AMELIA

AI Ops/Alite

AMELIA's Autonomic IT Management Platform

Release Notes 3.5.0

(Document Version 1.0)

Table of Contents

Document History

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

1. Release 3.5.0

This section briefly lists changes to AIOps for this release.

1.1 Release Highlights

None with this release.

1.2 Bugs

- [AP-29835] - The issue of exposing secured variable values in validation error messages has been resolved, ensuring that such values are no longer displayed. This change impacts the validation error messages in the Automations module, specifically within the Orchestrator and IPautomata interfaces. The purpose was to enhance security by preventing the unintended exposure of sensitive information, which could have been visible in error messages. While the change primarily affects the backend, it helps secure sensitive data across customer-facing interfaces.
- [AP-29703] - The issue with eligibility verification for ALite instances during execution has been fixed by correctly invoking the StandaloneIPautomataExecutionCache#isRunning method to ensure consistent eligibility checks throughout execution. This method has been moved to TaskExecutorV2, utilizing its own thread pool to prevent potential deadlocks. The change does not affect any user interface components, as it pertains solely to backend execution processes. It was initiated to resolve an inadvertent alteration during the refactoring of TaskExecutor, which caused eligibility checks to fail and posed a risk of deadlocking the system. While this change primarily impacts backend processes related to ALite instances, it enhances overall system stability and performance without affecting customers directly.
- [AP-29698] - Garbage collection in IPautomataLite has been optimized to efficiently free up memory after running multiple automations, addressing the issue of rising memory usage. This change is not directly visible in the user interface, as it involves backend processes. The primary purpose was to resolve a performance issue where the system did not release memory after completing automation tasks, which could lead to inefficient usage and potential slowdowns or crashes. While this change mainly impacts backend operations, it ultimately enhances system performance, benefiting end-users and administrators running automation tasks on IPautomataLite.

1.3 EPIC

None in this release.

1.4 Story

None in this release.

1.5 TASK

- [AP-29909] - The com.google.protobuf:protobuf-java library was upgraded from version 3.24.4 to 3.25.5 to address the critical security vulnerability CVE-2024-7254. This change does not directly impact the user interface, as it pertains to backend library dependencies. The main purpose is to mitigate the identified security risk, ensuring the system's security and preventing potential exploits linked to the outdated library. This change is backend-focused and does not affect the customer-facing UI, enhancing the security of backend processes utilizing the protobuf-java library.
- [AP-29909] - The com.google.protobuf:protobuf-java library was upgraded from version 3.24.4 to 3.25.5 to address the critical security vulnerability CVE-2024-7254. This change does not affect the user interface, as it pertains solely to backend library dependencies, ensuring that backend processes remain secure and free from potential exploits associated with the outdated library.