Autonomics

AMELIA’s Autonomic IT Management Platform

Release Notes 3.12.0

(Document Version 1.0)

Table of Contents

Document History

Author	Version	Date	Comments	Final Approval?
AMELIA Research & Development	1.0	May 21, 2025	Added tickets for 3.12.0 release	Yes

1. Release 3.12.0

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 Deprecation Notice: timestamp format in recurrence rules of scheduled events

Support for Unix timestamp values in the UNTIL field of recurrence rules is now deprecated. Starting from 3.15.0 release, only the RFC 5545 datetime format (e.g., 20250415T140000Z) is supported. This change ensures better compatibility with standard calendar systems and improves interoperability. Please ensure all recurrence rules use the correct datetime format before the deprecation takes full effect.

1.2 Bugs

- **Resolved Dry Run Error in Content Pack Import**. The issue causing a dry run error during the import of a content pack was identified and resolved, allowing all automata within the pack to run correctly without manual intervention. The change is related to the backend processes for importing content packs, and there is no direct change visible in the UI. The purpose of this change was to ensure that content packs can be imported seamlessly without errors, improving the reliability and user experience for administrators managing automata configurations. This change primarily affects the backend system processes and impacts administrators who manage and import content packs. It is not directly customer-facing but improves the systems robustness for administrative users. (AP-30816)

- **Resolve GraphQL Update Error for FlowCodes Exceeding 32 Characters**. The issue resolution addresses the error encountered when a camel flow with a flowCode exceeding 32 characters attempts to update tasks via GraphQL and fails due to data truncation in thesource column of the database. There is no direct change in the user interface; this issue pertains to the backend processes that handle GraphQL update tasks and database interactions. The purpose is to prevent task update failures that occur due to the truncation of data when flowCodes exceed the database column limit, ensuring that camel flows can reliably update tasks regardless of flowCode length. This change is primarily backend and affects developers and service integrators who create camel flows with longer flowCodes. It indirectly benefits end users by ensuring that task updates complete without errors. (AP-30834)

- **Fix implemented for Task Search by Requester when generated via Email/Amelia**. A fix was introduced to ensure that tickets generated via Email/Amelia can now be found when searching by the requesters email address in the radar UI. The change occurred in the task search functionality of the radar UI within the Support instance of the application. The purpose of this change was to address the issue where tickets created via Email/Amelia could not be located using the requesters name or email, thus improving the search accuracy and user experience. This change is customer-facing as it directly impacts users of the Support instance who are utilizing the radar UIs search functionality. (AP-30845)

- **Resolved jumbled characters in PowerShell 7 output formatting**. The output formatting in PowerShell 7, which previously resulted in jumbled characters during automated execution, has been adjusted to provide clearer and more consistent text output. This issue pertained to the backend output generated by PowerShell 7 applications and does not directly affect any user interface elements. The change aims to address the clients concern regarding the jumbled character output when running host commands in PowerShell 7. The output needed to be simplified to prevent automation scripts from failing or returning unclear data, thus improving reliability and usability. The change primarily affects backend operations, particularly for users and scripts that interact with PowerShell 7 to automate tasks. It ensures that the output is uniform and does not disrupt automated processes. (AP-30863)

- **Fix for Unintended Deletion of Calendar Events on Update All Action**. A bug was fixed that prevented the unintended deletion of past calendar events when the Update All option was selected after modifying a scheduled event in the IPCal configuration. The change affects the IPCal interface where users schedule and edit recurring calendar events. The purpose of this change was to correct a bug that caused all past scheduled events to be deleted without warning when editing the owner field of a future event and selecting All to apply changes. This change is backend-related but impacts users managing schedules in the IPCal system. Users experienced data loss when modifying recurring events using the Edit All Events option. (AP-30871)

- **Fix Redis Removal for Disconnected ALite Entries**. The logic in the Unregister Lua script was updated to ensure that a disconnected ALite entry is removed from the Redis ALite registry. There was no direct change in the UI; the change was backend-related and affected API responses. The change was implemented to ensure the accuracy of the ALite status API by removing entries for ALites that are no longer connected, which prevents outdated or misleading information from being presented to users. This change primarily affects backend operations, specifically the API responses provided to developers or systems interfacing with the ALite status endpoint. Indirectly, it also benefits end-users or services relying on the accurate status of ALite connections. (AP-30872)

- **Fixing Unintended Deletion of Scheduled Events When Changing Event Owner**. A bug was fixed that prevented the unintended deletion of events when the owner of scheduled events was reassigned or removed. The system now correctly handles the reassignment and removal of event owners without affecting other scheduled events. The change pertains to the backend logic involved in the calendar event management process. No direct UI component was updated, but users will experience a smoother process when managing ownership of scheduled events through the calendar interface. The purpose of this change was to correct a critical issue where modifying the owner of a scheduled event unintentionally resulted in the deletion of another event. This change ensures data integrity and provides a more reliable scheduling experience for users. This change primarily affects backend processes related to event scheduling and ownership management. However, it is customer-facing in terms of improving the user experience for those assigning or reassigning events within the calendar feature. (AP-30877)

