IBM Aspera High-Speed Transfer Server and IBM Aspera High-Speed Transfer Endpoint Considerations for GDPR Readiness

Notice:

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM Aspera High-Speed Transfer Server and IBM Aspera High-Speed Transfer Endpoint 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 High-Speed Transfer Server and IBM Aspera High-Speed Endpoint Admin Guides.*
2. *Aspera Ecosystem Security Best Practices (found in the appendix of the Admin Guides)*

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

1. Follow the instructions in the offering's Admin Guide to install the application.
2. Follow the instructions for Enterprise Server in the "Aspera Ecosystem Security Best Practices" article in the appendix of the Admin Guide.
3. If you are using the High-Speed Transfer Server's built-in web UI, the Node API, or HTTP Fallback, install a valid, CA-signed SSL certificate. For instructions, see "Installing SSL Certificates" in the Admin Guide.

Data Life Cycle

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

The High-Speed Transfer Server and High-Speed Endpoint are accessed by Aspera client applications through SSH connections. If the clients use the Node API or Watch Folders, they also access the server through HTTP/HTTPS connections.

Data Types

- Account data
    - Operating system username
    - Operating system password or SSH public key
    - Node API credentials (if using the Node API or Watch Folders)
    - Object storage credentials (if connecting to object storage)
    - IBM Aspera Transfer Service (ATS) access key ID and secret (if connecting to ATS)
    - Roles and privileges
    - Email addresses (only if using email notifications but this is being deprecated in the next High-Speed Transfer Server release)
- IP addresses or hostnames
    - Client IP address
    - Server IP address or hostname
- Client and server configuration
- Logs
- User content
    - Uploaded, downloaded, and moved files

Account Data Life Cycle

- An Aspera Transfer Server user is first created on the OS as OS system user. The user login credentials to the server are managed by OS. Aspera Transfer Server adds system users and configure them as Aspera Transfer Server users. The user configurations are saved in the Aspera configuration file (aspera.conf), which is in user's etc folder. The Aspera user exists until the user is deleted from the operating system by the admin. Refer to Admin Guide section Setting Up Users for details.

- If the admin adds the user's public SSH key, which the client sends to the admin, as a way for the user to authenticate to the server, the SSH public key is stored in the location specified in the Aspera configuration file (aspera.conf) on the Server or Endpoint. In general, only the admin has access to the users SSH public key. The SSH public key can be deleted by the admin.

- When the admin configures the user's docroot (the pathname of the directory on the Server or Endpoint to which the user is allowed access), if the Server or Endpoint is in cloud storage then the admin can enter the object storage credentials in the docroot. The docroot is specified in the Aspera configuration file (aspera.conf),

which only admins can modify. The credentials are stored in aspera.conf until the admin removes them.

- When the admin associates Node API credentials (username and password) with a system user, the credentials are stored in the Redis database. Node API passwords are not readable by any user or admin. Node API user passwords are encrypted in the Redis database.
- When the admin assigns permissions (ACLs) to a Node API username, the permissions are stored in the Redis database until the node user is deleted. System admins and Node API users with permissions can view permissions.
- When the user creates a connection in the GUI to a remote Server or Endpoint, they enter their SSH credentials, which are the system username and either the password or the path to the user's private key on the local computer. The user enters object storage credentials if the connection is to a remote Server or Endpoint in object storage.
- When the user creates a connection to an ATS storage in the GUI, they enter their ATS access key ID and secret.
- When the user starts an ascp, ascp4, or async session in the command line, they enter authentication credentials, as required. The SSH username and the path to the user's private SSH key are logged only by the initiator of the transfer.
    - SSH credentials – The username is required. If using password authentication, the password is optional and can be entered at the prompt or set as an environment variable if it is not supplied in the command. If using SSH key authentication, the path to the private key on the local computer.
    - Object storage credentials – The user might include the access key ID and secret for the object storage, if the credentials are not added by the admin to the user's docroot.
    - ATS credentials – The user provides the ATS access key ID and secret as a basic token.
- When the admin installs the Server or Endpoint application, the Aspera RunD service automatically launches a Watch service and a Watch Folder service on the local computer under the admin account (Unix-like OS) or the Aspera Service Account (Windows OS). The admin can view the username under which the services are running, but the password is not readable. This data is stored in the Redis database until the service is deleted.
- When the user creates a Watch Folder in the GUI, they enter their SSH credentials for the remote Server or Endpoint, which are the system username and either the password or the path to the user's private key on the local computer. The account data are stored in the Redis database until the Watch Folder is deleted by the user or admin.

