

# AI Ops

## AMELIA's Autonomic IT Management Platform

---

### Release Notes 3.9.0 (Document Version 1.0)

---

This AMELIA® documentation is copyright © 2025 Soundhound AI Amelia and their affiliated companies. All rights reserved.

This document is considered the confidential information of Soundhound AI Amelia and its affiliates. Disclosure to other parties is prohibited unless agreed to in a license or confidentiality agreement.

Trademarks, including AMELIA® and the AMELIA logo, are the intellectual property of Soundhound AI Amelia and its affiliated companies. Any other marks or intellectual property remain the property of their respective licensors or owners.

Table of Contents

**1. RELEASE 3.9.0 ..... 3**

1.1 RELEASE HIGHLIGHTS ..... 3

1.1.1 ROLLBACK TO A PREVIOUS VERSION ..... 3

1.1.2 MODULE-BASED ACCESS RESTRICTIONS IN REPORTING ..... 3

1.2 BUGS ..... 3

1.3 EPIC ..... 9

1.4 STORY ..... 9

1.5 TASKS..... 11

1.6 SUB-TASKS ..... 13

Document History

Author	Version	Date	Comments	Final Approval?
AMELIA Research & Development	1.0	January 31, 2024	Added tickets for 3.9.0 release	Yes

# 1. Release 3.9.0

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.

### 1.1.2 Module-based access restrictions in reporting

To access reporting data, users previously required either IPanalytics or Elasticsearch authority.

This has now been updated to allow access based on specific module authorities:

- events/metrics: IPredictive View
- connection\_session: IPconnect View
- ipcmdb\_ci: IPcmdb View
- ipcmdb\_audit\_log: IPaudit View
- knowledge\_document: IPkm View
- ipticket\_ticket: IPradar View
- ipautomaton\_version: IPautomata View
- ipautomaton\_execution\_history: IPautomata View

With the release of AIOps v3.11.0, the IPanalytics and Elasticsearch authorities will be deprecated.

**Action Required:** Please ensure that users requiring reporting data access are assigned the appropriate module-specific authorities instead of IPanalytics or Elasticsearch.

## 1.2 BUGS

---

- Added Missing Scroll Bar on Rules Page for Improved Navigation. A scroll bar has been added to the rules page, allowing users to navigate through content more easily. The change occurred on the rules page within the Problem Management component. The purpose of this change was to improve the user experience by providing a way to scroll through the rules list when it exceeds the viewable area on the page. This change is customer-facing, impacting users who interact with the rules page in the UI. (AP-28558)
- Removal of Deprecated HTTP Response Headers in GraphQL Component. Deprecated HTTP response headers were removed from the GraphQL component to address a vulnerability. The change does not directly affect the UI but involves HTTP responses handled by the GraphQL component. The purpose of

the change is to improve security by eliminating deprecated headers that could expose vulnerabilities. This change primarily affects the backend systems, although it has implications for all customer-facing services that interact with GraphQL APIs. (AP-28757)

