **Note**
>
> Valid only from version AL 23.03.00 and onwards.

1.11.2.1. SSH protocol usage and security considerations

SSH protocol is used for the following communications within the Sandvine end-to-end solution:

• ConfD for CLI (port 42002)

• ConfD for NETCONF access (port 2022)

• plcommd for Maestro Policy Engine to ActiveLogic communication (port 42007)

• maintenance ssh (port 42042)

Several methods for exchanging keys exist, and establish a secure connection. Sandvine provides the following settings:

Type	ConfD for CLI (port 42002) and NETCONF (port 2002)	plcommd (port 42007)	maintenance ssh (port 42042)
Compression	none zlib	none zlib zlib@openssh.com	none zlib@openssh.com
Encryption algorithms	aes128-ctr aes192-ctr aes256-ctr	aes128-ctr aes192-ctr aes256-ctr	aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com chacha20-poly1305@openssh.com
Host key	ssh-rsa	ssh-rsa	ssh-rsa rsa-sha2-256 rsa-sha2-512
Key exchange (KEX)	diffie-hellman-group-exchange-sha256	curve25519-sha256@libssh.org	curve25519-sha256@libssh.org diffie-hellman-group-exchange-sha256
Message Authentication Code (MAC)	hmac-sha2-256 hmac-sha2-512	hmac-sha2-256 hmac-sha2-512	hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha2-512 umac-128@openssh.com umac-128-etm@openssh.com

1.11.2.2. Migrating to more secure product version

SSH protocol negotiates while connecting to get the most secure configuration possible. Several cryptographic algorithms that were considered to be less secure were removed for SSH hardening. This resulted in License manager and Elements unable to communicate securely with the new and more secure version of the firmware distribution. Support for more secure cryptographic algorithms is added to License Manager and Elements within the following versions:

- Elements 23.03.00

- License Manager 1.0.8

All other parts of Sandvine product use `libssh` which supports secure cryptographic algorithms.

> **Note**
>
> No new configuration is supplied for SSH. Only upgrading to a more secure firmware version is required.

1.11.2.3. Maestro Policy Engine

Maestro Policy Engine supports configuration of SSH ciphers to communicate with `plcommd`. This configuration is deprecated in this (ACtiveLogic 23.03.00) release, and the strongest cipher will be used.

> **Important**
>
> If ActiveLogic is upgraded prior to Maestro Policy Engine, and Maestro Policy Engine is configured to use weak cipher, then it is required to reconfigure Maestro Policy Engine to use stronger cipher. For more information, see *Maestro Policy Engine Release Notes.*

1.11.2.4. Ability to supply licenses

To be able to supply licenses to all Elements in the deployment, upgrade software through either of the following:

1. Elements

   > **Note**
   >
   > For Elements, version 23.03.00 or newer is required.

2. License Manager

   > **Note**
   >
   > For License Manager, version 1.0.8 or newer is required.

1.11.3. Local account enhanced security

You are allowed to configure the following to enhance the local account security:

• Password complexity

• Session idle timeout

• Temporary account lockout

1.11.3.1. Password complexity

Added the following new CLI command to **enable** or **disable** the complexity of the passwords:

```
set system authentication password-complexity <enabled/disabled>
```

Passwords set after enabling the password-complexity feature should satisfy the following conditions:

• Password should have minimum 8 characters.

• Password should contain any three of the following:
   • one lowercase character
   • one uppercase character
   • one numeric character
   • one special character (all characters other than 1, 2, and 3 are treated as special characters)

> **Note**
>
> A warning message is displayed when switching between enabled or disabled, to ensure that the user is aware that passwords set henceforth need to satisfy the password complexity conditions.
> A sample warning message is as follows:
>
> ```
> 'system authentication password-complexity': Enabling or disabling this will
>  impact all the passwords
> set henceforth
> ```
>
> This also affects the users created in ActiveLogic client. A similar warning message is displayed with the password complexity conditions.

> **ℹ Important**
>
> This configuration impacts all the passwords set for the following configurations:
>
> - `set system authentication console password <password>`
>
> - `set system authentication users cli <username> password <password>`
>
> - `set system authentication users integration admin password <password>`
>
> - `set system authentication users integration dataextract password <password>`
>
> - `set system authentication users integration update password <password>`
>
> - `set system authentication users integration update rsync-password <password>`
>
> - `set system authentication users integration debugextract password <password>`
>
> - `system maintain password-admin`

1.11.3.2. Session idle timeout

You are allowed to configure the idle timeout for sessions such as FTP, SFTP, console, Netconf, and ConfD using the following CLI commands:

- `set system netconf-idle-timeout <duration (nYnMnDnHnMnS)>`

  where **n** indicates a numerical value

  For example, `set system netconf-idle-timeout 30M5S`

  - This is a newly added CLI command.

  - This configuration is applicable only for new NetConf connections.

  - Idle session timeout is not applicable for all the existing (opened) connections.

  - The maximum value should not be more than 1 year.

  - The idle timeout for netconf is **disabled** by default.

- `set system idle-timeout <duration (nYnMnDnHnMnS)>`

  where **n** indicates a numerical value

  For example, `set system idle-timeout 1H20M5S`

  - This CLI command already exists for ConfD which is now extended to support other protocols.

  - This configuration is applicable for all ConfD, console, SSHD, SFTP, and FTP connections.

  - This configuration is applicable only for new connections.

- Idle session timeout is not applicable for all the existing (opened) connections.

- The maximum value should not be more than 1 year.

- The default value of idle timeout is 0 second.

1.11.3.3. Temporary account lockout

This configuration is:

- applicable for ConfD, console, SSHD, SFTP, FTP, Netconf, and rsync daemon.

- applicable only for a new session.

- **not** applicable for all the existing (opened) sessions.

The user account is locked for a configurable duration using the following CLI commands when user reaches **N** failed login attempts:

where **N**, and timeout values are configurable

- **`set system authentication temporary-lockout attempts <unit>`**

  For example, **`set system authentication temporary-lockout attempts 5`**

  - The minimum configurable value is 0.

  - The maximum configurable value is 12.

  - The default value is 0.

    > **Note**
    >
    > If **`set system authentication temporary-lockout attempts`** is configured to **0**, then the feature becomes **disabled**.

- **`set system authentication temporary-lockout timeout <duration (nYnMnDnHnMnS)>`**

  For example, **`set system authentication temporary-lockout timeout 20M`**

  - The minimum configurable timeout value is 60 seconds.

  - The default value is 15 minutes.

1.11.4. Upgrade path

Carefully review and consider the notes in the table when you prepare an upgrade.

