SoundHound AI
AMELIA

Autonomics

AMELIA's Autonomic IT Management Platform

Release Notes 3.14.0

(Document Version 1.0)

Table of Contents

Document History

Author	Version	Date	Comments	Final Approval?
AMELIA Research & Development	1.0	July 2, 2025	Added tickets for 3.14.0 release	Yes

1. Release 3.14.0

This section briefly lists changes to Autonomics 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 Page Size Limit Enforcement

In an upcoming release, we will enforce a maximum page size limit of 100 items across all paginated REST API endpoints.

WHAT'S CHANGING

- Clients requesting more than 100 items per page will receive a 400 Bad Request response.
- This change improves performance, prevents timeouts, and ensures more consistent API response times.

RECOMMENDED ACTION

- Review your API usage and update any requests specifying pageSize > 100 to comply with the new limit.
- If your integration relies on larger payloads, consider processing results across multiple pages.

This change will be introduced in version **3.17.0** or later (exact version to be confirmed). Please plan accordingly.

1.1.3 API Deprecation Notice: Attachment Endpoints

The following attachment-related APIs are deprecated and will be removed in version 3.17.0 or later (exact version to be confirmed). Please update your integrations accordingly.

Deprecated Endpoints:

- POST /api/attachments
  Replaced by: POST /api/tickets/${ticketId}/attach

- GET /api/attachments/${attachmentId}/content
  Replaced by: GET /api/attachments/${attachmentId}/download

We recommend updating your implementations to use the new endpoints to ensure continued functionality.

1.2 BUGS

- **Issue with Fail To Tab When Selecting Automation Properties**. A fix was implemented to ensure the Fail To tab properly displays properties when a specific automation is selected. The change occurred in the Fail To tab within the automation properties panel of the AIOps Core UI. The purpose of this change was to resolve an issue where the Fail To tab failed to display the expected properties, leading to a UI error when a certain automation was selected. This change affects the customer-facing UI, specifically users interacting with the automation properties in the AIOps Core UI. (AP-31449)

- **Fix URL Accessibility in Autonomics Without Trailing Slash**. The handling of URLs in the Autonomics interface was updated to ensure they function correctly even when a trailing slash is not included in the URL. The change took place in the Autonomics section of the AIOps Core UI, specifically in how URLs are processed and accessed. The purpose of the change was to enhance user experience by resolving an issue where URLs were not working properly unless a trailing slash was included, which could cause confusion and hinder navigation. This is a customer-facing change, as it impacts the frontend UI that users interact with when accessing the Autonomics feature. (AP-31509)

- **Event Integration Authentication Key Exposure Fixed**. The issue of the authentication key being exposed on tickets in the EventFlow system when using payload-based authentication for event integration has been resolved. The change occurred in the attributes tab of the ticket view within the Autonomics system, where the previously visible authentication key attribute is now hidden or obfuscated. The change was made to enhance security by preventing the exposure of sensitive authentication credentials in user interface elements, which could potentially lead to unauthorized access or data breaches. This change affected both backend systems and customer-facing interfaces. It primarily improves security for customers using event integrations and interfaces with the EventFlow component of the system. (AP-31521)

- **Resolve Issues with Email Ticket Integration Creating Duplicate and Infinite Loop Tickets**. The issue where email replies to tickets resulted in the creation of new tickets instead of updating the existing ones has been identified, and steps are being taken to resolve it. Additionally, infinite loops caused by these duplicate tickets are being looked into to prevent confusion and management difficulties for ticket owners. This change affects the email ticketing integration system, specifically in the section where ticket updates from email threads are managed. There's no direct impact on the customer-facing UI until the back-end issue is resolved. The purpose of this change is to fix the incorrect behavior of the email integration system where replies to tickets mistakenly create new tickets instead of updating the existing ones. It also addresses the infinite loop issue caused by the creation of duplicate tickets, which leads to confusion and operational inefficiencies. This change affects both back-end systems as it involves fixing the integration logic, and indirectly affects customers, as they experience smoother ticket processing without issues of duplicates or loops in the customer-facing ticket management interface. (AP-31392)

- **Address Null Pointer Exception in Workflow Field Update on Ticket Creation.** A fix was implemented to prevent the persistence of empty values in the TicketWorkflowFieldUpdate component. This change addresses the issue where an empty workflow field value caused a null pointer exception in the IPanalytics notification service during ticket creation. The changes were made at the backend level; there were no direct user interface modifications involved in this update. The change was necessary to handle empty values in workflow fields properly. This prevents the propagation of null values that led to a null pointer

exception during notification processing, thereby improving system stability and reliability. This change affects the backend, specifically the integration between the ticketing system and the IPanalytics service. It is aimed at backend developers and system administrators monitoring ticket workflows and notifications. (AP-31266)

