IBM Aspera Orchestrator Considerations for GDPR Readiness

For PID(s): 5725-S59

Notice:

This document is intended to help you in your preparations for GDPR readiness. It provides information about configuration features of IBM Aspera Orchestrator as well as aspects of the product's use that should be considered to help your organization with GDPR readiness. This information is not an exhaustive list, due to the many options that clients can choose and configure. There is a large variety of ways that the product can be used in itself and with third-party applications and systems.

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Table of Contents

GDPR

General Data Protection Regulation (GDPR) has been adopted by the European Union ("EU") and takes effect in May 25, 2018.

Why is GDPR important?

GDPR establishes a stronger data protection regulatory framework for processing of personal data of individuals. GDPR brings:

- New and enhanced rights for individuals
- Widened definition of personal data
- New obligations for processors
- Potential for significant financial penalties for non-compliance
- Compulsory data breach notification

Read more about GDPR

- (EU GDPR Information Portal)[https://www.eugdpr.org/]
- (ibm.com/GDPR website)[http://ibm.com/GDPR]

Product Configuration - considerations for GDPR Readiness

References:

1. *IBM Aspera Orchestrator Admin Guide*
2. *IBM Aspera Orchestrator User Guide*

How to configure our offering such that it could be used in a GDPR environment?

1. Follow the instructions in the *IBM Aspera Orchestrator Admin Guide* to install the application.
    - See the *IBM Aspera Orchestrator User Guide* for additional configuration and security options

---

Data Life Cycle

What is the end-to-end process through which personal data go through when using our offering?

Data Types:

Account Data

- When an admin creates a new user account, account data for the user is saved in the database until the admin removes the user. However, if an admin "deactivates" a user account, the user information remains in the database.

- When an admin or manager modifies a role/group membership for a user, Orchestrator saves the new permissions in the database until an admin removes the user.
- When an admin adds a user to a group, the user inherits permissions set for the group until an admin removes the user from the group or removes the user account.

Server Configuration

- When an admin adds a remote node to Orchestrator, Orchestrator stores the node information in the database until an admin removes the node.
- When an admin changes system configuration settings, Orchestrator creates, updates, or deletes the settings in the database.

Logs

- Orchestrator logs all user activity in the application. The logs persist until deleted according to the customer admin's retention policies.
- An Orchestrator admin can change the log retention time using the Orchestrator `log_retention_days` configuration parameter, which can be found under "Engine > Configuration".

User Content

- Orchestrator is used to manage file-based workflows; it does not retain any user content.

Data Collection

Data Collected by this product

- Account Data
  - Admin users enter user data when creating and editing user accounts.
  - Non-admin users may edit their own data in their user account settings.
- IP Address
  - Admin users enter the IP address of a remote node when creating and updating node information, workflow templates, or monitors.
- Server Configuration
  - Server information is entered by an admin or a user with editing privileges when creating and editing a remote node (server).
- Logs
  - Log files record all user actions and network activity in Orchestrator.
- User Content (Unknown / Unclassified)
  - Orchestrator workflows may cause files to be saved on remote nodes. These files may be subject to cleanup (deletion) policies configured by the Orchestrator admin, if so intended.

Data Storage

Options to control/configure the storage of personal data

Storage in Account Data / IP Addresses / Server Configuration

- Orchestrator stores account data in the Orchestrator MySQL database. Only user passwords are encrypted in the database.
- Orchestrator stores IP addresses in the logs.
- Orchestrator stores server configuration data in the Orchestrator MySQL database.
- It is the discretion and responsibility of the customer admin to control and protect the logs and the MySQL database in the aforementioned points.

Storage in User Content (Unknown/Unclassified)

- Orchestrator stores user content on configured Aspera nodes. Encryption and local file permissions on Aspera nodes are managed by customer admins.
- Admins can manage content storage location through Orchestrator and can configure user permissions and access to the content. Application permissions are managed by customer admins.
- User content sent and received via Orchestrator is managed by the end user.

Storage in Databases

- The built-in MySQL database can be on the same server as the application or on a separate database. The database and host server are managed by the customer admin.
- The product also can sun with other compatible relational databases. If an alternative to the built-in MySQL database is used, the same comments apply as above about database and host server management.

Storage in Backups

- Admins can back up the MySQL database and configuration files as a compressed `.snap` file, which is saved to a location specified by the admin (or to a default location: /opt/aspera/var/archive/orchestrator/snapshots).
- It is advisable for the customer admin to set retention periods for any DB backups as those backups of Aspera Orchestrator databases may contain personal data.