Related feature	Description
Software upgrade	To perform a software upgrade to version 24.25.00, the system must be running at least the software version 17.2.x.x, 18.1.1.7, 19.0, 20.30, 21.30, 21.60, 22.20, 22.40, 23.20, or 24.40. Supported upgrade paths: • 17.2.x.x -> 18.1.1.7 -> 24.40.02 • 18.1.1.7 -> 24.40.02 • 19.0.0 -> 24.40.02 • 20.30.0 -> 24.40.02 • 21.30.00 -> 24.40.02 • 21.60.00 -> 24.40.02 • 22.20.00 -> 24.40.02 • 22.40.00 -> 24.40.02 • 23.20.00 -> 24.40.02 • 23.40.00 -> 24.40.02 **Note** For PL1800 platforms that are running software version 19.0.0 or later, the normal upgrade paths should be followed. If the PL1800 platform is running a software version earlier than 19.0.0, then the following upgrade paths are supported: • 17.2.x.x -> 18.1.4 -> 24.40.02 • 18.1.4 -> 24.40.02 **Note** For PL9420v4 platforms running software version 19.0 or later, the normal upgrade paths can be followed. If the PL9420v4 is running an earlier version than 19.0 and at least software version 16.2.9, 17.1.6, 17.2.5 or 18.1.4, the following upgrade paths are supported: • 17.2.5 -> 18.1.4 -> 24.40.02 • 18.1.4 -> 24.40.02 **Important** Before upgrading, it is recommended to have console access, and download a backup through the Command Line Interface (TUI or ConfD). This allows Sandvine Customer Support to better assist, if any issues are encountered during the upgrade process.

1.11.5. BIOS Upgrade

On certain platforms before upgrading to this release, it's mandatory to verify that the system BIOS is up to date. Download the software from http://files.support.sandvine.com and follow the upgrade procedure described in Section 1.11.7, "Upgrading BIOS/BMC using the CLI".

Related feature	Description
BIOS upgrade	When upgrading to version 17.2 and later, the following platforms require a BIOS/BMC upgrade: • PL8840 BMC-1.66-BIOS-6.10 • PL8840v3 BMC-1.16-BIOS-1.10 • PL8960v1 BMC-1.66-BIOS-6.10 • PL8960v3 BMC-1.16-BIOS-1.10 • PL9420v1 BMC-1.16-BIOS-1.10 • PL9420v2 BMC-1.16-BIOS-1.10 • PL9420v3 BMC-1.16-BIOS-1.10 • PL9420v4 BMC-1.16-BIOS-1.10

1.11.6. Credentials change

This section provides details on credentials change due to rebranding.

Upgrading to 22.20 or later from earlier versions

When an existing system is upgraded from firmware with ConfD to 22.40 or a later firmware:

- **authentication/cli**

  - If `pladmin` user did not exist before the upgrade, then the `admin` user will **not** be created.

  - If `pladmin` user exists before the upgrade, then the `admin` user duplicates the `pladmin` user. This implies that the `admin` user is created and the password is copied from the `pladmin` user. Therefore, you will be able to login with existing `pladmin/<your earlier system password>` credential and also with `admin/<your earlier system password>` credential.

    > **Note**
    >
    > If you already have an `admin` user in addition to the `pladmin` user, then the existing `admin` user is not touched.

- **authentication/integration**

  The `pladmin` container is hidden and deprecated. An `admin` container is created. If the password of the `pladmin` user is modified before the upgrade, then the password is copied to the new `admin` container. If not, the default password is set to `password`.

- **authentication/console**

  If the password is not configured before the upgrade, then the default password is set to `password`. Console requires the new password to log in.

- **Maintain Group**

  The `maintain` hideGroup in ConfD CLI is removed. From the release 22.20 on onwards, if you need to reach `system maintain ...` in ConfD, then you should unhide `debug` hideGroup. Run **`unhide debug`** and provide `secret` as password.

When an existing system is upgraded from firmware with TUI to 22.40 or a later firmware:

- **authentication/cli**

  An `admin` user is created and the password is copied from `pladmin` user of previous firmware.

- **authentication/integration**

  An `admin` container is created and the password is copied from `pladmin` user of previous firmware.

- **authentication/console**

  The default password is set to `password` and the console password configuration from the previous firmware is copied to the new firmware.

> **Note**
>
> PSFs relying on the legacy default credentials are affected after upgrading the system to 22.40 or later.
>
> To prevent any authentication issues, the legacy `pladmin` account can be added using the following CLI command:
>
> ```
> set system authentication users cli pladmin password <password> role
> admin
> ```

1.11.7. Upgrading BIOS/BMC using the CLI

To upgrade BIOS/BMC using the CLI

> **Note**
>
> This section is applicable only to PL8840, PL8960, PL9420, and PL15000 hardware platforms.

1. Download the BIOS/BMC upgrade file for the Active Network Intelligence platform from https://files.support.sandvine.com.

2. In ActiveLogic Client, open the **File Manager** and upload the file to the Upgrade files folder.

3. Log on to the Active Network Intelligence CLI using SSH or a serial connection.

4. Type **system update firmware file** `filename`.

5. Follow the instructions on the screen.

6. Type **restart system reboot** to reboot.

7. Type **yes** to proceed.

1.11.8. Advantech NIC Firmware Upgrade

Before upgrading the firmware, ensure that you upgrade the Advantech NIC firmware PL-0123A-4SR and PL-0124A-4LR to 6.01 drive for the following platforms:

- PL8840

- PL8840v3

- PL89660

- PL89660v3

- PL9420

- PL9420v3

> **Note**
>
> The Advantech NIC firmware is not field upgradable, contact Sandvine support for return merchandise authorization (RMA). For a list of supported Advantech NMC, refer to the hardware guide of the Sandvine hardware platform at https://docs.support.sandvine.com.

Appendix A. Information for previous releases

A.1. Features introduced in previous releases

A.1.1. New features introduced in Active Network Intelligence 24.40.00

A.1.1.1. Added support for Silicom Quad Port 10GE cards on iQ42300-REV-B platform

AHA Id:	DP-416
FEA Id:	FEA-590
Description:	This release adds support for the following Silicom Quad Port 10GE internal bypass NICs on the iQ42300-B platform: • PE310G4BPI71-SR • PE310G4BPI71-LR This prevents the external bypass from consuming extra rack space. The Silicom Quad Port 10GE card can be set in the following bypass modes: • Protected - The watchdog daemon monitors this NIC and puts it into bypass mode if the engine is unresponsive after the given BYPASS_TIMEOUT configuration value. • Forced bypass - The NIC is in forced bypass mode, which means that the ports are physically connected to each other and no packets are handled by the packet-processing engine. • Disconnect - The NIC has a link down. This helps in an LACP environment, where you do not want the traffic to be load-balanced to this NIC.
Reference:	For more information, see the *iQ42300 Hardware Installation Guide*, section *Traffic channels* option 4.