- **Resolved Issue with Automation Assignment Using New Matchers**. The ticket addressed a functionality issue where users were unable to assign automation to run automatically with new matchers in the system. The resolution involved fixing the error that prevented this assignment process. The change took place in the AIOps dashboard, specifically within the sections dealing with automation and matcher assignment. Users interacting with the automation or matchers' UI will be directly impacted by this fix. The purpose of this change was to enable seamless automation assignment using new matchers, which were previously resulting in errors. This fix ensures smooth operation and aligns with client requirements for pushing new automation in Version 3 (V3). This change primarily affects backend operations by ensuring backend systems handle matcher-automation assignments correctly. However, it also has customer-facing implications as the end-users (possibly system administrators or automation engineers) directly utilize this feature in the UI. (AP-30690)

- **Fix for Data Retrieval Error from ipautomaton_execution_history Index.** This ticket addressed a data retrieval issue from the ipautomaton_execution_history index, which was preventing reports from being generated over the past five days. The error was causing the dashboard to fail to load properly, displaying a null pointer exception. The change impacts the dashboard interface where reports from the ipautomaton_execution_history index are accessed and displayed. The purpose of this change was to fix a bug that was causing a null pointer exception, resulting in users being unable to load or view reports from the specified index on the dashboard. This fix ensures continuity in report generation and access without interruptions. This change affects both backend processes and is indirectly customer-facing, as users and administrators of the AIOps application would experience the issues with report retrieval on the production instance. (AP-31061)

- **Ensure Client Field is Mandatory in Automata's Update Task Block**. The client field is now mandatory in the Update Task block within the Automata feature. This change prevents the creation and execution of automata with an empty client field to eliminate associated errors. The change took place in the Automata UI, specifically within the Update Task block of the task creation and management interfaces. This change was implemented to prevent execution errors by ensuring that the client field must be populated when creating or updating tasks. It enforces data integrity and enhances the robustness of the automation execution process. This change is customer-facing, affecting users creating or updating tasks within the Automata feature, ensuring they provide necessary client information to avoid execution errors. (AP-31333)

- **Resolved Discrepancy in ALites Connection Status Display**. The issue causing the ALites connection status to inaccurately display as Disconnected even when the ALite is functioning correctly was resolved. The change specifically impacted the area of the UI where ALites connection status is displayed to users. The purpose of this change was to rectify the misleading status display, ensuring users can accurately monitor and manage the operational status of their ALites. This change is backend-focused but impacts the customer-facing experience by improving the accuracy of status information displayed to users. (AP-31384)

- **Calendar Event Modifications Not Recorded in Audit Log**. The application was modified to ensure that any changes made to calendar events, such as changing the owner or updating the Run latest approved status, are now accurately reflected in the audit log. The issue was related to the display of changes in the audit log section of the application. There is no direct UI change that users will interact with, but users will now see accurate information in the audit log when they check it. The change was implemented to improve security and accountability by ensuring that all modifications to calendar events are properly logged. This will help maintain accurate records and facilitate auditing processes. This change primarily affects the backend systems, ensuring that audit logging is functional and accurate. However, it indirectly impacts users who rely on audit logs for validating changes and ensuring transparency. (AP-31191)

- **Resolved UI Issue with Additional Tags Display in CI List**. The CI list display has been updated to properly show all additional tags, rather than using an n+ indicator. This ensures clarity in displaying all tags associated with a CI. The change occurred in the Configuration Management Database (CMDB) user interface, specifically in the list view where Configuration Items (CIs) and their associated tags are displayed. The purpose of this change was to improve the user experience by removing ambiguity. The previous n+ notation for additional tags was not informative, and users needed to see all tags explicitly listed for a clear and complete understanding. This change impacts users who interact with the CMDB interface, particularly those who need to review and manage Configuration Items and their associated tags. It is a customer-facing change as it directly alters the way information is presented in the UI. (AP-31256)

