AMELIA

AI Ops

AMELIA's Autonomic IT Management Platform

Release Notes 3.5.0
(Document Version 1.0)

AMELIA

Table of Contents

Document History

Author	Version	Date	Comments	Final Approval?
AMELIA Research & Development	1.0	October 14, 2024	Added tickets for 3.5.0 release	Yes

1. Release 3.5.0

This section briefly lists changes to AI Ops for this release.

1.1 RELEASE HIGHLIGHTS

1.1.1 Rollback to a previous version

Database schema is not compatible with previous releases. Once updated, it is not possible to rollback to the previous version without restoring from the backup.

This release brings percona 8.0.37 and percona 8.0.25 won't start with data from 8.0.37:

```
2024-09-05T13:10:29.209115Z 1 [ERROR] [MY-013171] [InnoDB] Cannot boot
server version 80025 on data directory built by version 80037. Downgrade is
not supported mysqld: Can't open file: 'mysql.ibd' (errno: 0 - )
```

1.1.2 ALite Garbage Collection Config Updated

- G1 garbage collector will be used by default
- Enables periodic garbage collection
- Multiple threads will be used for garbage collection irrespective of CPU core count
- Increased reserve to handle sudden spikes
- Config is part of JAVA_OPTS environment variable. If its overridden for ALite, please append the environment variable with following config:

  ```
  -XX:+UseG1GC -XX:-G1UseAdaptiveIHOP -XX:G1ReservePercent=20 -
  Xlog:gc*=info -XX:G1PeriodicGCInterval=30000 -
  XX:+G1PeriodicGCInvokesConcurrent -XX:ParallelGCThreads=8 -
  XX:ConcGCThreads=4
  ```

1.1.3 White List is Renamed to Allow List in API

API /automata/whitelisted-command is renamed to /automata/allowed-command. Please refer to Swagger UI for the details.

1.1.4 Optional Validation of Workflow Cascade Fields

A new setting is added to client settings: Validate cascade values. When enabled, only valid cascade values are allowed. When disabled, any values are accepted. By default, the setting is disabled.

1.2 BUGS

- [AP-26751] - The navigation behavior in the edit mode of the Automation feature within the IPautomata component was adjusted to take users directly to the failure point, rather than the initial or highest level of the application. This change enhances troubleshooting efficiency by streamlining navigation for developers and system administrators managing automations, reducing the time and effort previously spent navigating from a generic, high-level starting point. The update is customer-facing and designed to improve the user experience for those who debug automations within the application.
- [AP-28574] - A visual error message now appears in the UI when users with 'Read-only' permissions attempt to edit folders or their elements, replacing the previous backend-only error. This customer-facing change improves usability by providing immediate feedback, reducing confusion for users interacting with the IPlocksmith interface.
- [AP-28620] - A user-friendly error message now appears when a configuration name exceeds the character limit, replacing the generic internal server error. This change, in the Content Packs configuration section, improves usability by providing clearer feedback to users.
- [AP-28744] - The option for users to manually create anomaly detectors in the OpenSearch Dashboards UI was removed to comply with the updated policy, limiting detectors to the "metrics" index. This customer-facing change affects users managing anomaly detectors in the GUI.
- [AP-28779] - The issue of IPradar tickets lacking associated workflows has been resolved by ensuring workflows are properly defined and initiated for each ticket. This backend change improves ticket processing reliability, addressing errors caused by missing workflows, indirectly benefiting customer-facing operations.
- [AP-29199] - The issue causing linked child tasks in the IPradar system to be marked as resolved again one month after their initial resolution has been fixed, ensuring tasks remain in their resolved state. This backend fix prevents confusion in task management, indirectly benefiting users tracking task statuses.
- [AP-29340] - The event listing was updated to exclude duplicate events from the total count, ensuring that only unique events are reflected in the event tab's count within the EventFlow component. This backend change enhances data accuracy for users relying on event listings, indirectly benefiting customers.
- [AP-29632] - The Locksmith folder API now returns a "Forbidden" status instead of "OK" when accessing restricted resources. This backend update enhances security by accurately communicating access restrictions, affecting system integrators and developers who use the API, but it does not directly impact end-users or the GUI.
- [AP-29698] - Garbage collection in IPautomataLite was optimized to efficiently free memory after running multiple automations, addressing rising memory usage. This backend improvement resolves performance issues related to memory release, enhancing system performance and indirectly benefiting end-users and administrators running automation tasks.
- [AP-29703] - The issue with eligibility verification for ALite instances during execution has been fixed by correctly invoking the method `StandaloneIPautomataExecutionCache#isRunning` to ensure consistent eligibility checks. The method's invocation was also moved to TaskExecutorV2 using its own thread pool to prevent potential deadlocks. This backend change, resulting from a prior refactoring of TaskExecutor, enhances system stability and performance without affecting the user

interface. While not customer-facing, it improves the execution and scheduling of tasks on ALite instances.

