IBM Aspera Console 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 features of IBM Aspera Console that you can configure, and aspects of the product's use, that you should consider to help your organization with GDPR readiness. This information is not an exhaustive list, due to the many ways that clients can choose and configure features, and the 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 applies from 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 Console Admin Guide*
2. *Aspera Ecosystem Security Best Practice* (found in Appendix of Admin Guide)

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

1. Follow the instructions in the *Aspera Console Admin Guide* to install the application.
2. In the *Aspera Security Best Practices Guide* located in the Appendix of the *IBM Aspera Console Admin Guide*, follow the instructions in the topics below:
   - Securing the Aspera Application
   - Console
   - Securing Content in your Workflow
3. In the *Aspera Console Admin Guide*, follow the instructions in Securing Console section.

Data Life Cycle

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

Data Types:

- Account Data
  - Username
  - Password

  - First Name
  - Email
  - Roles & Privileges
- Transfer Monitoring and Reporting Data
  - IP Address
  - Timestamps
  - Session Information
  - File Metadata
  - Custom Fields (*see Creating Custom Fields*)
- Server Configuration
- Logs
- User Content (Unknown / Unclassified)

Account Data

- When admin creates a local user account, account data is saved in the database, until an admin removes the user.
- When admin imports a directory service user, Console creates a new account for the user account data. Account data saved in the database, until an admin removes the Console user.
- When admin imports a SAML user, Console creates a new account for the user and saves the usernames and email addresses in the database. Passwords are not saved by Console. Account data remains until an admin removes the new Console account.
- When users log in through SAML, Console creates a new account for the user and saves the usernames and email addresses in the database. Passwords are not saved by Console. Account data remains until an admin removes the new Console account.
- When an admin adds a user to a group, Console saves that authorization until an admin removes the user from the group or removes the user account.
- When a user modifies his or her user account settings, Console updates that information in the database.
- When a user adds an SSH key to Console, Console stores that key until the user removes the key or an admin removes the user account.
- When a user starts a transfer with personal login credentials to a node, Console stores those credentials until the user removes them or an admin removes the user account.

Transfer Monitoring and Reporting Data

- IP addresses are saved to logs whenever a user logs in. The information persists until the customer admin removes the logs.
- Console collects data on every monitored transfer, including but not limited to:
  - Node credentials and IP addresses
  - File metadata
  - Transfer user metadata

This information is stored in the Console database until a customer admin removes the data from the database. For more information about the specific data Console monitors and reports, see *Running Reports.*

Server Configuration Data

- When an admin adds a node to Console, Console stores the node address (IP or domain name), name, and credentials in the database, until an admin removes the node.
- When an admin adds a cluster to Console, Console stores the cluster's domain name, name, port, and credentials in the database, until an admin removes the cluster.
- When an admin changes system configuration settings, Console stores the settings in the database.
- When an admin changes node configuration settings, Console stores the settings in the node database.

Logs

- Console logs all activities. The logs persist until deleted according to the customer admin's retention policies.
- When Console initiates a transfer, Console collects metadata on the transfer. This data is stored on the database until an admin deletes the entry.

User Content

- All user content is stored on Console nodes, and users do not download from or upload to Console.

Data Collection

Data Collected by this product

- Account Data
  - Username
  - Password
  - First Name
  - Email
  - Roles & Privileges
- Transfer Monitoring and Reporting Data
  - IP Address
  - Timestamps
  - Session Information
  - File Metadata
  - Custom Fields (*see Creating Custom Fields*)
- Server Configuration
- Logs

- User Content (Unknown / Unclassified)

Data Storage

Options to control/configure the storage of personal data

Storage in Account Data / IP Addresses / Server Configuration

- Console stores account data in the Console MySQL database. Only user passwords are encrypted on the database. Console relies on the customer admin to control and protect the MySQL database.
- Console stores IP addresses in the logs. Console relies on the customer admin to control and protect the logs.
- Console stores server configuration data in the Console MySQL database. Console relies on the customer admin to control and protect the MySQL database.
- Console stores node configuration data in the node MySQL database. Console relies on the customer admin to control and protect the node MySQL databases.