- **Resolved Command Output Not Displaying on Terminal After Connection**. The issue causing command outputs to not display on the terminal after user connection to the host system has been resolved. Users can now execute commands and see appropriate outputs without errors. The fix was implemented in the terminal interface where command output was previously missing, ensuring functionality was restored in the command execution display area. The purpose of this change was to address a critical usability issue where users were unable to see command outputs after connecting to a host system, impacting their workflow and effectiveness. This change primarily affected end-users who interact with the terminal interface in customer-facing applications for issuing commands on connected host systems. (AP-31393)

- **Resolved NullPointerException in Session Retrieval for Specific Connections**. The issue causing a NullPointerException during the retrieval of session details for specific connections was identified and resolved. This fix ensures that session data can now be fetched without errors for the affected connections. The change affects the backend system responsible for processing API calls and does not have a direct user interface component. However, the error was affecting the ability to preview details of specific connections via the provided URLs. The purpose of this change was to address a critical bug that resulted in a NullPointerException during API calls for session retrieval. The error occurred because a null value was being passed where a non-null 'name' value was expected, causing a failure in the processing sequence for certain connections. This change primarily affects the backend services. However, it indirectly benefits end-users who access connection details through the platform by ensuring they do not encounter server errors when requesting session data for specific connections. (AP-31528)

- **Restriction on Editing Theme Code in the UI**. The ability to edit theme code through the UI was restricted, resulting in an error message if an attempt is made. The change occurred in the Edit Theme section of the Autonomics settings under the specified URL path. The change was implemented to prevent unauthorized or improper edits to theme code, which could potentially impact the application's integrity or performance.

This change primarily affects backend operations but has implications for frontend users attempting to modify theme settings through the UI. (AP-31228)

- **Standardized Error Responses for Login Failures**. The error message displayed when a non-existent user attempts to log in has been standardized. Previously, it exposed specific technical information; now, it returns simplified and secure error codes, such as `authentication.failed` along with a generic message of Login failed. The change occurs in the login error message display part of the user interface, specifically when login failures occur due to non-existent users. The purpose of this change was to enhance security by avoiding the disclosure of sensitive internal information in error messages, which could potentially be exploited by malicious users. Standardized error messages limit the amount of technical information provided. This change affects the backend processes involved in user authentication and is customer-facing because it alters the error messages visible to users. (AP-31229)

- **Incorrect Duplication of Request ID in SAML Auth System Audit Logs**. The SAML authentication system audit log was updated to remove the duplicate entry of the request ID, ensuring that it only appears once in the error messages. The change occurred in the UI section where the error messages related to the SAML authentication audits are displayed. The purpose of this change was to correct the error message formatting in the audit logs by removing the unnecessary duplication of the request ID, thereby making the log entries clearer and more accurate. This is a backend change that affects system administrators and developers who access and review the audit logs for authentication systems. (AP-31312)

- **Restriction of Default User Group Dropdown to Only Show Explicit Group Types**. The default user group dropdown has been updated to show only explicit group types, eliminating other unnecessary options like CLIENT and CLIENT_LEADS. The change occurred in the default user groups dropdown menu within the application's UI. The purpose of this change was to streamline the user selection process by displaying only the relevant, explicit user groups, thus improving user efficiency and reducing confusion. This change is customer-facing as it affects the user interface where users interact with the dropdown to select user groups. (AP-31321)

- **Implement Automatic Redirection to Login Page Post Session Expiration**. Automatic redirection to the login page after a user session expires or the user logs off has been implemented. Previously, users were not redirected automatically and had to click on a UI element to navigate to the login page. The change impacts the UI behavior post-session expiration, ensuring users are automatically directed to the login page without requiring further interaction with the application interface. The change aims to enhance user experience by ensuring a seamless transition to the login page once a session expires or the user logs off. This prevents confusion and improves security by guiding users to authenticate again before accessing the application. This change is customer-facing, as it directly affects the way users interact with the application upon session expiration or logoff. (AP-31329)

- **Fix Auto-Refresh Issue on IPlocksmith Page After Data Update**. This ticket resolves an issue where users had to manually refresh the IPlocksmith page to see updates after modifying the expiration date and notes. The change occurs on the IPlocksmith page, specifically when updating details that previously required a manual refresh to display correctly. The purpose of this change is to enhance user experience by ensuring that updates to the expiration date and notes are reflected automatically without requiring additional

manual steps, thus improving workflow efficiency. This is a customer-facing change that directly affects users interacting with the IPlocksmith feature in the UI. (AP-27029)