- **Fix Improper Default Task End Date to 1.Jan 1970 in IPcal Editing**. The improper default end date of 1st January 1970 that appeared when editing tasks in IPcal has been corrected. This change ensures proper date assignment and reporting functionality. The change happened in the task editing interface for the IPcal component on the support.amelia.com platform. The purpose of this change was to fix the incorrect default end date of January 1, 1970, that affected task management and reporting. By addressing this issue, tasks will now have accurate end dates, preventing errors in backup reports and improving the user experience. This was a customer-facing change as it directly impacted users managing and editing tasks through the IPcal scheduling interface. (AP-30904)

- **Fixed NullPointerException in ServiceNow Incident State Mapping**. The issue causing a NullPointerException during the state mapping process in the ServiceNow integration has been resolved. The integration should now correctly handle cases where not all states are mapped, and it will no longer throw exceptions in such scenarios. The change affects the integration backend responsible for ServiceNow incident synchronization. There are no direct UI changes as this is a backend fix. The purpose of this change was to fix a bug where a NullPointerException was thrown when trying to map a state for which no corresponding ServiceNow status was configured. This ensures that the system does not create exceptions in logs, maintaining system integrity and improving error handling. The change affects the backend of the integration between ServiceNow and the Autonomics platform. It is not directly customer-facing but improves the stability of the system for users who rely on the ServiceNow integration. (AP-30919)

- **Resolved Issue of Duplicate Task Creation When Updating Existing Tasks via Workflow**. A bug was fixed that previously caused a new task with the same name to be erroneously created in the radar when updating an existing task through the workflow process. The change affects the task management section of the Autonomics platform, specifically within the workflow-related task processing fields where task updates are handled. The change was implemented to eliminate the unintentional creation of duplicate tasks during workflow updates, thereby optimizing task management efficiency and improving overall system function. This change primarily affects the backend task management processes, although it indirectly improves the user experience for customers interacting with tasks within workflows. (AP-30939)

- **Ability to Add Duplicate Names in Requester Filter**. The requester filter now allows users to add the same requester name multiple times. The change occurred within the requester filter section of the application. This change was implemented to provide users with more flexibility in setting up their filters, allowing for scenarios where the same requester name might need to be duplicated for specific use cases. This change is customer-facing, impacting users who utilize the requester filter functionality. (AP-30941)

- **Resolved Issue: Black Right Panel Appearing on Double-Clicking Comment Box**. The issue where a black right panel was displayed when a user double-clicked on the comment box has been fixed to prevent the unwanted appearance of the panel. The change affects the comment box interaction in the applications user interface, specifically handling user input actions. The purpose of this change was to address a visual bug that could distract or confuse users, ensuring a smoother and more intuitive user experience. This is a customer-facing change, impacting users interacting with the comment box interface in the application. (AP-30942)

- **Post-Upgrade Workflow/Approvals Issue in Autonomics Core**. The resolution and approval workflows for change tasks in the Autonomics Core system are not functioning properly after an upgrade from version 3.9.1 to 3.10.0. Users are unable to change the workflow status to approved or pending, necessitating the use of Force Resolve. The issue is occurring in the UI of the Autonomics Core platform, specifically within the workflow management feature of change tasks. The purpose of investigating this change is to address the malfunctioning workflow and approval processes that emerged after the platform upgrade, ensuring that users can modify the status of change tasks without resorting to Force Resolve. This change affects backend operations concerning the workflow feature, but due to its impact on users ability to modify tasks, it has both backend and customer-facing implications. (AP-30946)

- **Reduce Excessive Logging for Missing Client ID in TaskExecutorV2**. The code was modified to suppress excessive logging messages regarding the missing client ID (via x-correlation-clientId) when invoking methods in TaskExecutorV2. This was achieved by ensuring all tasks executed with CompletableFuture in TaskExecutorV2 are wrapped with runWithContext. The change does not affect the UI, as it pertains to backend logging processes. The purpose of the change was to reduce the amount of unnecessary warning logs generated during the execution of certain methods in TaskExecutorV2, specifically preventing logs from appearing when a client ID is not required for data persistence tasks in Cassandra. The change affects backend systems and developers, improving log clarity and reducing noise in backend operations without any direct impact on customers or end-users. (AP-30960)

- **Added missing module name on the Automata Designer page UI**. The module name, which was previously missing, is now visible on the Automata Designer page. The change was applied to the Automata Designer page within the user interface where the module name should be displayed. The purpose of this change was to ensure that users have comprehensive information available on the Automata Designer page, improving navigation and usability. This change was customer-facing, affecting users who interact with the Automata Designer page UI. (AP-30968)

- **Workflow Button Visibility Issue Corrected in IPradar Component**. The visibility issue where the Workflow button appeared partially off-screen with only a red shadow visible was corrected. Users can now see and interact with the Workflow button fully without needing to employ any workaround. The change occurred in the IPradar component interface of the Autonomics application. The purpose of this change was to correct a UI defect where the Workflow button was not fully visible or clickable, which hindered users from performing necessary actions within their workflow efficiently. This change was customer-facing, as it directly impacted the end-users ability to interact with the Workflow button effectively. (AP-30984)