- When the user creates a Watch Folder using the Watch Folder API or the command line tool aswatchadmin, the Watch Folder configuration is usually created in a JSON file and contains the SSH credentials for the remote Server or Endpoint, which are the system username and either the password or the path to the user's private key on the local computer. When the Watch Folder is started, the account data are stored in the Redis database until the Watch Folder is deleted by the user or admin. The JSON file containing the Watch Folder configuration is under the user's control and deleted by the user or admin.

IP Address Life Cycle

- Client and Server or Endpoint IP addresses or hostnames are entered by users when they create a connection in the GUI, start an ascp, ascp4, or async transfer, set up a Watch Folder, or send a request to the Node API service. IP addresses or hostnames are saved to activity logs. For Watch Folder and Node API activity, they are also saved to the Redis database. The information persists in the logs until the logs are overwritten or the admin removes the logs. The information persists in the Redis database until it expires and is deleted. The admin controls the retention time for event logs in the Redis database.

Client and Server Configuration

- When an admin configures a user for Aspera transfers or configures Server or Endpoint settings, the configuration is stored in aspera.conf, which can be modified only by admins. The configuration persists until it is deleted by an admin or until aspera.conf is deleted.

- When a user submits a transfer request through the GUI or command line, including the Node API, the client transfer configuration and server transfer configuration are compared and applied following precedence rules. The log records the final transfer configuration, which can include settings from the client and the server.

- When a user submits an authorized GET request to the Node API /info endpoint, the response includes information about the server system, server capabilities, and configuration settings related to transfers. The user controls the configuration information in their possession.

Logs

- High-Speed Transfer Server and High-Speed Transfer Endpoint log all activities. Transfer session details, including SSH username, path to the user's private SSH key and the remote host IP address or hostname, are logged. Passwords are not logged. Admins can configure the logging location on the server. If allowed by the server configuration, clients can specify the directory where on the server their transfer activity is logged. Logs persist until they are overwritten or deleted by an admin, or the user if they have access to the log directory.

User Content

- When a user transfers content between their computer and a High-Speed Transfer Server and High-Speed Transfer Endpoint, the content is encrypted during transfer by default. The client and server admin can configure the cipher to use for in-transit encryption. In-transit encryption only applies to content while it is transit. Encryption of the content on the server or on the client computer is controlled by the server admin and client user, respectively.
- When a user uploads content to a Server or Endpoint, the content is stored in the destination directory that is specified by the client until the client deletes it or the admin removes it. The admin can configure the Server or Endpoint to use server-side encryption-at-rest, in which case the content is encrypted while it is stored on the Server or Endpoint.
- When a user downloads content from a Server or Endpoint, the content is stored in the destination directory on the user's computer. The user controls the content in their possession.

Data Collection

Data Collected by this product

- Account data
  - Operating system username
  - Operating system password or SSH public key
  - Node API credentials (if using the Node API or Watch Folders)
  - Object storage credentials (if connecting to object storage)
  - IBM Aspera Transfer Service (ATS) access key ID and secret (if connecting to ATS)
  - Roles and privileges
- IP addresses or hostnames
  - Client IP address
  - Server IP address or hostname
- Client and server configuration
- Logs
- User content
  - Uploaded, downloaded, and moved files