Storage in Logs

- Orchestrator saves user activities in unencrypted logs. User activities include: user login, changes in permissions, and access to user data. By default, the logs are overwritten in a rotated manner. Orchestrator relies on the customer admin to encrypt, save, or archive logs and set retention policies.

Storage in Archives

- Orchestrator has an archiving feature for plugins, which archive plugin configurations and other information.
- Such archives may contain personal data such as email addresses. It is the discretion and responsibility of the customer admin to encrypt, save, or archive these

Orchestrator archives and set retention policies for them.

Data Access

Controlling access to personal data

Roles and Access Rights

Customer admin can create user accounts with the following roles:

- Administrator: Administrators can configure all system and group/role (user) access and permissions. They can also elevate non-admin users to administrator.
- Operator: Can configure workflow monitoring only.
- Developer: Can configure and design workflows (including remote nodes, journals, and snapshots).
- System: Can configure backend and maintenance processes.
- Contributor: Has limited user input capabilities.
- Scheduler: Can configure and manage queues.
- Custom roles: Administrators can configure custom, named roles, and assign permission based on those custom roles.

See “Assigning a User to a Group” in the *Aspera Orchestrator User Guide*.

Authentication

Orchestrator supports two methods of user authentication: username / password and SAML. It also supports a username / api_key method for API access.

Authenticating with Username / Password

- The username and password for a user can configured by an admin; the admin can enable an option that requires the user to change his/her own password at login. Orchestrator saves both the username and password into the database, but encrypts only the password (if that option is set by the admin when configuring the account).
- Admins can configure Orchestrator to import Directory Service users. Those usernames and passwords are handled as above, unless the admin selects the “anonymous” or “simple” login method, in which case no login or password is required.

Authenticating with SAML

- Orchestrator saves usernames but does not save passwords. The SAML IdP (Identity Provider) is responsible for security of user passwords.

Authenticating APIs with Username / API Key

- Orchestrator saves the API authentication username and API key in the Orchestrator database. The Orchestrator admin should protect the database to ensure the security of the usernames and API keys.

Data Processing

Protecting personal data

Data protection in Motion

- Web interactions with Orchestrator are encrypted using HTTPS.

Data protection at Rest

- Orchestrator offers an encryption-at-rest (EAR) option in the Faspex Delivery plugin, if that plugin is applicable to the particular workflow.

Data Deletion

Deleting User Content

- Orchestrator is used to manage file-based workflows; it does not retain any user content.

Deleting Account Data

- Only admin accounts can remove user accounts. The admin account cannot be removed.

Data Monitoring

Monitor and logging

- Admin users and system users can see activity logs for the entire application.
- Operator users and developer users can see run-time logs ("journals").

Log Files

Orchestrator logs can be found in the following locations in the installation directory:

- Log file locations:
  - Linux: /opt/aspera/var/run/orchestrator/log/orchestrator.log
  - Windows: C:\Program Files (x86)\Aspera\Orchestrator\www\var\run\log\orchestrator.log
- Customer admin has full file access control of the logs.

Responding to Data Subject Rights

Right to Access

- Only admin users can access user account data.
- Customer admins can grant or revoke a user's permission to access customer data, by granting or revoking admin group status.
- Customer admins can access all personal data except for passwords.

Right to Modify

- Admin users can modify their own user account data and other users' account data.
- Non-admin users can only modify their own user account data.
- Customer admins can modify any user's management data.
- Customer admins can grant or revoke a user's permission to modify certain customer data.

Right to Restrict Processing

- Orchestrator requires all Orchestrator product and configuration data to provide adequate product functionality and service. The customer admin is in control of restricting data usage for other purposes.

Right to Object

- The customer admin has control of all Orchestrator processes and functions.

Right to Be Forgotten

- The customer admin can remove any end user from the active system.
- If Orchestrator workflows make references to the end user by email address, then in the event the user is to be removed from the system, the workflow will need to be modified to remove the user's email from the workflow configuration. If the email is the last email in a set of email addresses, the email will need to be replaced with another user's email address, or the workflow will need to be modified to not require any email notification step.
- Orchestrator does not provide off-the-shelf functionality to remove data from logs or database backups. It is up to the customer admin to design a way to remove data from logs and database backups.

Right to Data Portability

- Orchestrator does not provide off-the-shelf functionality to port data from logs or database backups. It is up to the customer admin to design a way to port user data.

Appendix

1. *IBM Aspera Orchestrator Admin Guide*
2. *IBM Aspera Orchestrator User Guide*