- **Resolved Tag ID Reference Error in Content Pack Automation Exports Post-Upgrade**. The ability to export content packs containing automation was restored after resolving an issue where outdated references to tag IDs were causing export failures post-upgrade. The changes took effect in the Autonomics > Administration > Content Packs > Configurations interface during the export process. The purpose of the change was to fix an error caused by persistent references to tag IDs, which remained after a system upgrade. This issue led to export failures, necessitating an update to ensure tags are handled correctly and allow the successful export of content packs. This issue was primarily backend-focused, affecting developers and administrators trying to manage content packs, particularly those at Fujitsu utilizing multiple instances (PROD, TEST, GDT). (AP-30988)

- **Issue with Connection Session Persistence in Sub Executions**. The issue of connection sessions not being maintained during the execution of automation processes was identified. Initially, connections closed unexpectedly after executing a sub-automation, leading to reconnections in the main automation. The change involves ensuring that the same connection is reused if the sub-automation executes on the same executioner. The change targets the automation execution processes and is not directly visible in the standard user interface. The purpose of this change was to fix a regression issue caused by the Autonomics 3.11.0 upgrade, impacting the automation workflows. Specifically, it aimed to rectify the connection closure after the transition between sub-automation and main automation to improve reliability and maintain consistent execution sessions. This change primarily affects the backend operations by ensuring stable connection sessions in automation processes. While it indirectly benefits end-users by improving automation reliability, it is mainly a backend-level fix affecting developers and system integrators using the Autonomics platform for automation tasks. (AP-30989)

- **Improved Visual Differentiation between SNOW and Autonomics Classes in the CMDB Integration**. This ticket introduced visual modifications to the user interface that allow SNOW classes to be distinguished from Autonomics classes within the CMDB integration field mapping card. The change occurred in the field mapping card of the CMDB integration section where multiple classes are present in the template. The purpose of this change was to resolve confusion caused by the lack of distinguishable features between SNOW and Autonomics classes, facilitating better user understanding and interaction with the field mapping cards. This change is customer-facing as it directly impacts the user interface that customers interact with in the CMDB integration section. (AP-31033)

- **Enhanced Clarity of Access Denied Error Message for Non-Live Automations**. The error message displayed when attempting to run a non-live automation has been revised to provide clearer and more informative guidance to the user. The change occurred in the error message UI element that appears when a user tries to execute an automation that has not yet been marked as Live. The purpose of this change was to alleviate user confusion by ensuring the access denied message explains why they are seeing it and what steps they need to take to successfully run their automation. This change is customer-facing, impacting any user attempting to execute automations that have not been activated fully. (AP-31038)

- **Inconsistent Main Menu Behavior Between Dark and Light Themes**. The main menus visual behavior was standardized to ensure consistency in both dark and light themes, allowing for clear visibility of menu selections and options. The change occurred in the main menu section of the Autonomics Core UI, where the display of possible and selected menu choices was adjusted for the light theme. The purpose of this change was to improve user experience by ensuring that the menu functionality and visibility are consistent regardless of the selected theme, preventing usability issues in the light theme. This change is customer-facing, impacting users interacting with the Autonomics Core UI who switch between dark and light themes. (AP-31083)

- **Code Promotion Issue: Automata State Values Lost When Transitioning From Dev to UAT**. The issue addressed was that during the code promotion process from the Development environment to the User Acceptance Testing (UAT) environment, the automations Create Task state values were not being retained. The change affects the UI portion where the client properties, specifically the automated task Create Task state values, are supposed to appear. Users noticed the missing settings in the client code dropdown after moving the automation from the Dev environment to the UAT environment. The purpose of this change is to ensure that automation settings configured in the Development environment remain consistent and are transferred correctly to the UAT and subsequently to the Production environment without requiring manual reconfiguration, thus improving efficiency and stability during code promotions. This change primarily affected the backend processes and developers responsible for managing and testing automations, but it indirectly impacts customers who rely on the stability and consistency of automation from configuration to deployment. (AP-31085)

- **Resolved Audit Log Page Loading Issue After Adding ROLE Entity Type**. The issue causing the Audit Log page to fail to load after adding a ROLE entity type has been fixed. The change took place in the Audit Log section of the user interface, correcting the loading issue for that page. The purpose of this change was to resolve the bug that prevented users from accessing the Audit Log page after a specific entity type was added, enhancing user experience and system functionality. This change is customer-facing, as it directly impacts users who interact with the Audit Log page in the application interface. (AP-31107)

- **Fix Import Error for Automation in Content Pack**. The issue causing the failure of importing automation within a Content Pack configuration was identified and resolved. This fix ensures that the automation is correctly included during import operations, thereby eliminating errors during both dry-run and actual import processes. The change affects the import functionality within the Content Pack management interface of the Autonomics application. The purpose of this change was to address a defect where specific automations contained in a Content Pack were not being imported successfully, causing disruptions for users attempting to deploy configurations across different environments. This change is customer-facing, primarily affecting users involved in deploying Content Packs and managing automations within the Autonomics application. (AP-31119)

- **Fix for Default Workflow Loading Issue for Non-Admin Users**. This ticket addresses a bug where default workflows set in Workflow settings were not automatically loading for users without Global Admin authorities. The fix ensures that non-admin users can now see and use the default workflows without needing to manually select them from a dropdown. The change was implemented in the Task view interface within the instance. When creating a new task, the default incident management workflow now automatically appears with all associated workflow fields for non-admin users. The purpose of this change was to streamline the workflow process for non-admin users by automatically loading the default workflows. This reduces the need for manual selection, thereby improving efficiency and reducing the risk of errors. This change affects the customer-facing UI, specifically for users in the instance who do not possess Global Admin authorities. It enhances their experience by ensuring ease of access to default workflows. (AP-31129)