- [AP-29709] - The loading time for the task summary in the IPradar support environment was optimized, reducing instances of delays over 10 seconds. This backend improvement enhances performance, ensuring quicker task summary loads, indirectly benefiting users interacting with the support interface.
- [AP-29711] - A version control mechanism was implemented to store document versions and trigger reimports only when modifications occur, improving efficiency by avoiding unnecessary reimports. This backend-facing change optimizes document integration with external systems, reducing processing time and resource usage without affecting the GUI.
- [AP-29758] - The error message display in the Integration module has been updated to allow up to 10 lines before collapsing, improving clarity by preventing important information from being trimmed. This change enhances the experience for developers and integrators by providing clearer error information, impacting backend processes.
- [AP-29791] - Tasks in AIOps are now properly attached to and displayed in the corresponding ServiceNow tickets, ensuring visibility of configuration items (CIs) added via AIOps. This change improves the accuracy and consistency of information between the two systems, enhancing the backend integration process while also benefiting end-users by providing accurate CI information on their ServiceNow tickets.
- [AP-29801] - The issue of overlapping time entries in the task summary on the Amelia Support Platform has been fixed to ensure accurate time representation. This change, made in the task summary section accessed through the "Overview" page, improves clarity and record-keeping for users. It primarily impacts customer-facing aspects of the UI, benefiting users who view task summaries.
- [AP-29808] - An issue preventing the Events tab from opening when the hostname contained unusual symbols has been fixed. This change affects the Events tab in the AIOps section, specifically on task events pages. The fix ensures users can access the Events tab without errors, regardless of hostname characters, and directly impacts users accessing the AIOps GUI.
- [AP-29822] - The extra empty lines in ServiceNow Work Notes and additional comments have been removed to enhance readability and formatting consistency. This change addresses a formatting issue in the ServiceNow integration and improves user experience for those interacting with ServiceNow through integrated applications, affecting the customer-facing interface.
- [AP-29829] - The system now sends only links to task attachments when the "Send task attachments data" option is enabled, rather than including full attachment data. This change affects email communication functionality, enhancing performance and security by reducing email size and minimizing risks associated with sending full attachments. While primarily impacting backend processes, it indirectly benefits end-users who receive emails with attachment links.
- [AP-29835] - The issue exposing secured variable values in validation error messages has been resolved, ensuring that these values no longer appear in error messages. This change affects the validation error messages in the Automations module, specifically within the Orchestrator and IPautomata interfaces. The purpose is to enhance security by preventing the exposure of sensitive information. While it primarily impacts backend systems, it secures sensitive data across customer-facing interfaces.
- [AP-29852] - The ticket addresses "Read timed out" exceptions in the MultiTenantAutoDeploymentStrategy by adjusting the timeout settings for the ipticket-service, setting the connect-timeout and read-timeout to 60 seconds. This change does not affect the user interface but

involves backend configuration to improve API request handling. The purpose is to enhance system robustness during client loading, reducing unnecessary retries if a batch fails and allowing for more efficient handling of requests. While it primarily impacts backend services, specifically the IPworkflow component, it improves stability and efficiency without directly affecting end-users.