- Incorrect Retry Statistics Displayed on Workflow UI. The display logic for retry statistics on the workflow UI was corrected. Previously, it incorrectly displayed "-1/0" when a user attempted to retry moving a workflow after encountering an error. The change occurred in the workflow tab of the ticket UI, specifically in the section where retry statistics are shown after a user clicks "Resume" and "Retry" on a workflow error. The purpose of this change was to correct the inaccurate display of retry statistics to ensure users receive accurate feedback on workflow attempts. It aimed to enhance user understanding of workflow operations and error handling. This change is customer-facing as it impacts the user interface experienced by end-users handling workflows in the ticketing system. (AP-29741)
- Fixed Regex OR Logic in Automation Matcher for IPradar Task. The issue with the regex OR logic not functioning correctly in conjunction with the 'contains' matcher for IPautomata was resolved. This ensures that matchers using "|" in regex correctly identify multiple words in IPradar tasks without requiring a wildcard. The change affects the Automata interface within the Orchestrator platform, specifically in the IPautomata component used for task matching logic. The purpose of the change was to address a defect where matchers configured with both 'contains' string logic and regex OR ("|") operators failed to match correctly. Ensuring automated tasks can match criteria accurately without unnecessary workarounds was essential for functionality. The change primarily affects backend operations, as it relates to the processing logic within the automation system. However, it ensures consistency and reliability in automated processes that customers configure in the Orchestrator platform. (AP-29750)
- Ensure cross-domain workflows do not trigger inaccessible automations. The import behavior was updated to prevent the execution of workflows and automations from domains for which the user lacks access. An error message will be displayed during import if there are inaccessible objects referenced. This change affects the import function in the UI where users import workflows and automations across domains. The change addresses a security vulnerability where automations from different domains could be triggered without proper access, potentially leading to unauthorized actions across domain boundaries. This change is customer-facing, specifically impacting users who import workflows and automations and ensuring they cannot trigger inaccessible or unauthorized components. (AP-30172)
- Implement User-Friendly Error Message for Task Linking Failure Due to Insufficient Authority. A user-friendly error message is now displayed when a user without the necessary authority attempts to link a task on the radar page. The change occurred on the radar page, specifically when a user tries to link tasks without the 'Elasticsearch View' authority. The purpose of this change was to enhance user experience by providing clear feedback when permissions are insufficient, preventing confusion and improving clarity on the required authority. This change affects the customer-facing side of the application, as it directly influences the UI elements that the user interacts with. (AP-30251)
- Resolved: Timer Execution Failure in Automations Due to Out of Memory (OOM) Error. The issue with the timer in the automations module not firing due to an out-of-memory (OOM) error was identified and resolved. This change pertained to the backend processing and did not directly affect the UI. The purpose was to fix a critical error where scheduled automations failed to execute as planned, which was causing disruptions for the clients using automation services. This change affected the backend systems, specifically those customers utilizing the automation feature in their workflows. The issue was customer-facing due to the direct impact on their scheduled automation tasks. (AP-30289)

- **Corrected Date Variable Handling Discrepancies in Workflow.** The handling of date variables in workflows was made consistent between versions. Previously, in v3, date variables were incorrectly formatted as arrays rather than plain fields as in v2. Additionally, issues with ISO 8601 date format acceptance were resolved, and propagation of date fields to sub-workflows was ensured. These changes are reflected in the API handling of workflow instances, affecting the format and propagation of date variables when tickets are created or updated via API or GraphQL. The purpose of this change was to align the handling of date variables across workflow versions, ensure compatibility with the ISO 8601 date format, and to fix issues regarding the propagation of date fields to nested workflows. This change primarily affects the backend of the application, particularly developers who interact with the API and those who manage workflows. It ensures consistency and reliability in date handling and processing within the system. (AP-30305)
- **Improved User-Friendly Error Message for Duplicate Tag Names.** An error message displayed when creating a tag with a duplicate name has been updated to be more user-friendly. The change occurs in the Tag Management section of the AIOps settings interface, specifically when attempting to create a new tag with a name that already exists. The purpose of this change is to enhance user experience by providing clear and understandable error messages, ensuring users are informed of the issue in a user-friendly manner when they attempt to create a duplicate tag. This change is customer-facing, improving the interaction users have within the AIOps Tag Management interface. (AP-30399, AP-30545)
- **Improve Tag Search Functionality to Return All Relevant Tags.** The search functionality for tags was enhanced to return all tags that contain the search term, not just those that begin with it. This change affected the tag search feature within the presales client interface on the platform. The purpose of this change was to improve the usability and effectiveness of the tag search feature by ensuring that all relevant tags containing the search term are returned, enhancing user experience. This change is customer-facing as it impacts how users interact with and search for tags in the client UI. (AP-30413)
- **Add Task Name to Success Message upon Task Resolution.** The task success message now includes the task name when a task is resolved, providing clearer feedback to the user. The change occurred in the user interface where task success messages are displayed upon task resolution. The purpose of this change is to enhance user clarity by ensuring that the success message is informative and explicitly indicates which task has been resolved. This change is customer-facing, affecting users interacting with the task management UI. (AP-30420)
- **Improved Error Messaging for ServiceNow Integration.** The error message for the ServiceNow Integration was updated to provide better clarity and guidance to the user on what they should do next after encountering an error. The change occurred in the ServiceNow Integration settings page, specifically in the section where error messages are displayed. The purpose of this change was to make the error message more informative and actionable, so users can understand what went wrong and how they can resolve the issue or whom to contact for support. This change is customer-facing, as it directly affects users interacting with the ServiceNow Integration within the application. (AP-30445)
- **Resolved issue with loading AIOps tasks with multiple attachments.** The issue preventing AIOps tasks with multiple attachments from loading has been identified and resolved. The change affects the task viewing section of the AIOps support UI where tasks with attachments are accessed. The change was implemented to address a WebSocket connection failure that caused tasks with multiple attachments to not load, ensuring users can access all task details and resolve support issues effectively. This change affects the customer-facing side of the AIOps support system, where users interact with support tasks. (AP-30449)