- **Assignment Groups Field Made Non-Editable in V3.11 Upgrade**. The Assignment Groups field was changed from a typeable input to a non-editable field, preventing users from manually entering data. The change occurred on the user interface specifically within the Prod application where the Assignment

Groups field is located. The purpose of this change was likely to standardize data input, ensure data integrity, and prevent errors that can arise from manual inputs by restricting users to select from pre-defined options. This change is customer-facing, as it directly impacts users of the Prod application who interact with the Assignment Groups field. (AP-31130)

- **Modify Opensearch Dashboards to Restrict Elasticsearch Update Authority for Report Downloads**. The OpenSearch Dashboards were modified so that they no longer require users to possess global Elasticsearch Update authority in order to download reports. Now, users with specific client/global module VIEW authorities can download reports based on their access level. The change affects the report downloading functionality within the OpenSearch Dashboards interface, ensuring users can download reports pertinent to their assigned VIEW authorities without needing broader update privileges. The purpose of the change is to enhance data security and access control by ensuring that users can only download reports and view data they are authorized to access, without needing elevated permissions that could expose unnecessary data. This change impacts users of the OpenSearch Dashboards, particularly those who download reports. It is relevant to backend systems where the access control logic is implemented, but its implications are customer-facing as it affects how end-users interact with dashboard data. (AP-31132)

- **Resolved Mismatch Issue in Ticket Status Between Workspace and Reporting**. A discrepancy between the ticket details and their representation in the Workspace and Reporting views was addressed. Mismatching data caused by the tickets CI attributes has been resolved, ensuring full synchronization between systems. The changes impact the Workspace view and Reporting tables within the Autonomics platform, specifically concerning the display and synchronization of ticket information. The purpose of this change was to correct a synchronization issue where ticket status and other details were displayed incorrectly in the Workspace and Reporting views compared to the actual ticket data. These inconsistencies could lead to confusion and impact operational efficiency. This change affects both backend and customer-facing components, as it ensures backend data processing is consistent and correctly displayed to users in the customer-facing Workspace and Reporting interfaces. (AP-31155)

- **Restrict CAB Approval Actions to Authorized Users Only**. This ticket addresses an issue where non-authorized standard users were inadvertently granted the ability to approve CAB actions on change tickets, a task that should be exclusive to designated CAB authority members. The change ensures that only authorized members of the CAB can see and access the approval functionality within the change ticket workflow section of the application UI. The purpose of the change was to rectify a security loophole that allowed non-authorized users to perform high-level approval actions, thereby compromising the integrity of the change management process. Restoring the exclusivity of CAB authorities ensures adherence to predefined roles and responsibilities. This is a backend change but affects customer-facing operations by ensuring that only the designated CAB members have the necessary permissions to approve actions, thereby maintaining the integrity of user roles in the application. (AP-31158)

- **Fix auto-reset of client domain on IPdeploy service restart**. The resolution prevents the automatic resetting of client domains to the string domain in the ipauthorization table whenever the IPdeploy service was restarted. This change does not directly affect the UI as it involves backend database operations. The purpose of this change was to ensure data integrity by preventing unwanted changes to client domain entries within the ipauthorization table after a service restart, which corrected the mismatch with ipportal.client. This change primarily affected the backend operations related to database management of client domains in the ipauthorization table. (AP-31178)

1.3 EPIC

- **Reinstate Independent Autonomics Authentication**. The authentication process for Autonomics has been modified to no longer depend on the Amelia system, reestablishing independent authentication capabilities. The change is primarily a backend modification, therefore it may not directly impact the UI. However, any related user interfaces that display authentication status or prompts might be indirectly affected. The purpose of this change is to remove dependency on the Amelia system for authentication, possibly to enhance system reliability, security, and to improve system architecture. This change primarily affects backend operations and might have some implications for developers and system administrators. It indirectly affects end-users if there are any visible changes to authentication-related interfaces. (AP-30807)

1.4 STORY

- **Update Filename Convention for Exported Content Packs to Ensure Uniqueness**. The filename for exported content packs is now unique for each export by incorporating the export name and the current timestamp into the filename. A new API parameter nameBasedOnTimestamp was introduced to enable this behavior without affecting existing automations. There is no direct UI component impacted by this change, as it primarily pertains to the download functionality via the API. However, any interface that facilitates content pack exports could indirectly reflect this change by showing the updated filename format. The purpose of this change is to prevent filename conflicts and improve file management by ensuring each exported content pack has a unique filename, thus avoiding overwriting files with the same default name. This change primarily affects backend processes and integrations, especially those utilizing the content pack export API. Its a hidden change for end-users but impacts developers and systems engineers who handle content pack exports and automation tasks. (AP-27391)