A.1.1.2. External PLDBD database connection limit increased from 400 to 1000

AHA Id:	DP-398
FEA Id:	FEA-774
Description:	The maximum limit of PLDB connection is increased from 400 to 1000. This mitigates connection exhaustion specifically in environments where a ruleset proxy is used in conjunction with large clusters of PL15000 devices.
Reference:	For more information, see the *ActiveLogic product guide*, section *Recommended use of proxy*.

A.1.1.3. CTI database updates every 15 minutes

AHA Id:	DM-221

FEA Id:	FEA-799
Description:	The frequency of the Cyber Threat Intelligence (CTI) database update is changed from 1 hour to 15 minutes. This enables you to detect new threats as close to real-time as possible.
Reference:	For more information, see the *ActiveLogic Product Guide*, section *Cyber Threat Intelligence*.

A.1.1.4. Introduced iQ42080 hardware platform

AHA Id:	DP-401
FEA Id:	FEA-801
Description:	The iQ42080 hardware platform with a 2U rack-mountable ActiveLogic appliance is introduced for medium- to small-range performance requirements. It is a single-socket system that, depending on the options chosen, supports 1G and 10G interfaces. SFP optics enable the 1G interfaces, and SFP+ optics enable the 10G interfaces. The platform is available with dual, hot-plug, redundant 800 W AC or 1100 W DC power supplies.
Reference:	For more information, see the *iQ42080 Hardware Platform Guide*.

A.1.1.5. TCP Acceleration integration within ANI architecture

AHA Id:	DP-455
FEA Id:	FEA-553 FEA-807 FEA-808
Description:	The integration of TCP acceleration within ActiveLogic improves subscriber experience. With this integration, ActiveLogic acts as a transparent proxy to TCP traffic, which improves TCP throughput and reduces network retransmissions. The TCP acceleration function in ActiveLogic supports the following prominent features: • Enables flow based acceleration, which optimizes TCP or IP for radio or other network-specific conditions, while optimizing internet traffic • Improves the performance of TCP slow-start, TCP congestion-avoidance, TCP Retransmission Time Outs (RTO), and variations in Round Trip Times (RTT) • Enhances TCP Fast Open (TFO) performance • Supports acceleration of MPLS and VLAN tagged flows • Supports loss probing for faster retransmission **Note** This feature supports the acceleration of symmetric TCP connections (where a single ActiveLogic NUMA instance handles both upstream and downstream traffic). **Note** This feature is qualified for use with iQ52600 and virtual ActiveLogic.
Reference:	For more information, see the *ActiveLogic Product Guide*, section *TCP Acceleration*.

A.1.1.6. PERC H355 RAID controller support on the iQ52600 platform

AHA Id:	DP-533
FEA Id:	FEA-898
Description:	The iQ52600 hardware platform now supports the PERC H355 RAID controller.
	Note The PERCCLI tool now supports and manages the H355 RAID controller.
	The `show system raid-status` ConfD CLI uses PERCCLI as a management tool for PERC H355 RAID controller.
	The `system storage configure-hwraid` ConfD CLI does not support PERCCLI as a management tool for PERC H355 RAID Controller. Instead, you can use the iDRAC web interface to configure the RAID Controller.
Reference:	For more information, see the *iQ52600 Hardware Platform Guide*, section *Support RAID Controller*.

A.1.1.7. Enhanced ActiveLogic data pipeline

AHA Id:	NA-414 NA-415
FEA Id:	FEA-891 FEA-945
Description:	To optimize ActiveLogic CPU and memory usage, key analytics functionalities (TrafficObjects and FlowObjects) are available in Packetlogicd (PLD).
	This eliminates the need to enable the Packetlogic Statistics Service if the deployment does not use these functionalities that are not ported to PLD yet:
	• Kafka export from ActiveLogic
	• NatStats and NatConfig data collection for Insights Data Storage
	• Forensics data collection for Insights Data Storage
	To enable the TrafficObjects and/or FlowObjects functionality in PLD, set the ANALYTICS_CONN_PROCESSING_ENABLED system configuration value to True.
	Note • This feature is available for early access. • StatisticsFS data collection will not be ported to PLD.
Reference:	None

A.1.1.8. Intelligence Feeds: Improved database distribution and loading process

FEA Id:	DM-225
FEA Id:	FEA-902

Description:	New SNMP traps (with appropriate severity), alarms, and syslog messages are added for Intelligence Feeds as follows: • SNMP traps added for Intelligence Feeds with appropriate severity. These traps are generated for database download failure, database processing failure, successive database update failure per database, and database license expiry. • SNMP traps added for ContentLogic, GeoLogic, and MS-OTT databases with appropriate severity. For the Intelligence Feeds database, the interval between each database update check is as follows: • Internet Filtering Database (IFD)/ IFD Lite- every 6 Hours • Internet Watch Foundation (IWF)- every 6 Hours • Internet Advertising Database (IAD)- every 12 hours With this feature, Intelligence Feeds raises appropriate SNMP traps and provides clear feedback in syslog for general Intelligence Feeds and database loading process operation.
Reference:	For more information, see the following guides: • *ActiveLogic Product Guide*, section *Intelligence Feeds*. • *ActiveLogic SNMP Guide*, section *Traps from Active Network Intelligence Firmware*.

A.1.1.9. Introduced INTERFACE_TCP_ENABLED system configuration

AHA Id:	DP-537
FEA Id:	FEA-903
Description:	In order to optimize the use of the available physical memory bandwidth, this feature provides an option to streamline the communication between the packet processing shared memory and other system processes. To enable this feature, set the INTERFACE_TCP_ENABLED system configuration setting to False. **Note** Only when ActiveLogic is operating in DPDK mode, you can set the INTERFACE TCP ENABLED system configuration to False.
Reference:	None

A.1.1.10. SSL latency metrics improvement

AHA Id:	DP-545
FEA Id:	FEA-911
Description:	This feature adds support for measuring SSL handshake RTTs and allows you to use it similar to existing TCP RTT metrics.
Reference:	For more information, see the *ActiveLogic Product Guide*, sections *SSL Latency* and *Filtering RTT metrics*.

A.1.1.11. Improved overload protection for ActiveLogic

AHA Id:	DP-508

FEA Id:	FEA-917
Description:	This feature adds support for monitoring the packet queues between the load balancer and flow processor threads. Now, ActiveLogic can take individual actions per flow processor thread. For example, shaping or disabling DRDL classification, shunting new connections when dynamically configurable queue thresholds are crossed. This granular control decreases the chance of triggering platform level actions due to NIC RX drops. **Note** • This feature is not supported on PL15000, as this chassis-based platform uses a separate load balancer blade. • This feature is supported on both PLOS and DPDK engine modes.
Reference:	For more information, see the *ActiveLogic Product Guide*, section *Overload Protection*.