- Optimize Alert Trigger Time for Prometheus Integration. The alert triggering time for Prometheus integration was investigated and optimized to reduce it from 4 minutes to a more expected timeframe, closer to the Zabbix alert triggering time of approximately 1-2 minutes. The change is primarily backend and does not directly affect the user interface (UI). The purpose of this change was to align Prometheus alert trigger times with expectations and benchmarks, similar to Zabbix performance, by investigating possible discrepancies and optimizing the integration and scraping intervals. This change primarily affects backend operations and developers managing monitoring integrations, rather than end-users or customers directly. (AP-30450)
- Enhance Tooltip Display for Ellipsed Service Names in Radar Component. The tooltip functionality was improved to ensure that the full service name is displayed when users hover over ellipses in the Radar component. The change occurred in the Radar component's UI where service names are displayed with ellipses. The purpose of this change was to improve user experience by ensuring that complete service names are visible on hover, facilitating easier identification and interaction with services that have longer names. This change is customer-facing, impacting users interacting with the Radar component in the UI. (AP-30507)
- Implementation of Proper Error Messaging for Duplicate Client Creation. A user-friendly error message is now displayed when attempting to create a duplicate client, enhancing error handling for users in the system. The change occurred in the client creation interface where error messages are displayed to the user. The purpose of this change is to improve user experience by providing clear and informative feedback when a duplicate client entry is detected. This change also contributes to system security by preventing data redundancy and potential conflicts. This change is customer-facing as end-users interacting with the client creation form will now receive better feedback when attempting to create duplicate entries. It also involved backend changes to ensure the proper detection and handling of such scenarios. (AP-30511)
- Fix for Data Integrity Violation in CassandraToPerconaMigrationOfRules. A data integrity issue during the migration of rules from Cassandra to Percona was fixed. Specifically, it addressed the issue where a non-flyway migration would fail due to 'client\_id' being null, causing a DataIntegrityViolationException. This change does not affect the UI; it is related to backend data migration processes. The purpose of this change was to correct a data integrity issue during the rule migration process that prevented the successful execution of database insert operations due to null values in critical fields. This change affected the backend processes, specifically the data migration operations between Cassandra and Percona databases. (AP-30527)
- Resolved issue with AIOps API automation state not opening in the UI. The issue preventing users from opening the AIOps API automation state in the UI has been fixed. The change occurred in the AIOps section where users navigate to view the automation state and properties. The purpose of this change was to address a bug that hindered users from accessing the AIOps API automation state, ensuring that they can view and interact with the automation properties without issues. This change is customer-facing as it affected the user interface for accessing AIOps API automation states. (AP-30546)
- Restored ability to create custom variables using the Field section in Automation UI. The functionality to enter custom field values manually in the Field section has been restored. Users can now input custom variable names like "ticket.attributes.amelia\_var\_taskID" instead of being restricted to selecting predefined dropdown options. The change occurred in the Field section of the Automation UI, where users create and manage custom variables. The purpose of this change was to re-enable the flexibility for users to create custom variables by entering specific field values, which they could no longer do in

the current version. This enhances customization and expands user control over the automation process. This change is customer-facing as it directly impacts users of the Automation UI who need to create and manage custom variables. (AP-30555)