- **Enhanced HTML Rendering for ServiceNow Knowledge Articles in SoundHound Autonomics**. This ticket introduces enhanced processing and rendering of HTML content within ServiceNow Knowledge Articles. It allows a broader range of safe HTML elements to be used while stripping out potentially dangerous elements like <script>, thus increasing the flexibility and aesthetic appeal of the content while maintaining stringent security standards. The changes apply to the backend processing of HTML content originating from ServiceNow Knowledge Articles, affecting how content is rendered when viewed within the SoundHound Autonomics interface. The purpose of this change is to provide users with the ability to display richer and more visually appealing content by utilizing a wider variety of HTML elements, without compromising on security. This aims to balance content rendering flexibility with the need to prevent security risks like cross-site scripting (XSS). The change affects the backend processing of HTML content, primarily impacting developers and administrators configuring integrations with ServiceNow. It indirectly affects users who view Knowledge Articles, as they will see the enhanced rendering in the content displayed to them. (AP-29874, AP-30229)

- **Introduction of Rich-Text Editor for Task Comments**. The task comments section now supports rich-text formatting, allowing users to create comments with structured elements such as bold, italic, code blocks, lists, and hyperlinks. The change took place in the Task Comments section, where a new rich-text editor equipped with a formatting toolbar is introduced to enhance the commenting experience. The purpose of this change is to enable users to create more expressive, structured, and visually organized comments. This feature is especially beneficial for providing detailed feedback, sharing code snippets, or organizing conversations related to tasks effectively. This change is customer-facing, affecting users who interact with the Tasks component, allowing them to use enhanced formatting options in their comments. (AP-30103)

- **Integration of Role-Based Access Control (RBAC) for Enhanced Access Management**. The integration of Role-Based Access Control (RBAC) has been added to the Autonomics platform, which allows administrators to define user roles and manage permissions more precisely and flexibly. The changes are reflected in the user profiles and settings, where users can view their roles and permissions. Administrators can create, assign, modify, and generate reports on roles through the administrative interface. The purpose of this change is to enhance security protocols and simplify user access management by providing a standalone access management solution, removing dependency on the Amelia Conversational AI platform, and ensuring appropriate access is granted based on user responsibilities. This change affects both the backend systems, due to changes in how access controls are managed, and is customer-facing, as it alters how users and administrators interact with and manage access within the platform. (AP-30192, AP-30880)

- **Integration of SAML2 Authentication and Role-Based Access Control**. This ticket introduced the capability for users to authenticate using SAML2, allowing for integration with external identity providers. It also implemented a role-based access control (RBAC) system that automates the assignment of roles and permissions based on SAML2 attributes and group memberships. The change is primarily located in the platforms settings where administrators can enable SAML2, configure identity provider metadata, and set role-mapping configurations. There may also be a UI component for managing user session behaviors in accordance with platform security policies. The purpose of this change is to streamline and enhance the platforms authentication process by integrating SAML2 support, which allows for secure user access through external identity providers. The implementation of RBAC further automates and personalizes role assignment, increasing security and the scalability of access management. This change primarily affects the backend components, as it involves authentication processes and role management. However, administrators and end-users will also experience changes as they will interact with the configuration and authentication mechanisms, making it partly customer-facing. (AP-30193, AP-30981)

- **Update Label and Icon for Disabled Integrations on Integration List Page**. The status label for disabled integrations on the Integration List page was updated from Unknown to Disabled. Additionally, the question mark icon used for these integrations has been replaced with a new icon that better represents the Disabled state. The change occurred on the Integration List page, where users can view the list of integrations and their corresponding statuses. The purpose of this change was to eliminate confusion among users by clearly indicating that certain integrations are intentionally disabled, rather than being in an unknown state. This improves the user experience by providing more accurate and informative status labeling. This change is customer-facing, affecting users who interact with the Integration List page within the application. (AP-30238)

- **Enhancements to Static Rule Configuration in Eventflow**. The ticket introduced two key changes: the removal of the State option from the Create Static Rule dropdown under Rules, as the metric lacks the state property, and the requirement for a Value matcher for Trigger rules, with an error message introduced for when it is not provided. The change occurred in the Create Static Rule interface, specifically affecting the Rules dropdown and the rule creation process for Trigger rules. The purpose of these changes was to streamline the rule creation process by removing irrelevant options and ensuring that rules are logically complete before they can be saved. Removing the State option prevents confusion, and mandating a Value matcher for Trigger rules ensures that only sensible rules are created. This change primarily affected users interacting with the Eventflow UI, thus it is customer-facing. (AP-30384, AP-30805)

- **Integration of LDAP Authentication in Autonomics**. LDAP (Lightweight Directory Access Protocol) support has been integrated into Autonomics, enabling organisations to authenticate users against existing LDAP directories. This implementation allows for centralised authentication, synchronisation of user attributes, and dynamic role assignments based on LDAP group memberships. The change appears in the platforms settings where administrators can configure LDAP server details, attribute mappings, role assignments, and test LDAP configurations. The purpose of this change is to improve security and efficiency by allowing users to authenticate through their existing LDAP directories, ensuring secure and centralised authentication. This adherence supports scalability, dynamic role management, and compliance with enterprise security standards. This change primarily affects the backend systems but is customer-facing as it involves how admins configure authentication settings and how users log in using LDAP credentials. (AP-30384, AP-30805)