A.1.1.12. Unlicensed data-plane platforms act as license expired and shunt traffic

AHA Id:	DP-540
FEA Id:	FEA-919
Description:	Unlicensed dataplane platforms bring up traffic channel interfaces and shunt traffic. While unlicensed, optics monitoring commands are available to allow the installer to determine the status of the individual traffic channel interfaces. This feature is only applicable on appliances and virtual ActiveLogic.
Reference:	For more information, see the *ActiveLogic Product Guide*, sections *Per-lane optics monitoring* and *Applying System Licenses*.

A.1.1.13. 100G CX5/CX6 hardware-assisted inner 5 tuple flow distribution

AHA Id:	DP-530 DP-556
FEA Id:	FEA-921 FEA-947
Description:	You can now configure physical and virtual platforms using Mellanox CX5/CX6 100G NICs to perform Receive Side Scaling (RSS) hash on the second level (inner) IP header. This offloads the load balancer CPUs from performing this function and ensures that flows are sent directly to the flow processor. This feature is supported for MAPe, DSLite, and GTP-U tunneled traffic.
Reference:	For more information, see the *ActiveLogic Product Guide*, sections *Load balancer (MAP-E/ DSLite tunnel traffic)* and *Load Balancer (GTP-U tunnel traffic)* .

A.1.1.14. ActiveLogic optics monitoring enhancements

AHA Id:	DP-531 DP-543

FEA Id:	FEA-926
	FEA-929
Description:	Previously, optics monitoring was supported only when Broadcom interfaces were assigned to the engine. With this release, iQ52600 hardware configuration option 1 now supports optics monitoring on the Broadcom 25/10G interfaces when assigned to userspace.
	Previously, core services reload was required after installing/removing optical transceivers. With this release, Optics monitoring information is now available after hot plugging optical transceivers.
	To view optics monitoring information, run the following CLI command:
	`request system optics-monitoring channels <channel-id> <int/ext>`
Reference:	For more information, see the *ActiveLogic Product Guide*, section *Monitoring optics diagnostics*.

A.1.1.15. Addition of flow behavior flags to indicate packet drops and delay due to shaping

AHA Id:	DP-527
FEA Id:	FEA-927
Description:	This feature adds new flow behavior flags in ActiveLogic, which can be used to define conditions in the ruleset:
	• Shaping delay incoming- Indicates that at least one incoming packet in the connection is delayed due to shaping.
	• Shaping delay outgoing- Indicates that at least one outgoing packet in the connection is delayed due to shaping.
	• Shaping drop incoming- Indicates that at least one incoming packet in the connection is dropped due to shaping.
	• Shaping drop outgoing- Indicates that at least one outgoing packet in the connection is dropped due to shaping.
	The configuration value SHAPING_FLAG_DELAYED_CONNECTIONS_MS sets the delay, in milliseconds, after which these flags are set.
Reference:	For more information, see the *ActiveLogic Product Guide*, section *FlagObjects*.

A.1.1.16. ActiveLogic supports Red Hat OpenStack 16.2

AHA Id:	DP-545
FEA Id:	FEA-982
Description:	ActiveLogic now supports Red Hat OpenStack Platform 16.2.
Reference:	For more information, see the *OpenStack ANI VNF Release Notes.*

A.1.1.17. New subscription type support for AppLogic

AHA Id:	DM-186
FEA Id:	FEA-998

Description:	This feature adds support for subscription based licensing for AppLogic.
Reference:	For more information, see: • *ActiveLogic Product Guide*, sections *Licenses* and *AppLogic* • AppLogic Reference Guide

A.1.1.18. Configurable volume threshold filter for TrafficObject

AHA Id:	NA-432
FEA Id:	FEA-1005
Description:	You can set a volume threshold filter for each TrafficObject. If you set a volume threshold filter, it filters the records that experience less traffic than the preset threshold within the aggregation interval and does not export them.
Reference:	For more information, see the *Activelogic Product Guide*, section *Configuring TrafficObjects*.

A.2. Enhancements introduced in previous releases

This section identifies the enhancements made in Active Network Intelligence releases.

A.2.1. Enhancements introduced in Active Network Intelligence 24.40.00

A.2.1.1. Tools such as virsh shutdown shuts down the guest VM

Issue:	DIST-4540
Description:	Sandvine firmware images can identify the power button event and sent a command to shut down and power off the guest virtual machine (VM) accordingly. This enables tools such as **virsh shutdown <my-machine>** to operate as intended.

A.2.1.2. Libexpat upgraded to version 2.4.9

Issue:	DIST-6048
Description:	This release upgrades libexpat to version 2.4.9 to address the following security vulnerabilities: • CVE-2022-40674 - libexpat versions earlier than 2.4.9 has a use-after-free in the doContent function in xmlparse.c. • CVE-2022-22822 - addBinding in xmlparse.c in libexpat versions earlier than 2.4.3 has an integer overflow. • CVE-2022-22823 - build_model in xmlparse.c in libexpat versions earlier than 2.4.3 has an integer overflow. • CVE-2022-22824 - defineAttribute in xmlparse.c in libexpat versions earlier than 2.4.3 has an integer overflow.

A.2.1.3. Elements - Addition of logs for load-container-images script

Issue:	DIST-6133
Description:	This enhancement adds a logging mechanism to the load-container-images script. This script: • Removes existing Docker images (if an upgrade is available). • Loads the images into the Docker environment. • Tags the Docker images with an associated tag. This enhancement logs a message in the log/messages.log file when any of these actions occur. These logs help you in troubleshooting in case errors occur while upgrading Elements. Using the filter function of syslog-ng, this enhancement also adds the load-container-images script logs that are logged in the log/messages.log file to the log/packetlogic/docker.log file.

A.2.1.4. Improved support for alternate LiveView credentials in ActiveLogic Client

Issue:	GUI-1099
Description:	The login dialog that appears when you select the **Use different password for LiveView login** checkbox now has a username field in addition to a password field. The new field allows you to change which user to authenticate as.

A.2.1.5. INSIGHTS_DIMENSION_SUBSCRIBER value is not needed

Issue:	PIC-5378
Description:	Now you do not have to provide a dummy value in INSIGHTS_DIMENSION_SUBSCRIBER if you enable INSIGHTS_DIMENSIONS_USE_IP_FOR_SUBSCRIBER to populate the subscriber column in score tables in Insights Data Storage using IP address.

