PROXEDO

API SECURITY

Proxedo API Security

Release notes for PAS 4.7.0

2023-10-19

The following new features, bug fixes and improvements have been completed for Release 4.7.0 Proxedo API Security.

Features

- **Backend Response Time selector**
  PAS now supports a selector that emits the time elapsed between sending the request to the backend and receiving the response. Combined with the insight functionality, this allows the administrator to monitor the performance of backend servers by measuring the response time and allows them to deploy countermeasures if the response time rises unexpectedly.
- **TLS Support in Elastic Insight Targets**
  PAS now supports TLS in *Elastic* type *Insight Targets*, which enables the administrator to ensure the integrity and confidentiality of the communication between PAS and their Elastic server(s).

Bug Fixes

- **High Availability Director does not remove service IP in certain cases**
  In certain edge cases PAS in a high availability setup has not removed the service address from the passive node, which resulted in service disruption. This has been corrected.
- **Incorrectly required client authentication in Syslog TLS**
  When configuring a *Syslog TLS* in a *Syslog* type *Insight Target* PAS incorrectly required the user to set the *Enable Client TLS Authentication* option to True. This has been corrected.
- **Miscellaneous fixes**
  - Several UI labels have been changed to be correctly capitalized.
  - *Flow Director* has emitted a traceback on invalid license usage beside the log message that indicates the fatal error. This has been corrected.
  - The *URLs* configuration element of *Services / Endpoint* has previously accepted query parameters in URLs, but they were not used by the Security Flow. URL validation now considers query parameters invalid to avoid ambiguous behaviour.

Improvements

- **Storage health check improvement**
  Instead of the simple service checks used in previous versions, the *Storage* component of PAS now uses in-depth health checks to assess the state of the component.
- **Installer label improvement**
  The *deb package installer* now provides more information on administrator password generation and the use of the docker registry used for PAS software updates.
- **Support upgrading with custom management certificate trust**
  PAS has previously only allowed management scripts to skip validating custom certificates which is suitable for most use-cases, but can present a security risk in certain deployment scenarios. The management scripts have been updated to accept a custom certificate chain as a command line parameter, that will be used for validation against the certificate presented by the *Management* component.