- Resolve Persistent Popup Issue on Automata Save. A persistent popup issue was fixed; now the popup closes or updates correctly when automata are saved. The change occurred in the section of the UI where users save automata within folders. The reason for this change was to improve user experience by ensuring interface consistency and preventing confusion by appropriately handling popup dialogs. This change was customer-facing, directly affecting users interacting with the automata generation interface. (AP-30586)
- Dropdown menu for legacy matcher shows incorrect tag list. The issue addressed in this ticket involves the dropdown menu for task tags when editing legacy matchers displaying tags from all clients accessible to the user instead of only showing tags from the specific automation client. The change affects the dropdown menu within the "Task tags" selection field found in the legacy matcher editing interface. The purpose of this change is to resolve a UI inconsistency where the dropdown menu was incorrectly displaying a broader list of tags, which could potentially lead to confusion and incorrect tag selection. Ensuring that only relevant tags are shown is crucial for maintaining accurate and efficient automation configurations. This change primarily affects customer-facing components, specifically users involved in editing automations with legacy matchers within the user interface. It does not impact the back-end functionality of the matching module. (AP-30587)
- Resolved Issue with Incomplete Tag List in Dropdown Menu. The issue where the complete list of tags was not displayed in the dropdown menu has been fixed, allowing users to scroll and access all available tags. The change occurred in the dropdown menu interface where tags are accessed. The purpose of this change was to ensure users can view and select from the full list of tags, enhancing functionality and user experience. This change is customer-facing, affecting users interacting with the tag selection UI in the application. (AP-30592)
- Enable email sending using "client\_credentials" grant type in native email integration. The integration system was updated to support sending emails using the "client\_credentials" grant type by leveraging the /users/{email}/sendMail API endpoint. This change does not involve any UI components as it is primarily a backend update affecting the email integration logic. The purpose of this change was to address the failure in sending emails for configurations using the "client\_credentials" grant type by implementing the correct API flow. Previously, the system attempted to use a delegated authentication flow that was not applicable for this configuration, resulting in errors. This change affects the backend systems responsible for handling email integrations, specifically for clients configured with the "client\_credentials" grant type. It does not directly impact end-users or customer-facing interfaces but indirectly allows emails to be sent correctly to end-users. (AP-30607)
- Fix to Display Events on Events Tab in Support Instance. This ticket addresses an issue where no events were being displayed on the events tab of the support instance. A solution was implemented to ensure events are correctly shown. The change affected the visibility of events on the events tab within the support instance of the application. The purpose of the change was to resolve a problem where events were not being displayed due to a back-end issue, thus ensuring users can view event data as expected. This change primarily affected the back-end, which resolved the display issues on the customer-facing events tab. (AP-30610)
- Resolved Aggregation Name Error in Move Frequently Used Attributes to Whitelist Migration. This ticket addressed a runtime exception that occurred due to the use of invalid characters in aggregation names



during the Move Frequently Used Attributes To Whitelist migration process. There were no changes to the user interface (UI) as this issue pertains to backend operations within the IPanalytics component. The purpose of this change was to prevent runtime errors during migration processes by ensuring that aggregation names do not contain invalid characters, specifically '[', ']', and '>'. This was causing HTTP 400 Bad Request errors. This change affected backend activities, specifically those related to data migration operations within the IPanalytics component. No direct customer-facing elements were impacted. (AP-30615)

- **Resolve Double Vertical Scrollbars in Automata Saving Prompt.** A UI issue was addressed where two vertical scrollbars appeared in the automata saving prompt, ensuring a clean and user-friendly interface. The change occurred in the automata saving prompt generated by GenAI. The change was made to improve user experience by eliminating unnecessary visual clutter, making the saving prompt more intuitive and aesthetically pleasing. This change is customer-facing, affecting users interacting with the automata saving feature in the interface. (AP-30628)
- **Fix for Downtime DSL Parsing Error in EventFlow.** A bug was fixed in the EventFlow service that caused an exception when parsing DSL inputs for downtime rules. This fix ensures the proper handling of static rules conversion to downtime objects. This change does not directly impact the UI as it involves backend processing within the EventFlow service. The purpose of this change was to resolve a backend issue where the system failed to parse downtime rules written in DSL if the value was missing before a logical operator. This caused the service to throw an `IllegalArgumentException`, affecting the application's functionality. This change primarily affects the backend. However, by fixing the parsing error, it indirectly ensures that end-users relying on downtime functionality in the UI will not encounter errors due to this backend exception. (AP-30635)
- **Resolved Error When Filtering Calendars in Content Packs.** The issue causing an error when filtering calendars within content packs has been resolved. This change affected the Calendar filtering functionality within the Content Packs section of the application. The purpose of this change was to fix an error that occurred when users attempted to apply filters to calendars in content packs, improving the reliability and functionality of the feature. This is a customer-facing change that affects users who interact with content packs and their calendar filtering capabilities. (AP-30640)
- **Restriction of Dashboard Access for Users Without Elasticsearch and Analytics Permissions.** With this change, users without Elasticsearch permissions will no longer see the Dashboards item in the menu. The change affects the main menu where the Dashboards option is typically listed. The purpose of this change is to ensure that only users with appropriate Elasticsearch permissions have access to the Dashboard feature, thereby enhancing security and resource management for the application. This is a customer-facing change, impacting users who attempt to access the Dashboards without the necessary Elasticsearch and Analytics permissions. (AP-30676)
- **Fix for Error When Creating Values Under Workflow Cascades.** The issue that prevented users from creating values under a cascade variable due to a "400: Bad Request" error has been resolved. Now, users can successfully create these values without encountering an error. The change primarily affects the backend processes related to workflow cascade variables and does not have a direct user interface component. The purpose of this change was to fix a bug that caused an error when users attempted to create values under a cascade variable in workflows, thus enhancing workflow functionality and preventing interruptions in user tasks. This change primarily affects backend systems but indirectly benefits users by ensuring that workflow-related tasks proceed without errors. (AP-30687)