- [AP-29864] - The full-screen script editor was updated to optimize screen space, enhancing the user experience to be more efficient, like other applications as Amelia. These changes are visible in the script editor interface during full-screen mode. The purpose is to improve usability and functionality, boosting user productivity and satisfaction. This change is customer-facing, impacting end-users who use the full-screen script editor within the application.
- [AP-29877] - The application was updated to fix communication with the OpenAI API. There are no changes to the GUI, as the update addresses issues stemming from the API's updates. This change affects backend functionality and resolves issues without impacting existing features for users.
- [AP-29878] - The session in AIOps will now remain active even if the Amelia Admin web interface is idle in another tab, preventing inappropriate session timeouts. This change impacts session management in multi-tab scenarios for AIOps and Amelia Admin. It addresses an issue where active AIOps users were incorrectly timed out and redirected to the login screen. This customer-facing change benefits users working with both interfaces in multiple tabs.
- [AP-29887] - The URL used by the Diff button on the Automata Page has been corrected to fetch the proper version data, resolving the issue of incorrectly calling an invalid URL. This change impacts the Automata Page, specifically the Diff button's functionality. The fix ensures that users can access the correct automation version details without errors. This customer-facing change affects all users interacting with the Diff functionality on the Automata Page.
- [AP-29922] - The alignment issue between the Type and Name fields in the right panel of the 'Allowed Command' entry type has been fixed, ensuring that values are displayed correctly without colliding. This change occurred in the right panel of the IPaudit component when users click on the 'Allowed Command' entry type. The fix enhances usability and improves the overall readability and professionalism of the UI. This customer-facing change impacts users interacting with the application's UI, particularly within the IPaudit section.
- [AP-29930] - Access to update matchers in the Automata component was restored after the upgrade to version 3.4.0, resolving authority requirement issues and allowing users to perform updates as before. This change impacted permissions management within the Automata section of the UI. The purpose was to resolve a loss of access caused by the upgrade, ensuring users could update matchers without new restrictions. This customer-facing change specifically affected users at Wells Fargo who interact with the Automata component.
- [AP-29945] - The issue with Cascades values not being accepted from integration updates after upgrading to version 2.20.4 has been resolved, preventing workflow suspensions. There were no direct changes in the UI, as this was a backend integration issue. The change was necessary to ensure integration updates are correctly accepted, maintaining smooth operations. While this change primarily affected backend systems, it indirectly impacted customers by ensuring reliability and continuity in operations.
- [AP-29951] - The issue of duplicate statements in the rating acknowledgment message for specific survey responses has been resolved. This change occurred in the survey acknowledgment message UI, particularly when displaying messages for certain survey ratings. The purpose was to enhance user

experience by eliminating redundant and confusing duplicate statements. This change is customer-facing, affecting end-users interacting with the survey acknowledgment messages.

- [AP-29964] - The "Time to Respond" metric calculation has been corrected to reflect the time between a ticket's initial creation and the first status change, rather than recalculating with subsequent changes. This change affects backend data processing and reporting in OpenSearch, with no direct UI changes for end-users. It resolves a logic error that caused inaccurate response times in reports when a ticket's status changed from NEW. Primarily impacting backend systems, this adjustment enhances reporting accuracy for internal teams like customer support analysts, while customer-facing aspects remain unaffected unless previous reporting errors were communicated.
- [AP-29965] - The confluence integration now features an "Automatic Sync" toggle option in the UI, aligning it with other knowledge integrations like Xwiki and SNOW. This change took place in the integration settings of Confluence, allowing users to enable or disable automatic synchronization. The purpose was to ensure consistency across knowledge integration options and enhance user control. This change is customer-facing, impacting users who manage Confluence integrations through the GUI.
- [AP-29975] - The issue preventing users from uploading and retrieving attachments on SOP pages in the Knowledge Base has been resolved. This change occurred in the SOP attachments tab of the Knowledge Base interface. It aimed to fix an error that hindered file uploads and retrievals, ensuring smoother operation and improved usability of the SOP pages. While this change primarily impacted backend processes, it ultimately enhances customer-facing functionality by improving the user experience for those interacting with SOP pages.
- [AP-29979] - The 400 "INTERNAL_SERVER_ERROR" issue when saving or updating workflows in the QA1 environment has been resolved, allowing users to create and modify workflows without errors. This change affects the workflow creation and cascade update functions in the IPworkflow module. It was implemented to ensure reliability in workflow management. While primarily a backend fix, it directly improves customer-facing functionalities by enabling seamless interaction with workflows for end-users.
- [AP-29980] - The issue preventing certain automata from executing within a workflow has been resolved, enabling users to progress through workflows without interruption. This change impacts the workflow execution interface in the AIOps platform, specifically when triggering automata from a workflow. It was implemented to fix a bug that hindered automata from triggering correctly, causing delays in workflow progression. This change affects both backend processes and customer-facing users who interact with workflow designs and automata executions on the AIOps platform.
- [AP-29990] - The retrieval process for trigger events evicted from the cache in the IPworkflow component has been fixed, ensuring accurate functionality. This update is backend-focused with no direct UI changes. It resolves an issue where trigger events could not be correctly retrieved after eviction, preventing failures in automated workflows. While not customer-facing, this change enhances the reliability of backend processes, indirectly improving user experience.