- **Resolve attachment cleanup issue for deleted clients**. The automatic attachment cleanup process was fixed to ensure it successfully deletes attachments for deleted clients according to the specified client setting. This change is not directly visible on the user interface, as it affects the backend service that handles attachment cleanup. The change was implemented to correct a backend issue where attachments would not be deleted when a client was removed, thereby posing a potential data management problem. The service was expected to delete attachments after a defined number of days post-task resolution but failed in cases where the client had been deleted. This change primarily affects the backend services responsible for attachment management, with indirect impacts on overall data integrity for users relying on consistent and efficient attachment cleanup. Contractors and technical teams managing client data are also impacted, as they benefit from improved backend processes. (AP-31201)

- **Adjusted Default Date Value for Workflow Tasks to Current System Time**. The default date value for the workflow field when creating a new task got updated. Instead of using the workflow creation date, it now uses the current system time to prevent must be a valid date errors. The change occurs in the task creation section of the workflow interface, specifically affecting the date field that initializes when a new task is being created. The purpose of this change was to eliminate the must be a valid date error that users encountered when the system defaulted to the workflow creation date. By using the current system time as the default, the task creation process becomes smoother and less prone to user error. This change is customer-facing as it directly impacts users interacting with the task creation feature in the workflow interface. (AP-31382)

- **Fixed All Clients selection issue in clients drop-down menu**. The issue where selecting All Clients from the drop-down menu defaulted to the AIOps client has been resolved. Now, choosing All Clients correctly selects the intended option. The change occurred in the clients drop-down menu within the application interface, specifically related to the All Clients selection functionality. The purpose of this change was to fix a bug that caused incorrect default selection, ensuring that users can accurately select the All Clients option without it defaulting to a specific client. This change was customer-facing, affecting users interacting with the application's client selection drop-down menu. (AP-31404)

- **Error Resolved: Delays in Redis Cache Clearing Due to Missing Deployment in Workflow Deletion**. The issue causing a failure in the workflow deletion process due to a missing deployment ID was identified and resolved. This fix ensures that Redis cache is cleaned properly during such deletions, enabling workflows with the same name to be recreated without encountering errors. This change involved backend processes related to workflow deployment management and does not directly affect the user interface. The change was made to address an error where the deletion of a workflow failed due to a missing deployment ID. The failure prevented the Redis cache from being cleared, thereby blocking the creation of new workflows with the same name. The purpose of the fix is to ensure seamless workflow management and prevent stale data in the cache. This is a backend change specifically affecting system operations related to workflow deployment management. The fix improves the backend process but has indirect benefits to users by ensuring smoother operations and preventing errors in workflow recreation. (AP-31549)

1.3 EPIC

- **Implementation of Private and Public Comment Visibility in Task Collaboration**. The implementation adds support for private and public comments, allowing users to control the visibility of their comments based on login groups. Users can now designate comments as public or private, ensuring that sensitive information is only visible to intended recipients. In the task collaboration interface, users will find options to classify their comments as public or private. This will typically be represented at the comment input section of the UI, where users choose visibility settings for each comment. The purpose of this change is to enhance confidentiality and collaboration by restricting sensitive information to specific login groups while ensuring availability of non-sensitive communication to relevant stakeholders. This prevents unauthorized access via integrations, email notifications, or external systems. This change is customer-facing as it directly impacts users interacting with the task collaboration interface, providing them with more control over comment visibility settings. (AP-30908)

1.4 STORY

- **Enhanced Content Pack Support for Authentication Systems**. This update allows users to export and import Authentication Systems and associated Password Policies within a Content Pack, enhancing the ability to transfer and reuse security configurations across different environments. It includes functionalities like sorting, searching, and bulk selecting Authentication Systems. Changes are implemented in the content packaging interface where users interact with Authentication Systems. This includes components to export, import, sort, search, and bulk select authentication configurations. The purpose of this change is to improve operational efficiency, consistency, and governance by enabling the structured reuse and transfer of authentication configurations and associated policies across different environments. This change affects users who manage security configurations across environments. It is primarily backend-focused, impacting system administrators and operations teams responsible for configuration management and deployment automation. (AP-31416, AP-31417)

- **Implement centralized configuration for platform cloud storage credentials in Helm charts**. The change allows for centralized configuration of cloud storage environment variables in Helm charts, ensuring that these variables can be applied consistently across multiple services. This change does not directly affect the UI. It involves configuration changes within the Helm charts for backend services. The purpose of the change is to streamline the configuration process by allowing environment variables needed for cloud storage authentication to be set in one place, making the setup more efficient and less error-prone. This centralization also aligns with best practices for managing cloud credentials securely. This change primarily affects backend configuration processes and DevOps teams managing service deployments. It is not directly customer-facing. (AP-31120)