- New Workflow Configuration Feature to Assign Default Task Type Workflows. A new Configuration page for Workflows has been introduced, allowing users to specify and manage a default workflow for each task type on a per-client basis. The change is visible in a newly created "Default Workflows" section within the existing Workflow configuration interface, where users can view, assign, update, or remove default workflows. The change was implemented to simplify the process of determining workflows tied to task types, reduce confusion caused by the Root workflow, and improve system performance by making task type to workflow assignments more explicit. This change has a user-facing impact in the UI, specifically for administrators or users responsible for configuring task type workflows. Although labeled as backend, this primarily influences workflow management from a client configuration standpoint. (AP-27877, AP-30222)
- Remove trailing slash requirement for API endpoints to improve request functionality. The requirement for a trailing slash in API endpoints was removed, allowing POST and PUT requests to work without appending a trailing slash. This change affects API endpoint URL behavior and indirectly impacts Swagger UI by ensuring its execute functions properly without requiring trailing slashes. The purpose of this change was to reduce confusion for API clients and prevent functional issues with POST and PUT requests that were caused by automatic redirection for URLs missing a trailing slash. It also aimed to improve the execution of API calls through Swagger UI. This change affected both backend processes and API consumers, enhancing their experience by allowing more flexible request formatting. (AP-28434)

## 1.3 EPIC

---

None in this release.

## 1.4 STORY

---

- Calendar Module: Implement Change Freeze Period Management. Functionality was added to the Calendar module allowing users to specify, view, and manage change freeze periods. During these periods, calendar events are disabled, but automations with specific tags can continue to run. Changes were made to the Calendar module within the Amelia AIOps platform, allowing users to configure and manage date and time windows for change freeze periods. The purpose of this change is to minimize potential disruptions during critical business periods by restricting calendar events execution while still allowing necessary automations with specific tags to operate. This change affects both backend functionality and is customer-facing, as users interacting with the Calendar module can configure and manage the change freeze settings. (AP-28441, AP-30223)
- Enhance Automation Engine with Configurable Retry Mechanism and Timeout Settings. The automation engine has been enhanced to include configurable options for retry count, retry timer, and timeout settings for the "Host Command State." This allows the system to automatically handle retries in case of request failures, aiming to improve workflow robustness. The changes are reflected in the Automation Settings view and the Automation Workplace, where users can configure retry counts, retry timers, and timeout settings for "Host Command State." The purpose of this change is to introduce a mechanism to handle transient errors effectively in automated workflows by allowing configurable retry attempts, timers, and timeouts. This aims to enhance the reliability of the system in case of temporary network or

service issues. This change primarily affects the backend but also impacts users such as Admins and Automation Developers who interact with the Automation Settings view and the Automation Workplace. (AP-30124)