1.3 EPIC

None in this release.

1.4 STORY

- [AP-27728] - A calculation feature was added to measure the resolve time for each group involved in a ticket's lifecycle, alongside the total resolve time. This change pertains to backend operations and does not directly impact the user interface. The purpose is to enable granular analysis of resolver group performance by providing insights into the specific time contributions of each group. This change primarily affects backend analytics and will be valuable for teams analyzing resolver group performance through generated reports.

- [AP-28823] - The API has been enhanced to allow users to specify any authorized user as the actor in a workflow transition, rather than defaulting to a system user. This change is not reflected in the GUI; it impacts the API request structure and backend processing. The purpose is to give customers flexibility in accurately reflecting the user initiating a workflow transition, improving tracking and accountability of user actions. This change primarily affects the backend, particularly those integrating or using the API for managing workflow state transitions.

- [AP-28971] - A new feature in the Automata module allows users to manage a deny list of prohibited shell commands, including options to view, create, update, delete, disable, and enable commands. Integrated alongside existing sections like Executions, Matchers, and Scripts, the UI now supports managing deny lists at global and client-specific levels. This enhancement aims to improve system security by enabling users to define potentially dangerous commands, helping organizations mitigate risks. The change affects both backend and customer-facing aspects, with new administrative functionalities for the backend and UI updates for users with VIEW and ADMIN authorities.

- [AP-29108] - The system now automatically removes expired knowledge documents after manual imports, preventing duplicates by considering updates from external systems. This change occurs in the backend processes of AIOps and does not affect the UI. The purpose is to optimize document management by ensuring that expired entries are removed, particularly when document paths or names are updated externally. This change is backend-related and does not directly impact customer-facing interfaces.

- [AP-29237] - The platform now retains the selected client across different Amelia AIOps modules, so users no longer need to reselect the client when switching between modules. This change was made in the GUI of the Amelia AIOps platform, specifically affecting module navigation and client selection displays. The purpose is to enhance user efficiency and streamline workflows by maintaining client context, reducing interruptions, and minimizing the need for repetitive selections. This change is customer-facing, impacting users who navigate between various application modules on the Amelia AIOps platform.

- [AP-29335] - Clients can now choose between the existing Amelia AIOps-specific grading system (0-2 scale) and a new NPS-compatible grading system (1-10 scale) for task surveys, allowing for a more flexible and industry-standard measurement of user satisfaction and customer loyalty. A new configuration setting has been added to the Settings interface, allowing admins to select the preferred grading system. If the NPS system is selected, surveys will present a 1 to 10 scale for applicable questions, where 1 is the lowest score and 10 is the highest. This change aims to provide organizations with the flexibility to select a grading system that best meets their needs, enhancing the measurement of user satisfaction and loyalty in line with industry standards such as the Net Promoter Score. This

update affects backend operations by introducing a new configuration setting and is customer-facing as it influences how survey questions are displayed to users.

- [AP-29385] - Usernames and emails for various modules have been updated to align with a new naming scheme, including changing email domains from "ipcenter.ipsoft.com" to "aiops.amelia.com," and removing obsolete user accounts. These changes are backend modifications and do not directly affect the UI but impact user data and email integration. The purpose is to standardize naming conventions for module-related accounts and emails, enhancing organization, reducing confusion, and supporting branding initiatives. This change primarily affects backend systems and administrative operations but also impacts customers through updated outbound email addresses for user accounts and automations.

- [AP-29450] - Task attributes are now displayed in alphabetical order in the task view, improving user access and convenience. This change was made in the task view interface, where task attributes are listed. The purpose is to help users locate and access task attributes more easily by organizing them systematically. This is a customer-facing change, affecting how users interact with and view tasks in the interface.