A.2.1.6. Added support for pushing TrafficObject data to schemas other than traffic

Issue:	PIC-6150
Description:	With this release, you can specify either traffic or custom Insights Data Storage database schema in TrafficObjects to push TrafficObject data to more database schemas than traffic. To specify a schema, add it as a prefix to the table name when creating a TrafficObject through the ActiveLogic Client or PythonAPI. To specify a schema, add the schema as a prefix to the table name when creating a TrafficObject through the ActiveLogic Client or PythonAPI. For example- custom.table.

A.2.1.7. System diagnostics value to track PLS_SCHEMA_COLUMN_SUBSCRIBER

Issue:	PIC-7012

Description:	A system diagnostics value **Subscriber Column Found in Schema** tracks whether the PLS_SCHEMA_COLUMN_SUBSCRIBER system configuration matches any column in a provided session context schema. This helps in troubleshooting issues related to the CONNECTION_UPDATE_BALANCE_TYPE system configuration value.

A.2.1.8. New system diagnostics liveview values to improve logs monitoring

Issue:	PIC-7092
Description:	When session context mapping for a connection or host stats entry fails, LiveView Daemon records them. When such a failure happens, it might lead to massive spamming of the logs.
	To improve monitoring of this issue, this enhancement introduces the following system diagnostics values for each failure recorded:
	• PL_SYSDIAG_LIVEVIEW_HOST_STATS_MISSING_ROWS • PL_SYSDIAG_LIVEVIEW_CONN_UPDATE_MISSING_ROWS
	The logs for these values are set to the Verbose level.

A.2.1.9. Changing insights-remote does not restart PLD

Issue:	PIC-7011
Description:	When you use `set service statistics insights-remote` to set up a new Insights Data Storage remote host and set the ANALYTICS_SCORE_ENABLED configuration to:
	• True, then both PacketLogic Daemon (PLD) and PacketLogic Statistics Daemon (PLSD) restarts. • False, then only PLSD restarts.

A.2.1.10. New system diagnostics zone is introduced to have necessary operational health metrics

Issue:	PIC-7111
Description:	A new **Analytics Pre-Processing** system diagnostics zone is introduced under the analytics area. This zone has the necessary operational health metrics corresponding to the Analytics Pre-Processing Daemon process.

A.2.1.11. AppLogic-related data in TrafficObjects, Score data export, and FlowObjects

Issue:	PIC-7443
Description:	New dimensions and fields (such as App Name, App Category, and App Content) are added to TrafficObjects, Score data export, and FlowObjects. These dimensions and fields are populated from ServiceObjects. This enhancement provides support when running the new AppLogic traffic classification.

A.2.1.12. PLSD spills only the datasets that do not fit in the queue to the disk

Issue:	PIC-7538
Description:	Previously, when the queue was unable to fit all the datasets, the PLSD spilled all datasets that it tried to send to Insights Data Storage to the disk.
	With this release, the PLSD spills only the datasets that do not fit in the queue to the disk.

A.2.1.13. Line feed behavior in flow record CSVs

Issue:	PIC-7816
Description:	Now CSV files produced from FlowObjects using dump-to-disk functionality include a trailing line feed at the end of the files. This makes it easier to concatenate files to extract and process them.

A.2.1.14. Introduced a new TrafficObject metrics

Issue:	PIC-7912
Description:	The ActiveLogic Client introduces new TrafficObject metrics **Shaping IBCM Packet Drops In** and **Shaping IBCM Packet Drops Out**. For shaping objects specified by the newly added configuration value INSIGHTS SHAPING OBJECTS USE CASE IBCM, these metrics act as packet-drop counters.

A.2.1.15. Improved the performance of TrafficObject

Issue:	PIC-7869
Description:	The performance of TrafficObject is improved as follows: • Avoids lock contention on larger systems with many threads • Uses less memory when not all dimensions are in use (which is most of the time) • Avoids handling connection updates for connections that do not have statistics rules. This improves the performance of systems that has rules, which do not hit every connection

A.2.1.16. SHAPING_OR_BORROWING default setting changed from False to True

Issue:	PRE-4045
Description:	In ActiveLogic, the system configuration SHAPING_OR_BORROWING is enabled (set to True) by default because it is necessary for configuration related to fairness to function properly.

A.2.1.17. Increased maximum limit of PLD_CONN_UPDATE_THREADS

Issue:	PRE-16425

Description:	For the following platforms, the maximum limit of the PLD_CONN_UPDATE_THREADS system configuration value is increased: • iQ42300 increased to 12 • iQ52600 increased to 16 • PLVM-KVM-LARGE increased to 12 • PLVM-VSPHERE-LARGE increased to 12

A.2.1.18. Distribution of re-evaluation operations

Issue:	PRE-21383
Description:	ActiveLogic distributes the re-evaluation operations for ContentLogic, GeoLogic, and Border Gateway Protocol (BGP) over a configurable number of connection update intervals to reduce the CPU load.

A.2.1.19. New system configuration value to configure blind forwarding

Issue:	PRE-22120
Description:	System configuration has a new value called OLPROT_BLIND_FORWARDING to configure the blind forwarding. Overload protection acts in three states: 1. DRDL Enabled 2. DRDL Disabled 3. Blind forwarding(Shunt) Enabling the blind forwarding mode creates more harm than dropping packets. Therefore, it recommended to set OLPROT_BLIND_FORWARDING value to False when using CGNAT use case.

A.2.1.20. Added processes PLD, PLSD and PLDBD in socket monitoring

Issue:	PRE-22227
Description:	Now you can view the latency value for PLD, PLSD and PacketLogic Database Daemon (PLDBD). These demons are added in **System Diagnostic >Zones>Data Plane>Socket monitoring**.

A.2.1.21. Improved overall packet processing performance

Issue:	PRE-22512
Description:	The efficiency of handling DRDL states during packet processing is improved. In ActiveLogic, this improves the overall packet processing performance.

A.2.1.22. ActiveLogic Client allows A and AAAA record for DNS generic action

Issue:	PRE-22556
Description:	In ActiveLogic Client, separate fields are added for A and AAAA records for DNS generic action in inject filtering rule to ease the configuration process.

A.2.1.23. QUIC_HANDSHAKE_RTT_INTERNAL/EXTERNAL_MAX does not allow min-filtering

Issue:	PRE-22676
Description:	Two new system configuration parameters are added to filter out the QUIC RTT values lesser than the newly added configurable minimum thresholds, while publishing statistics records. The following are the new parameters and the new minimum thresholds: • QUIC_HANDSHAKE_RTT_INTERNAL_MIN • QUIC_HANDSHAKE_RTT_EXTERNAL_MIN

A.2.1.24. Alarm when web LiveView client disconnected from ActiveLogic

Issue:	PRE-22682
Description:	If the connection between a web LiveView client and PLHTTPD client is lost due to exceed in limit to send buffers to the client, a notification window appears and SNMP notification will notify you about it. To reconnect web liveview, increase the PLD_CLIENT_SEND_RINGBUF_WEB_MB system configuration value.