- Clarification of Valid Values in "Event Webhook Sync Integration" Response. This ticket added detailed documentation on the valid values for the fields `event\_type`, `resolution`, `shortMetric`, and `metric` in the "Event Webhook Sync Integration" response, providing clarity on their significance. The change pertains to the documentation and integration settings of the "Event Webhook Sync Integration" component, but does not directly alter the visual user interface. Instead, it offers improved understanding for developers and users configuring the integration. The purpose of this change was to offer more comprehensive documentation that explains what values are valid for certain fields within the integration's response and to elucidate their meanings, which aids in accurate data interpretation and utilization. This change primarily affects developers and technical users who configure or troubleshoot the "Event Webhook Sync Integration." It is indirectly customer-facing, as it ensures they have accurate documentation to assist in proper setup and use of the integration. (AP-30133)
- Enhanced Automation Matchers Conversion and Content Pack Import/Export for Amelia AIOps. The ticket introduced a feature to convert version 2 automation matchers to version 3 within the Amelia AIOps platform and enabled the export and import of these matchers using the Content Pack format. This update provides a seamless transition between matcher versions, alongside improved portability and collaboration through the import/export functionality. The changes were implemented in the Matchers and Content Pack interfaces within the Amelia AIOps platform. Users can now convert matchers and perform import/export actions directly from these interfaces. The purpose of this change was to streamline matcher management by updating legacy matchers to a more efficient version (version 3), while also enhancing user experience with new functionalities for portability and collaboration, making it easier for users to manage and share automation work. This change is customer-facing, primarily affecting users of the Amelia AIOps platform who manage and utilize automation matchers within their workflows. It also involves backend components to support these functionalities. (AP-30353, AP-30541)
- Enhance UI to support dynamic "labels.\*" values for host, service, and metric fields. Support was added to allow host, service, and metric fields to contain dynamic "labels.\*" values, making them dependent on query results with specific labels. The change was implemented in the Integration and Prometheus components of the UI to accommodate dynamic label-derived values. The purpose of this change is to provide the ability for fields to dynamically adapt based on query results, thus offering more flexibility and precision in displaying relevant information. This is a customer-facing change, impacting users interacting with the UI, particularly those utilizing the Integration and Prometheus components. (AP-30408)
- Updated Execution and AutomatonModel to Use Tag Names Instead of Tag IDs. The Execution and AutomatonModel classes were updated to replace tag IDs with tag names in all automata-related objects. This change is not directly reflected in the UI as it pertains to backend data handling, but any displays or reports that pull tag information will now show tag names instead of tag IDs. The change was made to improve readability and clarity by displaying human-readable tag names instead of numeric tag IDs, which will facilitate better understanding and management of automata-related data. This is a backend change but it indirectly affects users who manage or consume reports or dashboards that include automata-related data by making the data more understandable. (AP-30460)

- Introduce Execution Group Parameter for HTTP Automations on ALite. The ability to specify an execution group for HTTP state automations was introduced, allowing particular HTTP calls to be directed through ALite. An "Execution Group" parameter was added to the user interface, which can accept a text value to specify the desired execution group for HTTP calls. The purpose of this change is to enable clients to perform HTTP calls through specific networks, such as ALite, especially when certain APIs are only accessible within their network. This ensures that the automation can function seamlessly regardless of the network constraints. Both backend processes and customer-facing components were affected, as it involves adjustments in how HTTP calls are executed in the automation platform and requires user interaction through the UI to specify execution groups. (AP-30532)
- Update Automation Execution to Use Tag Names Instead of Tag IDs. A new field, "tagNames," was added to the automation execution object to replace the existing "tagIds" field for easier identification and usage of tags by their names. The change was made in the automation execution interface where tag information is displayed or utilized. Users will now see tag names instead of tag IDs. The purpose of this change was to enhance user accessibility and comprehension by allowing users to identify tags by their names, which are more intuitive and easier to understand compared to numeric IDs. This change is customer-facing as it alters the user interface where automation execution details are presented. (AP-30540)
- Display Client Information on Native Integration View/Edit Pages. Client information, specifically Client Name and/or Client Code, is now displayed directly on the Native Integration View/Edit pages. The change occurred on the Native Integration View/Edit pages in the AIOps settings section. The purpose of this change was to improve user convenience and efficiency by eliminating the need to use the API to determine the client associated with a native integration. Previously, identifying the client required a cumbersome and time-consuming process. This change is customer-facing, impacting users who interact with the Native Integration View/Edit pages in the UI. (AP-30567)
- Creation of Announcement File for Amelia AIOps 3.9.0 Release. An announcement file was created for the Amelia AIOps 3.9.0 release. This file likely includes important information regarding the new features, changes, and improvements in the release. The change is primarily documentation and may not have a direct impact on the UI. However, information from the announcement file may be used in UI components that display release information or notes. The purpose of this change is to provide users and stakeholders with detailed information about the contents and highlights of the Amelia AIOps 3.9.0 release in a structured and official format. This is primarily a backend change for documentation purposes, but it is customer-facing as well because end-users, stakeholders, and teams involved in the release rollout will reference the announcement file for information about the release. (AP-30619)