- [AP-29587] - Advanced filtering capabilities have been implemented in Amelia AIOps for managing incoming and outgoing emails, allowing users to block specific addresses, control attachments, filter by subject patterns, and manage domain-specific processes. This change affects the administrative settings interface, where users can configure these filtering rules. The purpose is to streamline communication by processing only relevant emails, reducing unnecessary traffic, and improving task-related interactions, thereby enhancing the overall user experience. This update primarily impacts backend operations while also providing customer-facing tools for administrators to manage email interactions effectively.

- [AP-29590] - A new feature has been added to allow the direct upload of generated Standard Operating Procedures (SOPs) to ServiceNow, enhancing document management and sharing among engineering teams. This change introduces an SOP upload option after creation, offering a selection interface for ServiceNow knowledge bases and categories, along with auto-generation and editing options for a one-line summary. The purpose is to streamline documentation, reduce redundancy, and boost productivity by enabling engineers to manage and share SOPs within their workflows. This update impacts both backend integrations with ServiceNow and end-users with the necessary permissions to upload SOPs, while also involving admins in managing user permissions for this feature.

- [AP-29602] - The integration name and associated icon have been added to each knowledge article in the Knowledge module, indicating the source type. This change occurred in the Knowledge Article list within the Automation Workspace and aims to improve visibility for users regarding the source of each article, enhancing resource identification and integration tracking. This is a customer-facing change that affects users interacting with the Knowledge module in the Automation Workspace.

- [AP-29603] - An icon indicating the source of each knowledge article has been added to the Knowledge tab in the Task interface. This change enhances usability and integration transparency by providing users with a quick visual reference to identify the source of each article. It specifically impacts the customer-facing UI that users interact with while accessing the Knowledge tab in tasks.

- [AP-29606] - A change was made to the Knowledge API to include both the source and integrationID in each Knowledge Article returned from queries or searches. While this change does not directly affect the user interface, it enhances the backend API by providing additional data for better categorization and retrieval of information. The purpose is to enable users to identify and filter Knowledge Articles

based on their sources. This change primarily impacts backend systems and developers using the Knowledge API, but it ultimately benefits end-users by offering richer data in applications that utilize the API.

- [AP-29740] - This ticket led to the implementation of a native Gmail integration for the Amelia AIOps platform, allowing email exchange via the Gmail API with OAuth authentication. It supports inbound and outbound emails, including attachments, in both plain and rich text formats. Although the change mainly affects backend functionality without direct GUI modifications, interfaces for configuring email integrations will showcase these new capabilities. The aim was to enhance email functionality securely, removing the reliance on the Amelia Integration Framework. While primarily impacting the backend team, this change indirectly improves email capabilities for users on the platform.

- [AP-29781] - The terminology "White List" has been changed to "Allow List" in the Amelia AIOps platform to promote language inclusivity and clarity. This update occurred in both the Task Workspace and the Automation Workspace, where pre-approved commands are now labeled as "Allow List." The purpose of this change is to eliminate biased language and ensure clarity and precision in terminology aligned with its functionality. This update impacts both backend elements and the customer-facing UI, as users will now see the revised terminology throughout the platform.

- [AP-29805] - This ticket enabled downstream applications to send performance metrics to Amelia AIOps through both synchronous and asynchronous webhooks, allowing for real-time data processing and greater flexibility in transmission. As this update focuses on backend integrations with webhooks, it does not involve changes to the user interface. The purpose of this change is to improve Amelia AIOps by facilitating real-time monitoring and response to performance metrics, accommodating various use cases from immediate responses to high-volume data processing, thus enhancing system robustness. This change primarily impacts backend processes and is intended for developers and systems utilizing Amelia AIOps for performance metric monitoring and processing.

- [AP-29807] - An icon has been added to indicate the source of Knowledge Articles identified by Resolve with AI, replacing the existing AIOps icon with a source-specific icon (e.g., Confluence). This change was made in the Resolve with AI interface where Knowledge Articles (SOPs) are displayed. The purpose of this update is to help users easily identify the source of each Knowledge Article, thus improving transparency and usability within the system. This change primarily impacts the customer-facing UI, enhancing the end-user experience by providing clearer information about the origin of Knowledge Articles.