Storage in User Content (Unknown/Unclassified)

- Console stores user content on configured Aspera nodes. Console relies on customer admins of those nodes for encryption and local file permissions. Customer admins can take additional measures to control and protect their nodes by referring to the guidance provided by the *Aspera Ecosystem Security Best Practices* document as well as the GDPR guidelines for *IBM Aspera Enterprise Server*.

Storage in Databases

- The MySQL database can be on the same server as the application or on a separate database. Console relies on the customer admin to control and protect the database and its host server.

Storage in Backups

- Admins can back up the MySQL database and configuration files with a backup script in an unencrypted backup directory. Console relies on the customer admin for encryption, storage location, and retention policy.
- Customer admin has full control of the backup files.

Storage in Logs

- Console saves user activities in unencrypted logs. User activities include: user login, change of management, and access to client data. By default, the logs will be overwritten in a rotated manner. Console relies on the customer admin to encrypt, save, or archive logs and set retention policies.

Data Access

Controlling access to personal data

Roles and Access Rights

Customer admin can create user accounts with the following roles:

- Admin: Admins can create and configure all system and user settings and permissions. They can also elevate users to admins. Admins can access and configure all nodes and clusters. Admins can initiate transfers between any combination of nodes or clusters.
- User: Users can only access nodes or clusters they are given permission to access.

Separation of Duties

Customer admin has full control.

Authentication

Console supports two methods of authentication: username / password and SAML.

Authenticating with Username / Password

- The username and password is provided by the user during initial registration or configured by an admin. Console saves both into the database, but encrypts only the password.
- Admins can configure Console to import Directory Service users and groups. Those usernames and passwords are handled as above.

Authenticating with SAML

- Console saves usernames but does not save passwords. The SAML IdP is responsible for security of user passwords.

Data Processing

Protecting personal data

Data protection in Motion

- Admins can configure Console to initiate transfers using AES-128 encryption mode. See *Configuring Security Settings*.

Data protection at Rest

- Admins can configure encryption-at-rest (EAR) on Aspera Nodes to store content uploaded to the server in an encrypted state. When downloaded from the server, server-side EAR first decrypts the files and then transfers the files to the client's disk in an unencrypted state. For more information, See the *Aspera Enterprise Server Admin Guide: Server-Side Encryption at Rest (EAR)*.

- The encryption key for EAR is saved in the aspera.conf configuration file as cleartext. The customer admin needs to take proper protection to avoid unauthorized access.
- Console relies on the customer admin to handle account data, content storage, and access to databases and files on the server.

Data Deletion

Deleting Account Data

- Only admin accounts can remove user accounts.

Data Monitoring

Monitor and logging

- Admins can see access logs for the entire application.
- Diagnostics data is saved in logs. Admins can change the logging level to gather more data (though at the cost of performance).

Log Files

Console logs can be found in the following locations in the Aspera and Common Files folders in the Program Files directory:

- Aspera\Management Console\log\
- Common Files\Aspera\Common\asctl\
- Common Files\Aspera\Common\mysql\data\mysqld.log
- Common Files\Aspera\Common\apache\logs\Log

Customer admin has full file access control to the logs.

Responding to Data Subject Rights

Right to Access

- End users can access their account data.
- Customer admins can grant or revoke a user's permission to access certain customer data.
- Customer admins can give Console users permission to initiate transfers between nodes and clusters.
- Customer admins can access all personal data except for passwords.
- Console does not have the off-the-shelf functionality to single out a specific user's data from logs or database backup.

Right to Modify

- End users can modify their own 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.
- The activity log data cannot be modified by Console.

Right to Restrict Processing

- Console requires all data to provide adequate service. Customer admin is in control of restricting data usage for other purposes.

Right to Object

- Customer admin is in control.

Right to Be Forgotten

- Customer admin can remove any end user from the active system.
- Console 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

- Console 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 Console Admin Guide*
2. *Aspera Ecosystem Security Best Practice* (found in Appendix of Admin Guide)