- **Platform: Implementation and Management of Customizable Themes in Autonomics**. The introduction of theme management in Autonomics now allows users to create, modify, and delete custom themes. Users can personalize their applications by selecting logos, configuring color schemes, and determining whether to use gradient backgrounds. It also enables automatic switching between Light and Dark themes based on system settings. These changes are reflected in the theme settings section of the application interface, where users can manage their themes, including adding, updating, and removing custom themes. The purpose of this change is to enhance user experience and allow for greater customization and personalization, aligning application interfaces with user preferences or corporate branding requirements. This increases user engagement and provides visual consistency across the user interface. This change is primarily customer-facing, affecting admins and end-users who interact with the applications user interface to manage and apply themes. (AP-30384, AP-30805)

- **Introduction of Virtual Hosts for Enhanced Client Personalization and Scalability**. The implementation of virtual hosts was introduced, allowing custom Full Qualified Domain Names (FQDNs) for clients to enhance personalization and scalability. This change facilitates unique configurations for themes, authentication systems, and default landing pages. The change affects the administrative interface where admins can link custom FQDNs, assign themes, configure authentication systems, and set default landing pages for each virtual host. The purpose of this change is to support client personalization and scalability by enabling tailored experiences through custom domains, themes, and configurations, while also removing dependencies on Amelia. This change primarily affects backend configurations managed by admins, although it provides a customer-facing impact by offering personalized and branded user experiences. (AP-30644, AP-30966)

- **Implement Resolution Action Dropdown in Zabbix Event Integration to Manage Problem Closure**. A new feature was added to the Zabbix Event integration, introducing a dropdown parameter called Resolution action. This allows users to choose between closing a problem or unacknowledging a Zabbix problem when a task is force-resolved. The change occurred in the Zabbix Event integration settings within the UI of the system, where a dropdown menu was introduced to manage resolution actions. The purpose of this change is to offer more flexible problem management in Zabbix when resolving tasks. Particularly, it addresses issues with manually closing Zabbix problems by allowing the system to simply unacknowledge them instead, ensuring that problems can be accurately tracked and new related tasks can be created if necessary. This change affects both the backend and customer-facing aspects of the system as it involves backend logic to manage Zabbix problems and customer-facing UI elements allowing users to select their desired resolution action. (AP-30667)

- **Implementation of a Dedicated and Customizable Login Page for SoundHound Autonomics**. A dedicated login page has been implemented for the SoundHound Autonomics application, removing the dependency on SoundHound Amelia for authentication. This change introduces multiple authentication methods, enhances security features, allows for customization with company branding, and provides a user-friendly interface for password management and support access. The change was made on the login interface of the SoundHound Autonomics application, where a new, standalone login page has been introduced. The purpose of this change is to enhance security, improve user experience, promote system independence, and offer flexible authentication options. It aims to address user needs for ease of access, customization, and support, while ensuring a robust authentication framework. This change is customer-facing, impacting all users who access the SoundHound Autonomics application by logging in, including those managing their login preferences or requiring support. (AP-30808)

- **Improved Focus Retention Across Automation Versions in Automation Designer**. The change ensures that the users selected component in the Automation Designer remains in focus when switching between different versions, enhancing navigation and productivity. The change occurred within the Automation Designer interface, specifically concerning the component selection when toggling between automation versions. The purpose of this change was to prevent the loss of selection focus when moving between automation versions, addressing user frustrations related to inefficiencies and interruptions in workflow, thereby improving user experience and productivity. This is a customer-facing change, directly impacting users interacting with the Automation Designer in the UI. (AP-30827)

- **Enhance SoundHound Autonomics with Support for Uninitialized and Null Variables**. This ticket introduced the ability for users to create and manage uninitialised, null, and empty variables within the SoundHound Autonomics application, providing more flexibility in automation scenarios. The change involved adding a Variable Type dropdown to the user interface, allowing users to select and define the state of variables (uninitialized, null, empty). The change allows users to improve workflow automation by giving more control over variable states, thus not requiring all variables to have initial values. This enhances usability and adaptability in various automation scenarios where initialization needs to be deferred or left empty initially. This change is customer-facing as it directly impacts users interacting with the Autonomics application to define and manage workflow variables. (AP-30829, AP-30972)

- **Removal of Obsolete AMELIA Menu and Icon from SoundHound AI Autonomics Application**. The AMELIA-specific icon and related menu with links to three unnecessary components have been removed from the top row of the SoundHound AI Autonomics application. The change occurred in the top row of the SoundHound AI Autonomics applications user interface, where the AMELIA menu and icon were previously located. The purpose of this change was to streamline the user interface by removing outdated and unnecessary AMELIA-specific components, improving the user experience. This change is customer-facing as it affects users interacting with the SoundHound AI Autonomics applications user interface. (AP-30933)

- **Integration of Login Attempt Details into Audit Logs for All Authentication Methods**. Details of login attempts, whether successful or unsuccessful, including specifics such as email, attempt type (e.g., success, failure, locked, or wrong password), and external IP addresses, are now recorded in the audit log. This applies to logins via LDAP, SAML, and internal methods. There is no direct change in the UI for end-users; however, for administrative users, the audit logs now capture these additional authentication details. The primary purpose of this change is to enhance security by ensuring that all login attempts are auditable, thus providing better tracking for security incidents and improving the ability to identify unauthorized access attempts. This change primarily affects the backend processes and will be of particular interest to system administrators and security personnel who utilize the audit logs for monitoring and security analysis. It is not directly customer-facing in terms of the user interface. (AP-30959)