- [AP-29812] - A new feature has been introduced in Amelia AIOps, allowing users to choose whether to retain or delete imported knowledge articles when an integration is deleted. This change is reflected in the UI through a prompt that appears when a user attempts to remove an integration, giving them the option to keep or remove the associated knowledge articles. The purpose of this update is to provide users with greater control over their knowledge base content, ensuring it meets organizational needs. This change is customer-facing, impacting users who manage integrations and knowledge articles within the platform.

- [AP-29814] - An icon has been added to indicate the source of each knowledge article in the list when using the "Automate with AI" feature from existing Knowledge Articles. This change is reflected in the knowledge article list interface, accessible through "Automate with AI" -> "From existing Knowledge Article." The purpose of this update is to visually show the source of each article, enhancing users' ability to quickly identify and distinguish between articles based on their origin. This change is customer-facing,

directly impacting the user interface and experience for those interacting with the "Automate with AI" feature.

- [AP-29844] - The Workflow menu item has been relocated from the Operations section to the Configuration section in the platform's navigation menu. This change enhances user experience and navigation by logically positioning the Workflow menu under Configuration, reflecting its role in setting up and managing tasks. This adjustment is customer-facing, impacting users who interact with the platform's UI to design and configure workflows.

- [AP-29893] - A new feature is introduced in Amelia AIOps that allows users to choose whether to retain or delete imported knowledge articles when deleting an integration. A prompt has been added to the UI during the integration removal process, giving users the option to keep or delete the associated articles. This change is designed to give users better control over their knowledge base, ensuring content aligns with their organizational needs. It is customer-facing, impacting users who manage integrations and knowledge articles.

- [AP-29819] - The terminology "White List" has been updated to "Allow List" in the Amelia AIOps platform to ensure language inclusivity and clarity. This change occurred in both the Task Workspace and the Automation Workspace, where pre-approved commands are now referred to as "Allow List." The purpose of this update is to promote inclusivity, eliminate biased language, and ensure that the terminology is clear and aligned with its functionality. The change affects both backend elements and the customer-facing UI, as users will now see the updated term in the platform interface.

- [AP-29902] - A new option is introduced in Amelia AIOps allowing clients to choose between the existing 0-2 grading system and a new NPS-compatible 1-10 scale for task surveys. Admins can select the preferred grading system in the Settings interface, and if NPS is chosen, applicable survey questions will display a 1-10 scale, with 1 being the lowest and 10 the highest. This change provides more flexibility and aligns with industry standards for measuring user satisfaction and loyalty. It affects both backend operations with new configuration settings and is customer-facing, impacting how surveys are presented to users.

- [AP-29917] - A native Gmail integration was added to Amelia AIOps, enabling secure email exchange via the Gmail API with OAuth authentication. Supporting inbound/outbound emails, attachments, and rich text, this backend change enhances email capabilities, with UI updates in configuration sections. It eliminates reliance on the Amelia Integration Framework, indirectly benefiting users configuring email integrations.

- [AP-29923] - A new feature allows users to upload generated SOPs directly to ServiceNow, streamlining document management. The UI now includes an upload option with a selection interface for ServiceNow categories and summaries. This change improves productivity and reduces redundancy, impacting backend integrations and customer-facing users with upload permissions, managed by admins.

- [AP-29926] - An advanced filtering system has been woven into the fabric of Amelia AIOps, offering granular control over email exchanges. Administrators can now sculpt rules in the settings, blocking addresses, managing attachments, filtering by subject lines, and tailoring domain-specific email flows. This upgrade sharpens the efficiency of communication, carving out the noise and ensuring only relevant emails reach the surface. Though rooted in backend processes, it brings a direct benefit to customer-facing users, giving them the reins to fine-tune email handling and streamline task interactions in powerful, targeted ways.

1.5 TASKS

- [AP-29381] - The number of database queries for insert, update, and select operations in the execution_search Percona table has been significantly reduced to enhance performance and alleviate bottlenecks during performance testing. This change involves backend optimizations within database operations and is not directly reflected in the UI. The aim is to improve the performance of IPautomataExecutioner by reducing the query load on execution_search, minimizing unnecessary select operations, optimizing inserts, and ensuring updates only affect modified fields. While this change primarily impacts backend processes and internal performance, it optimizes system resource use and efficiency without directly affecting end-users or customer-facing features.