- **Automated Cloud Storage Integration for Secure Platform Data Management**. A new, automated Cloud Storage Integration was introduced to securely store platform-related data like imported knowledge articles. This integration supports multiple cloud providers, including AWS S3, Google Cloud Storage, Azure Blob Storage, and Oracle Cloud Storage. It eliminates the need for user-configured integrations by utilizing application properties for automatic provisioning and management. There is no change in the UI, as the integration is managed entirely through backend application properties instead of a user interface. The purpose is to enable safe, centralized storage of vital platform data across various cloud storage services

without requiring manual user configuration. This ensures flexibility, security, adherence to best practices, and seamless integration with existing frameworks. This change primarily affects the backend of the platform, as it impacts how data is stored and managed. It indirectly benefits users and administrators by providing more reliable and automated data storage solutions without requiring user interaction on the front end. (AP-30836)

- **Migration to Google Gemini 2.0 Models in Vertex AI for Enhanced Performance and Stability**. This ticket facilitated the migration from deprecated Google Vertex AI Gemini 1.5 models to the Gemini 2.0 models, ensuring continuity of services and access to improved performance and features across the platform. It included endpoint replacements, performance testing, and updated documentation. The change primarily affected the backend services rather than the user interface, specifically in the AI model endpoints that interact with Google's Vertex AI platform. The purpose of this change was to prevent service disruption due to the deprecation of Gemini 1.5 models, and to take advantage of the enhanced performance, stability, and advanced features offered by the Gemini 2.0 models. This change affected backend operations and was directly relevant to internal teams responsible for AI model integration, testing, and documentation. End users would indirectly benefit through improved AI output and functionality. (AP-30963)

- **Enhancement of Outbound SMTP Email Integration for Diverse IT Environments**. The system now supports outbound email functionality through any standard SMTP server, with options for authenticated and unauthenticated configurations. It includes support for various authentication methods (LOGIN, PLAIN) and secure connection protocols (STARTTLS, SSL). The user interface allows configuration of SMTP server details, such as hostname and custom port numbers. The change occurred in the email integration settings within the user interface, where users can now configure SMTP server details, choose between authentication options, and secure connection methods. The UI also includes settings related to hostname and port configuration. The purpose of this change is to enhance the flexibility and compatibility of the platform's email capabilities across diverse IT environments by allowing users to send automated emails through any standard SMTP server. This enhancement aligns with security best practices by securely managing credentials and supports a variety of secure transmission methods. This change is primarily customer-facing, as it enhances the options available to end-users and administrators when configuring outbound email capabilities in the platform. However, it also requires backend updates to handle the various connection protocols and authentication methods securely. (AP-31056, AP-31057)

- **Integration of AWS Cloud Storage Support into Platform**. The platform has been updated to support integration with AWS Cloud Storage, enhancing our cloud storage options. This change is not UI-specific; it involves backend integration allowing AWS Cloud Storage to be utilized for storage solutions. The purpose of this change is to expand platform capabilities by allowing users to leverage AWS Cloud Storage for their data, providing more flexibility and options for cloud storage. This change primarily affects the backend infrastructure, although it ultimately benefits customers by offering additional storage solutions. (AP-31096)

- **Added Support for Azure in Platform Cloud Storage Integration**. Support for Azure has been added to the Platform Cloud Storage, allowing it to integrate with Azure's cloud storage solutions, similar to existing support for GCP and AWS. There were no direct UI changes, as this is a backend integration. Changes primarily occurred in the backend platform's configuration and integration modules. The purpose of this change was to expand the platform's cloud storage options to include Azure, thus providing users with more flexibility in choosing their preferred cloud storage provider based on their specific needs and existing

infrastructure. This change primarily affects the backend, specifically developers and engineers who work on the platform's integration capabilities. However, it indirectly benefits customers by offering them more storage integration options. (AP-31097)

- **Implement Oracle Cloud Storage Support for Platform**. Oracle Cloud Storage support has been added to the platform, allowing for integration and usage similar to existing GCP and AWS implementations. This change does not directly affect the user interface as it is related to backend integrations. The purpose of this change is to extend the platform's cloud storage capabilities by supporting Oracle Cloud Storage, providing users with broader and more versatile cloud storage options. This change is primarily backend-focused, affecting developers and systems that rely on cloud storage integrations. It does not directly alter the customer-facing elements of the application. (AP-31098)