- **Implement Wildcard Support for ISC Fallback Flows Automation**. Wildcard support, represented by {{*}}, was added to ISC Fallback Flows, allowing all flows to be deployed automatically in Amelia. There was no specific UI change for this feature as it is a backend enhancement within the ISC Fallback Flows automation setting. The purpose of this change was to streamline and simplify the deployment process by enabling the use of a wildcard to automatically deploy all relevant flows in Amelia, rather than specifying each individually. This change primarily affects backend processes and integrations. (AP-30975)

- **Implement Rich-Text Editor for New and Edit Task Actions**. A rich-text editor was introduced for the New Task and Edit Task actions, allowing users to format task notes with options such as bold, italic, lists, headings, links, and code snippets. This brings the task actions in line with the existing rich-text capabilities for Task Comments. The change occurred in the task creation and editing interfaces, specifically in the note fields for New Task and Edit Task actions. These areas now support rich-text formatting. The purpose of this change is to improve the clarity and readability of task notes by allowing users to apply rich-text formatting. This enhancement ensures a seamless and consistent editing experience between task comments and task notes. This change is customer-facing and affects users who create or edit tasks within the application. No backend changes were necessary for this feature. (AP-31128)

- **Expand Note Field in Task Modals for Better Usability**. The task note field in the Create and Edit Task modals has been expanded to allow line entries of up to 80 characters without forced line breaks, enhancing readability and usability. The change occurred in the note input field within the New Task and Edit Task modal views of the Task Management application in IPradar. The purpose of this change was to modernize the user experience by aligning the note input capabilities with contemporary productivity tools, thus allowing for more natural and readable note-taking without awkward line breaks. This change is customer-facing, affecting users who interact with the task creation and editing modals within the Task Management application.(AP-31164)

- **Implement Enabled Property and API Enhancements for Auth Systems**. A newenabled property was introduced in the authentication system to track active authentication methods. This required a new database column and was set to true by default. The system now uses AuthSystem.isEnabled() instead of previously used methods and includes a filter in the AuthSystemApi.getAuthSystems() API. Additionally, only enabled systems are returned for user login API calls, and a new API to get an authentication system by code was introduced. The changes primarily impacted the backend API. There are no direct UI changes as the modifications are related to how authentication systems are managed and filtered in API responses. The change was made to streamline the authentication management process by enabling filtering and management of active versus inactive authentication methods. This ensures that only active and valid authentication systems are utilized during user login processes, enhancing system efficiency and security. This change affected backend systems and processes. It is not customer-facing, but it influences how authentication data is managed and retrieved in backend operations. (AP-31167)

- **Enhanced Visual Indicators for Authentication Systems in List View**. The authentication systems list view in the Administration Settings has been updated to include new visual indicators. A new Enabled column now displays Yes or No to indicate if each authentication system is active, and distinct icons have been added next to each type of authentication system for easier identification. The changes were made in the Authentication Systems list view within the Administration Settings. Specifically, a new Enabled column was added, and icons are now displayed in the Type column. The purpose of this change is to improve usability and consistency in the user interface by providing clearer visual indicators. This allows users to quickly identify the status and type of each authentication system without needing to delve into additional details, aligning the experience with the existing Integration list view. This change is customer-facing, impacting users who interact with the Administration Settings to manage authentication systems. (AP-31192)

1.5 Tasks

- **Remove Unused System Variables in IPworkflow**. Unused system variables, including IS_CONNECTABLE_CHECK_RESULT, LAST_MONITOR_STATE, and IS_AUTOMATABLE_CHECK_RESULT, were removed from the IPworkflow backend system, with new implementations planned for dynamic resolution. This change did not affect the user interface; it occurred in the backend system variables. The purpose of this change was to clean up the codebase by removing redundant system variables that were not in use and to address technical debt. Dynamic resolution methods will replace these where necessary. This change affects the backend infrastructure and internal workflows without direct impact on end-users or customer-facing systems. (AP-25688)

- **Remove synchronous trigger execution mode; enforce asynchronous execution in IPautomata**. The trigger execution async property flag was removed, permanently enforcing asynchronous execution for IPautomata trigger events. This change does not directly affect the UI as it involves backend configuration concerning trigger execution modes. The synchronous execution mode was initially retained as a fallback in case of issues with asynchronous execution. However, the asynchronous mode has been stable and reliable for three years, rendering the synchronous option obsolete. Removing it simplifies configuration and reduces technical debt. This change affects the backend systems and developers who previously managed or configured the synchronous execution option. It is not directly customer-facing. (AP-27711)

- **Enhance AIF Api block to utilize Native Java Integration when applicable**. The AIF Api block has been modified to attempt executing the integration using Native Java Integration, if applicable. If the integration cannot be handled by Native Java Integration, the system will revert to the current implementation using the Orchestrator. The change does not directly affect the UI, as it involves backend modifications to the integration execution process for the *AIF Api* block. The purpose of this change is to streamline the process by automatically utilizing Native Java Integration, which can enhance performance and reduce dependency on the Orchestrator when handling integrations, thus improving efficiency and reducing potential overhead. This change primarily affects the backend processes, as it modifies the way integrations are executed behind the scenes. There are no direct customer-facing changes. (AP-30850)