- [AP-29436] - The IPworkflow and IPradar databases have been merged, enabling all ticket-related operations, including workflow progression and data modifications, to occur within a single database transaction. This change does not directly impact the user interface, as it pertains to backend database operations. The purpose is to enhance performance and stability by allowing operations to be conducted in a single transaction, thereby reducing technical debt and potential data inconsistencies. This change primarily affects the backend components of the system and is not directly customer-facing.

- [AP-29443] - The event handling mechanism in the IPradar component has been optimized by eliminating a redundant SQL query for existing events and enhancing the caching strategy for event counts related to ticket performance data. This change does not directly affect the user interface, as it focuses on backend performance improvements. The purpose is to boost system performance by reducing unnecessary database queries and optimizing event data caching, which in turn improves the efficiency of event processing in IPradar. This change primarily impacts the backend processes of the event handling system and is not directly customer-facing, but it contributes to overall application performance.

- [AP-29444] - The workflow for IPticket event handling now initiates immediately after the optimization and merging of the IPradar and IPworkflow databases. This change aims to enhance performance by reducing unnecessary variable creation and ensuring efficient execution. Since it is a backend optimization, there is no direct change in the user interface. The goal is to improve the start time of the IPworkflow, boost system performance, eliminate technical debt from redundant processes, and ensure stability without affecting execution speed. This change primarily impacts backend processes, enhancing performance and stability in the system, without directly affecting end-users.

- [AP-29735] - The ticket aimed to optimize database queries in the AbstractUpdateResponse implementations by consolidating multiple queries into a single query, thereby enhancing performance. This change did not occur in the user interface; it primarily affected backend processes related to database queries within the IPworkflow component. The purpose was to reduce the number of database queries, improving overall performance and addressing technical debt within the system. This change specifically impacted backend operations, enhancing how the system queries subscriptions related to ticket notifications.

- [AP-29798] - The Java runtime environment has been upgraded to address security vulnerabilities. This change does not affect the user interface, as it is a backend modification. It primarily impacts backend processes and is not customer-facing.

- [AP-29799] - Weak TLS ciphers have been disabled to eliminate potential security vulnerabilities. This change does not impact the user interface, as it is a backend modification. It primarily affects backend processes and is not customer-facing.
- [AP-29804] - The Percona database has been upgraded to address security vulnerabilities. This change does not affect the user interface, as it is a backend modification. It primarily impacts backend operations and is not customer-facing.
- [AP-29880] - The GUI layout for creating and editing Metrics Integration configurations has been updated to match the design of the Event Webhook Sync Integration Configuration. This change is visible in the New and Edit sections of the Metrics Integration configuration interface. The purpose of this update is to enhance user experience and ensure consistency by using a familiar layout. This is a customer-facing change, as it directly affects the interface used by customers to configure Metrics Integration.
- [AP-29889] - The Spring framework has been upgraded from version 6.1.6 to 6.1.13 to address the CVE-2024-38816 security vulnerability. This change is a backend update and does not affect the UI. The purpose is to mitigate the identified security risk. This change primarily impacts backend systems and services that rely on the Spring framework, without directly affecting end users.
- [AP-29909] - The com.google.protobuf:protobuf-java library has been upgraded from version 3.24.4 to 3.25.5 to address the critical security vulnerability CVE-2024-7254. This change is a backend update and does not directly impact the user interface. Its primary purpose is to mitigate the identified security risk, ensuring the system's security and preventing potential exploits related to the outdated library. This update primarily affects backend processes that utilize the protobuf-java library, without affecting the customer-facing GUI.
- [AP-29934] - Virtual threads in the IPradar and IPworkflow components have been disabled to address issues related to thread pinning. This change is a backend operation and does not directly impact the user interface. The decision to disable virtual threads is temporary, with plans to revisit and resolve the underlying problems in future updates (as noted in AP-29931). As a result, this change primarily affects backend systems and does not have a direct impact on customers or the customer-facing interface currently.
- [AP-29962] - The Locksmith password configuration for the ipdeploy-service was updated to remove hardcoded values, aligning with recent changes from AP-28897. This change does not impact the UI; it involves backend modifications to application properties related to password handling. The purpose is to resolve issues with Content Pack imports of Locksmith data that were failing due to outdated password management methods. This change primarily affects backend services, specifically the ipdeploy-service, and indirectly improves operations for processes relying on Locksmith data.

1.6 SUB-TASKS

None in this release.