Data Storage

Options to control/configure the storage of personal data

Storage of Account Data / IP Addresses / Server Configuration

- SSH account data for High-Speed Transfer Server and High-Speed Transfer Endpoint is stored in the operating system. Server and Endpoint rely on the server admin to control and protect system account data.
- Node API credentials are stored in the Redis database. Passwords are encrypted in the database. Server and Endpoint rely on the server admin to control and protect Node API account data.
- Server and Endpoint store IP addresses and hostnames in the logs, in aspera.conf, and in the Redis database. Server and Endpoint rely on the server admin to control and protect the logs, Aspera configuration file, and Redis database.
- Server configuration settings are stored in aspera.conf. Server and Endpoint rely on the server admin to control and protect the Aspera configuration file.

Storage of User Content (Unknown/Unclassified)

- User content is stored on the High-Speed Transfer Server and High-Speed Transfer Endpoint. Server and Endpoint rely on the server admin to control and protect the user content by managing user access and following the best practices described in "Aspera Ecosystem Security Best Practices" in the Admin Guide.
- Users can encrypt their content before uploading it to the server or while it is stored on their local computer; for instructions see "Client-Side Encryption at Rest (EAR)" in the Admin Guide.
- Admins can configure the server to encrypt content when it is uploaded to the server; for instructions see "aspera.conf – Server-Side Encryption at Rest" in the Admin Guide.
- Admins can control file system access by setting docroots or restrictions for system users and setting system users' shells to the Aspera shell, aspshell. For instructions see "Set up Users and Groups" in the Admin Guide.
- Node API users with admin privileges can limit access to user content by Node API users who authenticate with bearer tokens by setting file permissions with the /permissions endpoint.

Storage of Databases

The Redis database is located on the same computer as the High-Speed Transfer Server and High-Speed Transfer Endpoint. Server and Endpoint rely on the server admin to control and protect the database.

Storage of Backups

Admins can back up all or parts of the Redis database by using Aspera command line tools that create the backup in an unencrypted backup directory. High-Speed Transfer Server and High-Speed Transfer Endpoint relies on the customer admin for encryption, storage location, and retention policy for the database.

The High-Speed Transfer Server or High-Speed Transfer Endpoint admin has full control of the backup files.

Storage of Logs

High-Speed Transfer Server and High-Speed Transfer Endpoint save user activities in unencrypted logs. By default, the logs are overwritten on a rotation. Server and Endpoint rely on the admin to encrypt, save, or archive logs and set retention policies.

Storage of Archives

Clients who transfer with High-Speed Transfer Server and High-Speed Transfer Endpoint can archive content in an archive directory within their docroot or restriction after it is downloaded to the client computer. The Server or Endpoint admin has full control of the file system.

Data Access

Controlling access to personal data

Authentication

- Admins restrict access to High-Speed Transfer Server and High-Speed Transfer Endpoint by creating system users with SSH credentials. For instructions, see “Set up Users” in the Admin Guide.
- Admins restrict HTTP/HTTPS access to High-Speed Transfer Server and High-Speed Transfer Endpoint by creating a derivative of SSH credentials, such as Node API credentials, access key, basic token, or bearer token. For instructions, see the “Authentication and Authorization” section of the Admin Guide.

Server Configuration

- Admins configure the SSH server and firewall to prevent unauthorized access to High-Speed Transfer Server and High-Speed Transfer Endpoint. For instructions, see “Configuring the Firewall” and “Securing Your SSH Server” in the Admin Guide.
- Admins keep system software and Aspera software up to date.

User Configuration

- Admins restrict client access to the High-Speed Transfer Server and High-Speed Transfer Endpoint filesystem by configuring a docroot or restriction. For instructions, see "Set up Users" in the Admin Guide.
- Admins restrict the actions that clients can do on the High-Speed Transfer Server and High-Speed Transfer Endpoint by setting the client's shell to the Aspera shell, aspshell and configuring user permissions and settings. For instructions, see "Set up Users", "Authorization Configuration", and "Aspera Ecosystem Security Best Practices" in the Admin Guide.