A.2.1.25. Introduced new system diagnostic alarms and system diagnostic counter

Issue:	PRE-22762
Description:	In ActiveLogic, the following new system diagnostic alarms and system diagnostic counter are introduced: • PL_SYSDIAG_CONNECTION_CONNPROT_STATUS system diagnostic alarms track the connection protection in active/passive state. • PL_SYSDIAG_CONNECTION_UNESTABLISHED_COUNT system diagnostic counter displays a current unestablished connection count.

A.2.1.26. Renamed system configuration values related to balancer

Issue:	PRE-22803

Description:	The following system configuration values are not specific to PLOS engine mode. They can also be used in DPDK engine mode. Therefore, the following system configuration values are renamed: • PLOS_BALANCER_ALLOW_CPU0 is renamed to BALANCER_ALLOW_CPU0 • PLOS_BALANCER_ALLOW_LB_ON_FP is renamed to BALANCER_ALLOW_LB_ON_FP • PLOS_BALANCER_ENTRY_FACTOR is renamed to BALANCER_ENTRY_FACTOR • PLOS_BALANCER_LB_CPUS is renamed to BALANCER_LB_CPUS • PLOS_BALANCER_LOCAL_NODE is renamed to BALANCER_LOCAL_NODE • PLOS_BALANCER_QUEUE_LENGTH is renamed to BALANCER_QUEUE_LENGTH • PLOS_BALANCER_USE_5TUPLE is renamed to BALANCER_USE_5TUPLE

A.2.1.27. MAC address display in ConfD CLI

Issue:	PRE-22875
Description:	When you run the `show data-plane channels` CLI command in ConfD CLI, you can view the MAC addresses of internal and external channel interfaces.

A.2.1.28. Seamless channel role switch

Issue:	PRE-23158
Description:	With this release, interface links do not go down when you change the channel role in ActiveLogic between **Traffic** and **Shunt**. This avoids TX drops and link flaps when switching channel roles.

A.2.1.29. Introduced a new QueueSync system diagnostics value called (ext update) Update packets loss percentage

Issue:	PRE-23378
Description:	This enhancement adds new QueueSync system diagnostics counter **(ext update) Update packets loss percentage** and removes alert levels for the existing system diagnostics (ext update) Update packets lost and (ext status) Status packets lost. This avoids unnecessary alarms for QueueSync update packets when the packet loss is trivial and does not affect the shaping behavior. The **(ext update) Update packets loss percentage** value records the percentage loss of QueueSync update packets that are lost in the last 1-minute interval. It raises an alert when the loss percentage is more than the threshold value.

A.2.1.30. Moved IP protocol 58 (IPv6-ICMP) from IPv6 to control traffic

Issue:	PRE-23846
Description:	In ActiveLogic Client, the **IP protocol 58 (IPv6-ICMP)** option is moved from **Categories>IP Protocols>IPv6** to **Categories>IP Protocols>Control traffic**.

A.2.1.31. Default maximum ARM size not updated after upgrade

Issue:	PRE-23846
Description:	The default maximum size of the DRDL Application Recognition Module (ARM) file does not get updated after upgrading ActiveLogic. This fix provides a log message if the size of the ARM file is large and notifies you to increase the size of the DRDL_MAX_ARM_SIZE system configuration value to mitigate the issue.

A.2.1.32. Enabling RSS on PF devices

Issue:	PRE-24034
Description:	A new configuration value DPDK_I40E_USE_RSS is introduced in this release. With this configuration value, you can enable RSS on physical function (PF) devices using the i40e driver.

A.2.1.33. Added DRDL_MAX_ARM_SIZE system configuration value

Issue:	PRE-24057
Description:	This enhancement adds a system configuration value DRDL_MAX_ARM_SIZE, which configures the allocated size for the signature bundle in engine memory. The size is pre-allocated.

A.2.1.34. Set channel bypass mode using ActiveLogic Client

Issue:	PRE-24567
Description:	The ActiveLogic Client > Channel editor now contains a column to set the bypass mode of channels with built-in bypass controllers. The supported bypass modes are protected, disconnected, or forced-bypass. This setting is only available when using Silicom X710 NICs and when the engine mode is DPDK.

A.2.2. Enhancements introduced in Active Network Intelligence 24.40.01

This section describes the enhancements made in this release.

A.2.2.1. Allocation of more shared memory buffers

Issue:	PRE-25091
Description:	The shared memory buffers are increased for CPUs that need to communicate shaping information to system daemons from the engine.

A.3. Resolved issues in previous releases

This section identifies issues resolved in previous Active Network Intelligence releases.

A.3.1. Resolved issues in Active Network Intelligence 24.40.00

The following issues are resolved in this release:

Description	Identified in	Issue
Title: GPG allows overwriting of existing files **Description:** After a failed GNU privacy guard (GPG) installation, reinstalling GPG prompts you to overwrite existing files. If you accept this overwrite prompt, this might lead to unexpected system behavior. This fix cleans up the unsuccessful installation files so that the new installation is successful.	ActiveLogic 22.40.04	DIST-5149
Title: ActiveLogic Client audit logs not clear **Description:** ActiveLogic Client audit logs do not include information regarding the type of command. This causes confusion as the audit logs lack clarity. With this fix, the cmd field of TACACS+ audit message, which previously showed none, now displays the correct cmd command.	ActiveLogic 24.03.00	DIST-5977
Title: Missing the machine ID after the system start **Description:** When the system starts, services also start as part of the system start process. If the services using machine ID (such as confd_oper_notifications) start before the services that populate the machine ID (such as confd_value_mapper), the services using machine ID do not receive the machine ID value. With this fix, the system dynamically reads the value from the persistent file system instead of the cached value.	ActiveLogic 24.20.00	DIST-6242
Title: Log rotation stops working **Description:** Log rotation stops working when you install Professional Services Framework (PSF), such as a legacy license manager. The following error message appears: `error root: newsyslog failed to rotate log` This unnecessarily consumes the system's storage and increases the possibility of the system running out of storage.	ActiveLogic 23.40.05	DIST-6295
Title: Console password changes **Description:** When you configure the console password and then if you run the load replace or load override command, the console password changes. This results in a console sign in failure. With this fix, the password is an encrypted string instead of masking.	ActiveLogic 24.24.00	DIST-6324
Title: Intelligence Feeds service status appears incorrect **Description:** When you run the **set service intelligence-feeds disabled** CLI command to disable the intelligence-feeds service, the service is disabled. However, when you run the **show system services** CLI command to view the status, the status does not show that it is disabled.	ActiveLogic 24.25.00	IF-3383
Title: URL purge issue in ContentLogic custom database **Description:** When subnet data has the same group category as the URL and the subnet data with common categories are loaded, the ContentLogic custom database URL data is not purged from memory. This causes unwanted ContentLogic categorization of URLs. With this fix, the subnet data loading does not affect the addition or deletion of URL data from memory.	ActiveLogic 23.40.00	IF-3393