- **Introduce Customizable Password Reset Email Templates**. Password Reset email subject and body templates, which were previously hardcoded, are now customizable and integrated into the existing email integration system. This change affects the backend system; hence, there is no direct user interface component affected. However, it allows for configuration flexibility through the email integration module. The purpose of this change is to allow easier customization of the Password Reset email templates, enabling adherence to branding guidelines and personalized communication. This change primarily affects the backend system but has customer-facing implications as it enhances the flexibility of email communications with end-users. (AP-31125)

- **Addition of Password Reset Email Template to Email Integration**. The Password Reset email's subject and body templates, which were previously hardcoded, have now been integrated into the email integration system. This makes them similar to the Ticket Update email template in terms of management and customization. The change affects the email integration settings where email templates are managed. Users can now configure or customize the Password Reset email templates in the same section as other email templates. The purpose of this change was to provide a more flexible and easier way to manage the Password Reset email templates by allowing them to be customized within the email integration settings. This aligns with the existing structure for other templates and allows for uniformity and easier updates. This change is customer-facing as it affects how administrators can customize and manage email templates that are sent to end users for password resets. (AP-31225)

- **New Automation Generation Setting for AI-Driven Automation Control**. A new Automation Generation Setting was introduced within the Automation Settings view in Amelia AIOps. This feature allows administrators to choose between automatic and manual generation of automations using generative AI. The change occurred in the Automation Settings view, specifically adding options for the Automation Generation Setting and a Generate Automation button on the SOP page when the manual option is selected. The purpose of this change is to provide administrators with enhanced control and flexibility over the automation generation process. It enables users to decide when and how automations are generated, allowing alignment with their company's standards and avoiding unnecessary generation of automations. This change affects backend processes but has a customer-facing impact as it provides administrators and users interacting with the Amelia AIOps interface with new settings and controls over automation generation. (AP-30632, AP-30866)

- **Enhanced Comment Visibility in Automation Engine: Private and Public Options**. The Automation Engine now supports distinguishing between public and private comments within its Designer interface. This allows automation-driven task updates to be categorized based on their visibility, ensuring sensitive information is only accessible to intended audiences. This change occurred within the Automation Engine's Designer, where users can specify the visibility of comments as either public or private when automations update tasks. The purpose of this change is to enhance control over task-related communications by providing options for specifying comment visibility. It aims to ensure compliance and security by restricting access to private comments and preventing them from being shared externally. This change primarily affects backend systems by modifying how comments are managed within automations. It indirectly impacts end users who interact with task updates via automations in the Automation Engine. (AP-27681, AP-30912)

- **Enhancements to Task History: Filtering and Sorting Capabilities**. The Task History View now includes the ability to filter and search based on the source of updates, as well as any content in the history. Additionally, users can sort the Task History either by newest or oldest entries on top. The changes are implemented in the Task History View section, where users can now select filters and sorting options for viewing task updates. The purpose of this change is to enhance user experience by providing more control over how Task History data is viewed. This includes the ability to isolate updates from specific sources and sort information according to user preference, making it easier to navigate and manage task-related information. This change is customer-facing, impacting users who engage with Task History View to manage task information and history logs. (AP-28884, AP-31368)

- **Transition Attachment Storage to S3 for Enhanced Performance and Scalability**. Attachments that were previously stored in the Percona MySQL database are now stored in S3 object storage. This transition optimizes database performance and enhances scalability by offloading file storage. There were no changes to the UI. Users can continue to upload, download, and delete attachments as they did previously, without any perceptible differences in the interface. The purpose of this change is to optimize database performance and scalability by moving attachments to an external file storage solution. This allows for improved performance and a scalable architecture capable of handling larger volumes of data while ensuring secure and seamless access to attachments. This change primarily affects the backend system. While it is not directly customer-facing, it impacts backend operations related to file storage and retrieval, ensuring enhanced performance and security for the end-users in an invisible manner. (AP-30854)

- **Implement Public and Private Comment Functionality in Workflow Designer**. The Workflow Engine's Designer now supports distinguishing between public and private comments within tasks, allowing users to control comment visibility based on login groups and ensure sensitive information remains secure. The change appears in the comment section of the Workflow Engine Designer, where users can now choose between adding a public or private comment, and specify the visibility of private comments to particular login groups. The purpose of this change is to enhance security, compliance, and communication relevance within workflows by enabling users to restrict the visibility of private comments and prevent them from being shared externally. This change is customer-facing, as it impacts end users working within the Workflow Engine who manage or view task-related comments. (AP-27680, AP-30911)