Data Processing

Protecting personal data

Data Protection in Transit

- By default, data is encrypted using AES-128 in transit between the client and the High-Speed Transfer Server or High-Speed Transfer Endpoint.
    - Admins can require a stronger encryption cipher by modifying aspera.conf; for instructions, see "Authorization Configuration" in the Admin Guide.
    - Node API admin users can require encryption for transfers that are started by access key users; for instructions, see "Access Key Authentication" in the Admin Guide.
    - Clients can request a stronger encryption cipher in the transfer request; for instructions, see "Transfer Files in the GUI," "Ascp Command Reference," "Watch Folder Configuration Reference," and "Aspera Sync Command Reference" in the Admin Guide.
- Admins can configure a valid, CA-signed SSL certificate to protect content transferred by Node API request and HTTP/HTTPS transfers. For instructions, see "Installing SSL Certificates" in the Admin Guide.
- Admins can set the server's SSH fingerprint in aspera.conf. This enables clients to confirm the SSH fingerprint and prevent transfers if the fingerprints do not match. For instructions see "Securing Your SSH Server" in the Admin Guide.

Data Protection at Rest

- Admins can configure the server to encrypt content when it is uploaded to the server; for instructions see "aspera.conf – Server-Side Encryption at Rest" in the Admin Guide.

- The encryption key for server-side EAR is not encrypted in the Aspera configuration file (aspera.conf). The admin must protect aspera.conf to avoid unauthorized access.
- Users can encrypt their content before uploading it to the server or while it is stored on their local computer; for instructions see “Client-Side Encryption at Rest (EAR)” in the Admin Guide.
- Admins can control access to the operating system user information, Aspera configuration file (aspera.conf), user content, and the Aspera Redis database through user permissions. Server and Endpoint rely on the admin to control and protect this content.

Data Deletion

Deleting User Content

- Admins can delete content on a High-Speed Transfer Server or High-Speed Transfer Endpoint.
- Users can delete content within their docroot or restriction.

Deleting Account Data

- Only system admins can remove user accounts and delete Node API credentials.

Data Monitoring

Monitor and logging

- Admins can view the activity logs for the entire application.
- Node API users can view events associated with their authentication method, if event logging is enabled on High-Speed Transfer Server or High-Speed Transfer Endpoint.
- Users can view content transfer progress in the GUI.
- Diagnostics data is saved in logs. Admins can change the logging level to gather more data (though at the cost of performance).

Log Files

- For the default log location, see “Log Files” in the Admin Guide.
- Users can configure different logging locations if allowed by the server configuration.

- The system admin has full file access control to the logs and can configure log size, location, and intensity. For information, see "Server Logging Configuration for Ascp and Ascp4" and "Logging and Reporting" (for Aspera Sync) in the Admin Guide.

Responding to Data Subject Rights

Right to Access

- Users can access their account data.
- Admins can grant or revoke a user's permission to access certain customer data.
- Admins can access all personal data except for passwords.
- High-Speed Transfer Server and High-Speed Transfer Endpoint do not have the off-the-shelf functionality to single out a specific user's data from logs or database backup.

Right to Modify

- Users can modify their own account data.
- Admins can modify any user's management data.
- Admins can grant or revoke a user's permission to modify certain customer data.
- The activity log data cannot be modified by High-Speed Transfer Server or High-Speed Transfer Endpoint.

Right to Restrict Processing

- High-Speed Transfer Server and High-Speed Transfer Endpoint require 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 user from the active system. High-Speed Transfer Server and High-Speed Transfer Endpoint do 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

- High-Speed Transfer Server and High-Speed Transfer Endpoint do not provide off-the-shelf functionality to port individual user data from logs or database backups. Client admin needs to design a way to port user data.

Appendix

1. IBM Aspera High-Speed Transfer Server and IBM Aspera High-Speed Endpoint Admin Guides.
2. Aspera Ecosystem Security Best Practices (found in the appendix of the Admin Guides)