Description	Identified in	Issue
Title: Unexpected Packetlogicd thread error when disabling GeoLogic **Description:** When the GEOLOGIC_ENABLED configuration is set to false, Packetlogicd encounters an unexpected GeoLogic error when restarted. With this fix, ActiveLogic handles the GeoLogic-disabled state restart gracefully.	ActiveLogic 22.40.00	IF-3416
Title: Changing the network interface configuration deletes virtual IP of that interface **Description:** Changing the network interface configuration deletes the virtual IP address of that network interface and does not reconfigure the virtual IP address. As a result, high-availability configurations using virtual IP addresses do not work. With this fix, changing the network interface configuration does not affect the virtual IP of the network interface.	ActiveLogic 22.40.11	KOI-66
Title: Unable to write the dataset to disk more than once **Description:** If a file name generated for the dataset exceeds the 255 characters limit, then the system is unable to write the dataset to disk more than once.	ActiveLogic 23.20.00	PIC-7491
Title: Score statistics accounts traffic under the wrong service **Description:** Score statistics accounts traffic under the base service instead of the final service if the INSIGHTS_DATA_COLLECTION_SCORE_DEVICE_NAME system configuration is enabled. This issue primarily affects the virtual services.	ActiveLogic 24.20.00	PIC-7543
Title: Incorrect inter-packet arrival time and jitter **Description:** The ActiveLogic Client > LiveView displays the inter-packet arrival time mean and jitter data as 0 instead of 'no data' if there is no data to calculate them.	ActiveLogic 24.20.00	PIC-7679
Title: Unexpected PLSD shutdown when using BGP dimensions **Description:** PLSD runs out of memory if BGP dimensions are used for traffic objects. This causes PLSD to shut down unexpectedly after an undefined time. This fix resolves the BGP path references in traffic objects.	ActiveLogic 23.40.04	PIC-7689
Title: Unexpected Statistics demon shutdown **Description:** When you enable only the export of NAT stats on KAFKA, the statistics demon shuts down unexpectedly.	ActiveLogic 23.20.00	PIC-7710
Title: iQ42300- Unexpected PLSD restart in the string cache **Description:** When you enable the host stats, PLSD restarts unexpectedly in the string cache.	ActiveLogic 24.20.01	PIC-7789
Title: Unexpected PLSD restart **Description:** PLSD restarts unexpectedly due to an empty pool name in NAT statistics. This fix adds the logic to handle null string cache pointers in NAT statistics and NAT configuration statistics.	ActiveLogic 23.20.08	PIC-7814
Title: Incorrect ShapingObject statistics when traffic is not present **Description:** When there is no traffic for a specific ShapingObject, the ShapingObject statistics include incorrect values. With this fix, ShapingObject statistics considers no traffic as valid data.	ActiveLogic 24.20.01	PIC-7860

Description	Identified in	Issue
Title: TrafficObject leak **Description:** After removing all TrafficObjects and committing the ruleset, the memory does not get clear properly. This sometimes leads TrafficObjects to leak while doing some combination of deleting and creating TrafficObjects in the ruleset.	ActiveLogic 24.24.00	PIC-7874
Title: Exporting HostStats data to Insights Data Storage generates a Vertica error **Description:** If AppLogic-related columns do not exist in Insights Data Storage, exporting host stats data to Insights Data Storage generates a vertica error. With this fix, a check is introduced to only export AppLogic dimensions to the score tables if AppLogic related columns exist.	ActiveLogic 24.25.00	PIC-7941
Title: PLD shuts down unexpectedly **Description:** After the PLD restart, if PLD receives information from an engine with a shaping rule before receiving information from PacketLogic Ruleset Compiler Daemon (PLRCD), PLD shuts down unexpectedly.	ActiveLogic 24.25.00	PIC-8008
Title: Python3 API - Unable to use host stats LiveView data **Description:** An issue in Python3 API prevents the use of host stats LiveView example code.	ActiveLogic 24.20.01	PIC-8024
Title: GROUP_ID system configuration value is incorrectly set in PLSD **Description:** PLSD receives the TrafficObject group ID dimension's value from PLD. If the group ID is set in PLSD before it receives the shared configuration values from PLD, the GROUP_ID system configuration value is incorrectly set in PLSD	ActiveLogic 24.22.00	PIC-8040
Title: Incorrect increment in system diagnostics value **Description:** On ActiveLogic, the received NATsync or IPrewrite sync packets incorrectly increase the **TX packets not allowed** system diagnostics value.	PacketLogic 15.1.6	PRE-23318
Title: ActiveLogic incorrectly reports more status packets **Description:** ActiveLogic system diagnostics reports more status packets than the number of QueueSync peers. This occurs because the system diagnostics also reports duplicate status packets. There is no functionality impact. This fix adds the logic to handle duplicate status packets so that the system diagnostics correctly reports them.	ActiveLogic 23.20.05	PRE-23618
Title: PLSD restarts if PLS_STATISTICS_ENABLED is enabled on ActiveLogic CNF **Description:** On ActiveLogic Cloud Native Functionality (CNF), StatsFS statistics collection is not supported. Therefore, if you enable StatsFS on ActiveLogic CNF, then the PLSD process restarts unexpectedly after the PLS_DUMP_INTERVAL ends. This fix disables the StatsFS statistics-collection system configuration PLS_STATISTICS_ENABLED on ActiveLogic CNF by default and hides the system configuration.	ActiveLogic 24.20.00	PRE-23994

