Autonomics / Alite

AMELIA's Autonomic IT Management Platform

Release Notes 3.13.0

(Document Version 1.0)

Table of Contents

Document History

Author	Version	Date	Comments	Final Approval?
AMELIA Research & Development	1.0	June 4, 2025	Added tickets for 3.13.0 release notes	Yes

1. Release 3.13.0

This section briefly lists changes to Autonomics ALite for this release.

1.1 Release Highlights

1.1.1 MID-server Endpoint Proxy Support for Events and Metrics

ALite has been updated to function as an Integration Endpoint Proxy. As a result, it now starts a web server that listens on port 8443 by default. This can be changed using the following property:

```
server.port=8443
```

By default, a self-signed certificate for localhost is used. However, it is recommended to configure a valid certificate instead. The relevant properties are:

```
server.ssl.key-store=/full/path/to/file
server.ssl.key-store-password=
server.ssl.key-alias=
server.ssl.key-store-type=
```

1.1.2 HashiVault Certificate Authentication

HashiVault authentication using client certificates has been introduced. Certificates can be stored either in Locksmith or on the ALite file system.

To use certificates stored in Locksmith, define the **HashiVault Certificate Locksmith Element** on the connection and point it to the corresponding Locksmith entry.

To use certificates stored on the ALite file system, configure the following absolute paths on the connection:

- **HashiCorp Vault TLS Certificate Path** (required)
- **HashiCorp Vault TLS Private Key Path** (required)
- **HashiCorp Vault CA Certificate Path** (optional if the server uses a certificate signed by a CA that is already trusted by system’s trust store)

1.2 Bugs

- **Fix for JDBC Driver Class Loading Error in Automata Execution.** The issue with the JDBC driver class not being loaded, resulting in execution failures for SQL, MySQL, and PostgreSQL jobs in Automata, has been resolved. This change ensures that JDBC driver classes are correctly identified and loaded during the execution of automatic jobs. There was no direct change in the UI, as this fix pertains to backend operations involving the execution of automatic jobs using JDBC connections. The purpose of this change was to rectify a connectivity issue caused by the failure to load the JDBC driver classes. This was essential to allow successful execution of automation jobs that interact with SQL databases, thus restoring the normal operation of these processes. This change primarily impacted the backend, specifically affecting developers and system administrators who rely on Automata for executing database-related jobs. It indirectly benefits end users who depend on these backend processes. (AP-31217)

1.3 EPIC

None in this release.

1.4 STORY

- **MID-server Webhook Proxy Support for Secure Event and Performance Metric Integration.** Support for webhook endpoints is extended to use the MID-server to enable event and performance metric data transmission, ensuring adherence to compliance and security requirements for customers that restrict infrastructure exposure. This change does not reflect directly in the end-user interface but affects how webhooks interact with the MID-server for backend processing, allowing users to configure and manage webhooks through the existing MID-server setup. The purpose of this change is to allow customers with stringent security and network policies to send event and performance metric data securely through a MID-server instead of directly exposing platform endpoints. This enables compliance with security standards while ensuring seamless data integration. This change primarily affects the backend, specifically targeting customers who need secure data routing options via the MID-server for event and performance metric ingestion, without exposing their infrastructure externally. (AP-31066)

- **Add Certificate-Based Authentication for HashiVault Integration in Automations Lite.** Support for certificate-based authentication has been introduced for HashiVault integrations within Automations Lite. This enhancement allows for the use of client TLS certificates for secure authentication, complementing existing credentials-based methods. The changes are manifested in the configuration settings related to authentication methods within Automations Lite. Users can now choose and configure certificate-based authentication as an option for HashiVault integrations. The purpose of this change is to provide a more secure, certificate-based authentication method for environments integrating HashiVault with Automations Lite. This enhancement caters to users requiring robust identity verification to ensure the integrity and security of their credentials. This change affects both backend processes and customer-facing configurations, as it involves backend authentication mechanisms and provides an additional option for end-users administrating authentication settings in Automations Lite. (AP-30469)

1.5 TASKS

- **Security Vulnerabilities Remediation through Library Upgrades**. The affected libraries, org.apache.httpcomponents.client5:httpclient5 and org.apache.tomcat.embed:tomcat-embed-core, were upgraded to newer versions, 5.4.3 and 10.1.40 respectively. This action mitigated several known security vulnerabilities (CVE-2025-27820, CVE-2025-24813, CVE-2024-50379, CVE-2024-56337, CVE-2025-31651, CVE-2025-31650). This change does not directly reflect in the UI, as it impacts the backend libraries of the application. The primary purpose of this change was to address and remediate critical security vulnerabilities identified in the specified packages, thereby enhancing the security posture of the backend system. This change primarily impacted the backend infrastructure of the application. It indirectly benefits end-users by ensuring a more secure and robust service environment but is not directly customer-facing. (AP-31185)