1.5 TASKS

- **Ensure Mutual Exclusivity Between Dynamic Link Variable and Explicit Automation**. The system was updated to ensure that when linking automation, only either a Dynamic Link Variable or an Explicit Automation Name is provided, not both. The change was implemented in the automation linking interface found within the AIOps Core UI. The change was made to prevent conflicts and ensure correct execution of the linked automation by enforcing a mutually exclusive condition between the two types of input. This change affects both backend processes handling automation link execution and customers using the interface to link automation. (AP-31380)

- **Improve AIOps Service Resilience Against Single Node Failure in External Backend Setups**. The AIOps services were updated to ensure continued functionality even if one node out of three in external backend configurations (Redis, Percona, Cassandra) goes down. There were no changes in the UI as this update affects backend service stability. The purpose was to enhance the robustness and resilience of AIOps services by making sure they can tolerate the failure of a single node in a three-node configuration, thus minimizing service disruptions. This change affects the backend systems and enhances the overall stability and reliability of the services provided to the customers. (AP-31400)

- **Update Setting Label to 'Auto Approve Automations'**. The label for a setting has been changed from 'Auto Approve linked Automations' to 'Auto Approve Automations' to better reflect its functionality. The change occurred in the settings section of the Content Pack UI. The change was made to clarify that the setting applies to all automations, not just linked ones, thereby reducing user confusion. This is a customer-facing change, affecting users who interact with the Content Pack user interface. (AP-31422)

- **Implement Custom Autonomic Headers in Gmail and Office365 Email Integrations**. Custom autonomic headers have been added to Gmail and Office365 email integrations for better management of incoming emails based on specific email activities. These headers are pre-configured with default settings and are toggleable boolean fields. The change occurred in the email integration settings under the section labeled Drop Incoming Mail With Header, where the new boolean toggle fields corresponding to custom autonomic headers have been added. The purpose of this change was to allow users to classify and manage incoming emails automatically using specific custom headers. This feature enhances the ability to process emails based on the source, such as user tasks, mail activities, and other automated email actions, providing greater control and automation within the integration. This change is customer-facing, affecting users who utilize Gmail and Office365 email integrations, providing them with new configuration options within the user interface to manage incoming emails more effectively. (AP-31452)

- **Improved Automation Link Action Configuration Validation**. The ticket improved the handling of automation link actions by enhancing validation messages and removing an unused option (Inline checkbox) from the configuration. It also streamlined what variables and connections are shown and allowed for better configuration of Spawned executions. The changes took place on the automation configuration page within the IPautomata component where users define link actions for automations. Specifically, adjustments were made to the visibility of variable and connection drop-down lists when configuring automation Overrides. The purpose of this change was to prevent misleading configurations that could lead to incorrect automation behaviors. By ensuring only relevant options appear, and improving validation messages, users are guided toward the correct setup more effectively, reducing confusion and potential errors. This change

affects both the backend and customer-facing components, as it involves UI changes that users interact with directly and backend validation enhancements. (AP-30849)

- **Upgrade Dependencies to Mitigate ALite Security Vulnerabilities**. Dependencies were upgraded to their latest supported versions, excluding Python-related dependencies such as pip and setuptools, to address and remediate existing security vulnerabilities in the ALite component. The change does not directly impact the user interface as it involves backend dependency updates. The purpose of the change was to mitigate security vulnerabilities identified in the ALite component by updating dependent libraries and tools to ensure the system remains secure and up-to-date. This change affects the backend systems and is not directly customer-facing. It ensures enhanced security and stability within the backend infrastructure. (AP-31359)

- **Upgrade Dependencies to Mitigate ALite Security Vulnerabilities**. Dependencies used by IPautomataLite were upgraded to their latest supported versions to address and remediate identified security vulnerabilities. This change does not affect the user interface; it involved backend dependency upgrades. The purpose of this change was to ensure the security and stability of the application by mitigating known vulnerabilities in the dependencies. This change affected the backend systems. It is not customer-facing and does not impact the user interface directly. (AP-31496)

- **Removal of Unused 'Add Connection Sessions to Reporting' Setting**. The 'Add connection sessions to Reporting' client setting has been removed as it is no longer in use. The change occurred within the client settings section of the application interface where this setting was previously available. The purpose of this change was to declutter the user interface and configuration options by removing a setting that is no longer functional or relevant, thereby improving user experience and maintaining application relevancy. This change is primarily customer-facing, affecting end-users who would have interacted with or configured the 'Add connection sessions to Reporting' setting in their application setup. (AP-31288)

