IBM Aspera Connect Considerations for GDPR Readiness

For PID(s): 5725-S57

Notice:

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM Aspera Connect 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 Connect User Guide*

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

1. Follow the installation instructions in the *IBM Aspera Connect User Guide*.
2. In the *IBM Aspera Connect User Guide*, follow the procedures in *Part 4: Security Configuration* in order to:
    - specify servers that are trusted and servers that are restricted
    - configure authentication options
    - configure content protection (encryption)

Data Life Cycle

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

- User ID and password, when a user or admin sets up an account on a target server, and when a user specifies those credentials to establish a connection to a target server. Removal of this data occurs when an admin deletes an account from the target server.

- IP address of the server host, when the user specifies the address of the target server in the browser address bar.
- Log files: activities, performance, errors, and various activities are recorded in automatically created log files. The default location of the log files is specified in the user guide. Removal is left to the owners of the data.
- Any personal data that may be included in transfer content (files uploaded/downloaded. Removal or retention is at the discretion of the data owners on the client and on the server.

Data Collection

Data Collected by this product

See *Data Lifecycle* above.

- User ID and password
- IP address of server
- Log files
- Transferred content

Data Storage

Options to control/configure the storage of personal data

- Connect stores account data, IP addresses, and configuration settings in a database. Control and protection of the database is the responsibility of users or system administrators for the client and server; it is not managed through Connect itself.
- Storage of transfer content:
  The initial storage location of transferred data is the destination set by the Connect user. Any subsequent location of storage is at the discretion of users or system administrators for the client and server; it is not managed through Connect itself.
- Storage in databases:
  The location of Connect's database file, **`connectdb.data`**, varies by platform and is indicated in the *Connect User Guide*. Security and removal of database files is at the discretion of users or system administrators for the client; it is not managed through Connect itself.

- Storage in logs:
  Location of log files varies by platform and is specified in the *Connect User Guide*. Security and removal of log files is at the discretion of users or system administrators; it is not managed through Connect itself.
- Storage in backups:
  The location of backups and the tools for doing backups is left to users or system administrators; it is not managed through Connect itself.
- Storage in archives:
  The location of archives is left to users or system administrators; it is not managed through Connect itself.

Data Access

Controlling access to personal data

- By requiring authentication credentials: user ID and password
- By adding Aspera servers to the Restricted Hosts list, settable from Connect. Hosts on the list will require confirmation every time a user attempts to initiate a transfer with that host.
- By using the Content Protection feature, configurable from Connect. This feature allows users to encrypt files for transfer. Access to the data in the encrypted files requires decryption with a password.
- System administrators can use OS facilities to set file and directory access permissions on client and server file systems based on user roles (administrator, regular user, and so on). However, access permissions are not settable from Connect.

Data Processing

Protecting personal data

- Protection of data in motion:
  - By using Connect's Content Protection feature, which lets users encrypt files for transfer. Access to the data in the encrypted files requires decryption with a password.
  - By configuring transfers to go through HTTP/HTTPS – this is server side configuration. On the server side, customer can configure to use http or https when the default transport protocol FASP is not working.
- Protection of data at rest:

- By configuring data storage to use encryption-at-rest.
- By protecting data-storage (described above in *Data Storage*) using the methods described above in *Data Access*.
- User login credentials are encrypted.
- User can choose OS level disk encryption to further protect data on the local drive. This is not the feature of Aspera Connect but the feature of Operating System.

Data Deletion

- Using the methods described above for protecting data and controlling user access.
- Using standard OS administrative processes (not Connect features), administrators can revoke user access when accounts expire or are unused for a specified period of time.

Data Monitoring

Monitoring and Logging

- Connect users can configure three logging levels: **Info** (basic level), **Debug** (verbose), **Trace** (extra verbose). Details and how to specify the levels are described in the *Connect User Guide* under *Part 3: Basic Configuration*.
- The location of log files is not configurable. Location varies by platform and is specified in the *Connect User Guide*. The folder containing a user's log files can be opened directly from the Connect application.
- By default, log files are created with permissions set to allow access only by the Connect user or system administrator. Removal of log files is at the discretion of users or system administrators; it is not managed through Connect itself. Information about removing log files is provided in the *Connect User Guide* under *File Cleanup*.
- Log file retention is at the discretion of the user or system administrators; it is not managed through Connect itself.

Responding to Data Subject Rights

Since Aspera Connect is a client application deployed on the local computer, the local computer admin has full rights to the data that is on the local computer. It is up to the admin of the local computer to manage:

- Right to Access
  - Customer provide individuals access to their data
  - Customer provide individuals information about what data the customer has about the individual
- Right to Modify
  - Customer allow an individual to modify or correct their data
  - Customer correct an individual's data for them
- Right to Restrict Processing
  - Customer stop processing an individual's data
- Right to Object
  - Same as right to restrict.
- Right to Be Forgotten
  - Customer delete an individual's data
- Right to Data Portability
  - Customer provide an individual with the information that they have about the individual in a user-friendly/machine readable format

---

Appendix

1. IBM Aspera Connect User Guide