## 1.5 TASKS

---

- Enhance Module-Based Access Control for Reporting. Module-based access restrictions have been implemented for the reporting component, requiring specific authority assignments for each data index. This change introduces new, index-specific authorities to enhance security and replace the previously generic authorities. The change affects access permissions configurations related to different data indices. This is primarily a back-end modification and does not directly affect the UI but impacts how users access data through the system. The purpose of this change is to provide a more granular level of access control over different data indices. The enhancement ensures better compliance with security

requirements and aligns the access control mechanism with the most up-to-date requirements. This change primarily affects backend systems and administrators managing user permissions. It indirectly impacts customers by requiring them to update their authority configurations to maintain access to data. (AP-26320)

- Upgrade Zabbix Grafana Plugin to Support Zabbix > 6.4. The Zabbix Grafana plugin was upgraded to a version that supports connections to Zabbix version 6.4 and higher, enabling compatibility for the client. This change does not directly impact the UI but ensures backend compatibility between the Zabbix Grafana plugin and Zabbix version 6.4 and above. The upgrade was necessary because the previous version of the Zabbix Grafana plugin didn't support connection to Zabbix versions greater than 6.4, preventing the client from using the plugin effectively. This change was backend-related, affecting the technical setup and functionality used by the client, ensuring their staging instance is compatible with newer Zabbix versions. (AP-30476)
- Integration of Gemini Tokenizer with Existing DocumentSplitter. The ticket explores the integration of a tokenizer API for Gemini with the existing DocumentSplitter implementation. This change is not reflected in the UI as it pertains to backend processing. The purpose of this change is to enable the use of a tokenizer for Gemini to split documents more efficiently, aligning with functionality currently used by OpenAI, thereby utilizing the capabilities of the Gemini tokenizer API. This change affects the backend systems, particularly those dealing with document processing using Gemini. (AP-30479)
- Implement Length Validation for Metric Fields in Webhook Integration. The change introduced length validation for all metric fields in the webhook integration according to specified AIOps limits. This change did not directly affect the user interface as it pertains to backend validation processes. The purpose of this change was to ensure that all metric fields conform to AIOps specified limits, preventing potential errors or data issues caused by exceeding these limits. This change primarily affected the backend system, ensuring data integrity and compliance with predefined limits. It does not have a direct customer-facing impact. (AP-30516)
- Upgraded Spring Security Core to Address Security Vulnerabilities. The version of the Spring Security Core library was upgraded from 6.2.3 to 6.2.8 to remediate security vulnerabilities. This change did not directly affect the UI as it pertains to backend security components. The purpose of this change was to address identified security vulnerabilities by using a more recent version of the Spring Security Core library that contains necessary patches and enhancements. This change primarily affects the backend systems. It does not have immediate customer-facing changes but enhances overall security. (AP-30550)
- Removal of Automatic Closure Timer in Announcements Modal. The timer and automatic closure feature of the announcements modal have been removed. The change occurred in the Announcements modal within the AIOps Core UI. The purpose of this change is to provide users with the ability to manually close announcements at their convenience, ensuring they have adequate time to read and comprehend the content without being rushed by a timer. This change is customer-facing, as it affects users interacting with the announcements modal in the AIOps Core UI. (AP-30616)
- Fix Import Failure for Automation Without Tags Due to IPtag Admin Restriction. A permissions issue was resolved to allow users without IPtag Admin authority to import automation that does not include any tags. The change primarily affects backend logic and permissions, so there is no direct change in the user interface. The purpose of this change was to correct an access denial issue that prevented users without certain admin privileges from importing automation processes that didn't contain tags, thus hindering

workflow operations. This change primarily affects backend operations but indirectly benefits end-users by allowing smoother automation import processes. (AP-30670)

## 1.6 SUB-TASKS

---

None in this release.