- **Deprecate Unused IPportal APIs for Optimization**. Several unused APIs related to external providers, login availability, shifts, skills, skill ratings, support tiers, and work schedules were deprecated and removed from the codebase. There was no direct change in the UI as this update pertains to backend API management. The purpose of this change was to clean up technical debt by removing deprecated APIs that were no longer in use, thereby streamlining the codebase and potentially improving system performance and maintainability. This change primarily affected the backend team, with no direct impact on customer-facing features or the user interface. (AP-31316)

- **Enhanced Node Failure Tolerance and Dependency Update for Redisson Integration**. Redisson library was updated from version 3.27.2 to 3.49.0 to address issues with node failure tolerance and potential hanging during RLock acquisition. The update includes the possible requirement to manually include jboss-marshalling dependencies due to their removal and addresses deprecated use of certain Redisson objects. Configuration properties may also be exposed to allow dynamic connectTimeout settings. This change is not directly visible in the user interface as it primarily affects backend operations. The purpose of this change was to improve stability and reliability by enhancing node failure tolerance from Redisson, addressing PubSub-related issues, and resolving hanging operations. Additionally, fixing deprecated Redisson object usage and providing configurable timeout settings were goals to increase system robustness. This change affects the backend operations, specifically those involving Redisson distributed locks and queues. While

customers may experience indirect benefits like improved system stability, the change is not directly customer-facing. (AP-31401)

- **Improved Percona Driver Stability with Failover Configuration**. This change updates the Percona driver's configuration to improve fault tolerance by implementing a shorter connection timeout and enabling failover modes, allowing the system to better handle situations where one out of three nodes is down. This change primarily affects the backend configuration settings and is not directly visible in the UI. It involves configuration of the Percona driver's timeout and failover settings which affect how the system interacts with database nodes. The purpose of this change is to prevent system hang-ups when accessing a downed Percona node. By implementing a shorter connect timeout and enabling the failover mode, the system can quickly reroute to an available node, thus improving overall stability and performance when node failures occur. This change primarily affects backend operations and the development team managing database connection settings. It indirectly benefits customers by providing a more stable and reliable system performance. (AP-31402)

- **Optimize Cassandra connection timeout to reduce startup delay**. The connection timeout for the Cassandra driver was reduced to the default value of 5 seconds, and it was made configurable through environment properties. This change affects the backend configurations and does not have a direct UI impact. The purpose of this change was to minimize the startup delay caused by the Cassandra driver attempting to connect to a down host, which took 35+ seconds due to multiple connection attempts with a long timeout. This change affects the backend systems, particularly those relying on the Cassandra driver for database connectivity. It is not directly customer-facing. (AP-31403)

- **Automated Key Generation and Storage for SAML Authentication Setup**. With this update, when setting up SAML authentication, if the user does not provide an existing private/public key pair, the system will automatically generate them and store them in Locksmith. This ensures users can utilize the *sign request* and *encrypt assertions* options without manual key input. The change impacts the SAML authentication system setup page, where users configure options such as *sign request* or *encrypt assertions*. There is no direct UI change, but the functionality now includes automatic key generation and storage. The purpose of this change is to streamline the setup process for SAML authentication by reducing the burden on users to manually provide or configure cryptographic keys, thereby enhancing the user experience and reducing setup errors. This change primarily affects the backend process and indirectly benefits users who set up SAML authentication systems by simplifying the configuration steps. (AP-31470)

- **Improve Attachment API to Enhance Security and Data Integrity**. A review and potential removal of insecure APIs related to handling attachments in IPradar are suggested. Specifically, the changes aim to remove the ability to attach any accessible attachment blob to a ticket without proper ticket update entries. The handling of cloned ticket attachments is also addressed to ensure they are retained during cleanup operations. The changes are backend-related and involve the IPradar API, specifically the AttachmentApi.java file. There is no direct user interface change as it primarily concerns API functionalities and security. The purpose of the changes is to address security risks where attachments can be inexplicably linked to multiple tickets without proper authorization or tracking. It also aims to prevent data loss issues related to attachment content when tickets are cloned and cleaned up. This change affects backend processes and is primarily of interest to developers and system administrators managing the IPradar API. It is not directly customer-facing. (AP-31197)

1.6 SUB-TASKS

None in this release.