Description	Identified in	Issue
Title: Default maximum ARM size not updated after upgrade **Description:** The default maximum size of the DRDL Application Recognition Module (ARM) file does not get updated after upgrading ActiveLogic. This fix provides a log message if the size of the ARM file is large and notifies you to increase the size of the DRDL_MAX_ARM_SIZE system configuration value to mitigate the issue.	ActiveLogic 22.40.00	PRE-24027
Title: Frequent reset of displayed channel statistics **Description:** In ActiveLogic Client, the channel statistics toggle between zeros and actual values. There are no packet drops due to this issue and the actual counters are not affected. However, the channel statistics values in ActiveLogic Client > LiveView are reset and revert to normal periodically.	ActiveLogic 24.25.00	PRE-24175
Title: Engine restarts repeatedly **Description:** When the engine restarts, Network Time Protocol (NTP) (configured on an AUX interface) fails to publish the time zone to the system, and due to this engine is unable to receive PCI entries. This occurs because of the difference between the current and last updated timestamps. This causes a repeated restart of the engine until it receives the PCI entries.	ActiveLogic 23.40.05	PRE-24186
Title: Increased default value of PACKET_POOL_SIZE on platform iQ31020 **Description:** With DPDK as engine mode on platform iQ31020, you need to have a larger PACKET_POOL_SIZE. If not increasing this system-configuration-value, engine would not start. Therefore increasing the default value of PACKET_POOL_SIZE from 300000 to 550000.	ActiveLogic 24.20.00	PRE-24279
Title: System memory consumption increase in PL15000 **Description:** The PL15000 internal process uses the Python 3 API. This process is consuming a lot of system memory due to the memory leak in the Python 3 API. This leads to an out-of-memory situation. This fix resolves a leak in the Python 3 API.	ActiveLogic 24.22.00	PRE-24355
Title: NIC RX drops not accounted for on all NICs **Description:** When the data-plane channel-layout is set to single-port-per-nic and Mellanox CX-6 NICs are in use, RX drops due to limited shared resources on the NIC are not accounted for on all channel ports. The drops are not accounted for in either the **Packet Processing** or the **Channel Statistics** system diagnostic zones. With this fix, the NIC RX drops are now accounted for on all NICs, irrespective of channel layout.	ActiveLogic 24.24.00	PRE-24390

Description	Identified in	Issue
Title: Changed OPTICS_MONITORING_UPDATE_INTERVAL system configuration default value to zero **Description:** Previously, the default value of the OPTICS_MONITORING_UPDATE_INTERVAL system configuration was 300 seconds and the minimum value was 1 second. Now, the default of the OPTICS_MONITORING_UPDATE_INTERVAL is set to 0. This fix removes the OPTICS_MONITORING_ENABLED system configuration, as it is redundant because of the OPTICS_MONITORING_UPDATE_INTERVAL system configuration updated values. To enable optics monitoring, use OPTICS_MONITORING_UPDATE_INTERVAL and set it to the recommended value, which is 300 seconds or greater. To disable the optics monitoring, set OPTICS_MONITORING_UPDATE_INTERVAL to 0, which is the default value. **Note** You can get the optics monitoring values using the confd-cli `request system optics-monitoring` command even when OPTICS_MONITORING_UPDATE_INTERVAL is set to 0.	ActiveLogic 24.24.00	PRE-24397
Title: Thread value on DRDL appears in negative **Description:** On ActiveLogic Client>System Diagnostic>Zone>Data Plane>Drdl> **Number of slice state structures used** for some threads the values appear in negative, which is working as expected but leads to confusion. This fix displays only the aggregated value and the thread level value to avoid confusion.	ActiveLogic 23.25.08	PRE-24559
Title: MPLS Ethernet packet processed as IPv4/IPv6 packet **Description:** ActiveLogic incorrectly processes MPLS Ethernet packets as IPv4/IPv6 packets, which leads to unexpected behavior. This fix provides a new system configuration value TUNNELING_GRE_MPLS_GUESS_PREFER_ETH that lets you decide how ActiveLogic processes the next packet header after MPLS when it is not possible to identify the type of header.	ActiveLogic 23.40.06	PRE-24709
Title: Auxiliary interface down after iQ52600 reboots **Description:** The auxiliary interface bonding group-2 (port 5/1 and 9/1) goes down after iQ52600 reboots. With this fix, if any physical interface moves to the Userspace mode during restart, all bonds (interfaces) that are created on this physical interface are recreated.	ActiveLogic 24.20.01	PRE-24817

A.3.2. Resolved issues in Active Network Intelligence 24.40.01

The following issues are resolved in this release:

Description	Identified in	Issue
Title: **LiveView > ContentLogic** displays incorrect sum for Unknown **Description**: In LiveView, the **Total** in the **Unknown** ContentLogic item does not match the sum of the individual items. With this fix, if the connections category information is null or if its size is zero in the ContentLogic dynamic LiveView category filter, then LiveView does not account for such connections.	ActiveLogic 24.20.02	PRE-24508
Title: PL15000 - System diagnostics display negative values **Description**: In PL15000 platforms, ActiveLogic Client incorrectly displays negative values for the rate and minimum fields in **System Diagnostics > Zones > Load Balancer**. This fix ensures that ActiveLogic Client does not display negative system diagnostics values for the rate and minimum fields.	ActiveLogic 22.40.11	PRE-24599
Title: UDP 4791 port traffic dropped **Description**: 100G interfaces in DPDK engine mode drop packets destined for UDP port 4791. With this fix, the interfaces successfully forward the packets.	ActiveLogic 24.20.01	PRE-25031
Title: Thread0 buffer in iQ52600 gets exhausted **Description**: In iQ52600 platforms, the thread0 buffers are sometimes exhausted when they are heavily loaded. With this fix, the maximum value of the INTERFACE_SHM_SIZE system configuration is updated to 4095MB to improve the performance of the thread0 buffer.	ActiveLogic 23.20.11	PRE-25101
Title: Unexpected PLSCD restart when processing pending barrier messages **Description**: An unexpected PLSCD restart occurs in a deployment where multiple Maestro Policy Engines connect to ActiveLogic and there are multiple partitions. The issue happens because ActiveLogic attempts to send a barrier ack message to an older barrier message from a Maestro Policy Engine. However, by this time, the Maestro Policy Engine leaves the partition and rejoins it. With this fix, ActiveLogic handles pending barrier messages gracefully.	ActiveLogic 22.40.09	PRE-25109
Title: FlowObjects sent to PLSD even if APD is enabled **Description**: When both APD and PLSD are enabled, FlowObjects data is incorrectly sent to PLSD in addition to being processed in APD. This causes duplicate record creation. With this fix, FlowObjects data is only processed in APD when APD is enabled.	ActiveLogic 24.40.00	PRE-25183
Title: LSP stops working if external interface goes down with bypass NICs **Description**: Using link state propagation (LSP) with bypass NICs causes the channel to enter bypass mode if the external interface link goes down. With this fix, the bypass remains active regardless of the link state.	ActiveLogic 24.40.00	PRE-25309

SANDVINE

The App QoE Company

USA
5800 Granite Parkway
Suite 170
Plano, TX 75024
USA

EUROPE
Svärdfiskgatan 4
432 40 Varberg,
Halland
Sweden
T. +46 340.48 38 00

CANADA
410 Albert Street,
Suite 201, Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

ASIA
RMZ Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333

SANDVINE.COM