- **Enhance UI with Explanatory Hints for Client Properties**. Hints and explanations were added to specific elements in the client form to clarify their purpose and function, reducing user confusion. Changes were made to the client form, including the Knowledge Engine search threshold, rate limiting features, and reporting retention policies. The purpose of this change was to provide clear and direct explanations for complex properties, ensuring users better understand how to utilize these features and what values represent. This change is customer-facing, specifically impacting users who interact with the client form on the UI to configure and understand client properties. (AP-30852)

- **Default Automation Validation Disabled in Content Pack Export**. The default setting for Do not validate exported Automations in the Content Pack export configuration is now set to Yes. This change is reflected in the Content Pack export configuration interface. The purpose of this change is to prevent export failures by allowing warnings to be printed instead, due to the introduction of client scoped users to run automations. This is a customer-facing change affecting users who export Content Packs. (AP-30898)

- **Implement Backend Control for Credential Access through Instance-Level Setting**. A new instance-level setting was introduced to control the reading of credentials via API calls. This setting, when enabled, restricts credential access to internal calls only, enhancing security by preventing external API access to passwords. There is no direct UI change; the change impacts how API calls are managed in terms of reading credentials. It extends existing frontend controls to the backend. The purpose of this change is to enhance security by ensuring that passwords and sensitive credentials cannot be accessed through public APIs. By enforcing credential access restrictions at the backend level, the system aims to prevent unauthorized access to sensitive data. This change primarily affects the backend system, although it has indirect implications for customer-facing aspects by ensuring better protection of their credentials. It is chiefly of interest to developers and administrators managing the applications security settings. (AP-30958)

- **Optimize Workflow Activity Publishing to Prevent Message Loss and Improve Performance.** The workflow activity publishing mechanism was optimized to reduce the number of unnecessary activities being published. This helps in preventing message loss due to Redis stream trimming and enhances overall performance by ensuring that only relevant messages reach the listeners. This change does not affect the UI directly as it pertains to backend processes and system optimizations. The primary reason for this change was to address the issue where high-frequency radar tasks caused automations to miss some tasks. These unnecessary workflow activities were causing message loss due to the default maximum length of Redis streams being reached (10000). This change affects the backend system. It is not customer-facing but enhances the efficiency of backend processes by reducing unnecessary operations and preventing message loss. (AP-30992)

- **Enable Zero Input for Number Fields in UI**. The change allows users to input the number 0 in number-type input fields within the UI. The change was implemented in input fields across the user interface where the input type is set to number. The purpose of this change was to address the limitation preventing users from entering 0 in number-type fields, enhancing data entry flexibility and accuracy. This change affects the customer-facing side of the application, enhancing usability for end-users interacting with the UI. (AP-31062)

- **Update to Audit Log: New Authentication Log Action Types and Note Field Correction**. Two new action types were added to the authentication log: AUTHENTICATION_SUCCESS and AUTHENTICATION_FAILURE. Additionally, the note field in the AuditLogDetails type was corrected to match the APIs AuditLog object field, ensuring the reason for authentication failure is displayed correctly. The change affected the backend UI component that displays audit log details. The correction ensures that thenote field, which contains reasons for authentication failures, is visible in the UI. The purpose of the change was to enhance the audit log by adding specific actions related to authentication outcomes and correcting a discrepancy in the field naming to improve data visibility and debugging capabilities. This change primarily affected the backend systems but has customer-facing implications by improving the accuracy and detail of audit logs displayed to users. (AP-31137)

- **Inclusion of Remote IP in HAProxy-Web Access Logs**. The HAProxy-web configuration has been updated to capture theX-Forwarded-For header, which logs the remote IP of incoming requests. This change is not applicable to the UI as it involves backend configuration. The purpose of this change is to enhance logging by capturing remote IP addresses, which can be useful for security audits and monitoring incoming traffic. This change affects the backend operations, primarily benefiting the DevOps and security teams by providing them with more detailed access logs. (AP-31147)

- **Update Request Matchers to List Authenticated URLs Only**. This ticket changed the way URLs are listed in the request matchers by specifying only the major URLs that require authentication and are accessed frequently, rather than listing unauthenticated URLs. This change does not affect the UI directly as it involves backend configuration related to request matchers. The purpose of this change was to avoid security issues and confusion caused by unauthorized internal accesses. By listing only the authenticated URLs, the system enhances security and ensures that only necessary URLs that require user authentication are exposed. This change affects the backend configuration. However, it indirectly improves the security of customer-facing services by ensuring proper authorization mechanisms are in place. (AP-31182)

- **Enhancements to Auth System API and Entity Structure**. The auth system API was updated to include a new filter mechanism based on the HTTP origin, SAML system immediate authorization handling, and an added parameter for filtered system return. Additionally, modifications were made to the Auth System entity, including the introduction of a new boolean field, renaming types, and adding created/updated metadata fields. These changes are backend-centric and happen within the API layer as well as the database structure for the auth system management. There is no direct user interface component affected since the adjustments relate to API functionality and database schema. The purpose of these changes is to improve the flexibility and clarity of the auth system selection process by using logical filters and renaming conventions, as well as enhancing system management with explicit metadata fields. Moreover, returning only the relevant systems ensures efficient authentication processing. This change affects the backend systems and developers who interact with the auth-system API and database. It has indirect implications for end-users by ensuring optimized authentication processes but does not have direct customer-facing UI changes. (AP-31195, AP-31196)

1.6 SUB-TASKS

None in this release.