IBM Aspera Cloud Services Information Security Practices

A Technical Discussion on the Security Practices for Aspera Cloud Services

Contents:

Aspera provides both single tenant and multi-tenant cloud services for high speed, secure transfer of digital content. These services are application software platforms running on multiple public cloud environments, managed by Aspera, and offer customers several choices of specific Aspera product interfaces, cloud infrastructure providers, and pay-as-you-go as well as continuous, pre-committed deployment options. All Aspera cloud service options are engineered to provide secure, private protection of the customer's digital content transferred and managed by the Aspera software platform. This document covers the key practices Aspera uses to achieve this security in its cloud services including Aspera software features, deployment practices, and infrastructure management practices.

The primary objective in securing Aspera Cloud Services is to protect the customer's digital content from unauthorized access or compromise. This includes the following requirements:

- Securing the Aspera application and transfer software by fully utilizing its rich security capabilities and configuring the infrastructure and software for best protection.
- Securing the cloud infrastructure on which the software runs.
- Securing operation including verifying the security of the end-to-end workflow through self-testing, audit and 3rd party audit review and responding efficiently to new vulnerability announcements and security incidents.

We describe how we achieve these requirements in the following sections.

Securing the Aspera Application and Transfer Software

The Aspera Enterprise Server and Faspex, Shares and Files application software have multiple security capabilities that are enabled in the Aspera Cloud Services, and depend on certain system services that are configured in a hardened manner. Secure, Reliable, High Performance Aspera FASP Protocol for Data Transfer: All Aspera transfers use the FASP protocol which provides on the wire strong encryption, optional strong encryption of content at rest (client and/or server side), integrity of the data transferred, and secure host and end user session authentication. The details of the FASP protocol security model are detailed in the FASP Security Model.

SSH Service: The system SSH service on Linux provides secure authentication for the Aspera Enterprise Server transfer software, the foundation transfer server software for all Aspera Cloud services. The SSH service is configured to run on port 3001; no access is allowed on port 22. SSH tunneling is disabled; TCPForwarding is turned off; Root Login is disabled; and Password Authentication is disabled. All authentication with Aspera applications such as Faspex, Shares, Console and Files is done with SSH keys, and is only enabled if the workflow includes client software that requires password authentication. Finally, the allowed SSH ciphers are configured to permit only the strongest ciphers according to current best practices (which are continually reviewed).

Firewall Configuration: All Aspera Cloud Services include a firewall configuration that permits inbound access only to TCP and UDP ports 33001 for transfer, and on TCP 9092 (443 in the case of Files) for connectivity between the application and the asperanoded daemon. For Faspex, Shares, Console and Files, the Firewall is configured to permit inbound access to TCP Port 9092 or 443 (depending on the application) from the application's host to the Enterprise Server host.

Aspera Enterprise Server Configuration: Aspera Enterprise Server Configuration: The Enterprise Server software is configured to use its secure shell, the 'aspshell', which strictly limits process execution and file path access within the shell to Aspera authorized processes and pathnames within the configured root path. The main configuration file, aspera.conf is configured to deny all access within the shell and to allow only the specific authorization required by the application, e.g. token authorization for Faspex/Shares.

- A secure docroot with a restriction setting that limits the type of storage root allowed (e.g. s3://*) is configured for all transfer users. Where the cloud infrastructure provides it, a role based account is used for the storage root access to the cloud storage, e.g. IAM Roles for AWS s3.
- Encryption in transit is configured as required, using AES128 (for more details on the FASP protocol security please see the FASP Security Model). Server-side encryption at rest is configured ON based on a customer's request. The asperanoded and asperahttpd services are configured with properly signed SSL certificates to secure the application to server node communication. In Shares and Faspex, asperanoded credentials are stored in a hashed, encrypted format. In Files, the asperanoded access keys are not stored at all by the application.

Aspera Application Configuration: (Aspera Shares, Aspera Faspex, and Aspera Files): The Aspera web applications also include a host of capabilities to harden their security, which are configured on as much as possible given customer capabilities in all Aspera Cloud Services: All Applications support single sign-on with enterprise SAML 2.0 identity providers; the SSO provider should be configured with strong passwords and if possible multi-factor authentication. For local user authentication, the applications are configured to enforce strong passwords, a limited number of authentication attempts, and periodic password expiration and reset. Connectivity to the Aspera server nodes is configured to require SSL certificate verification.

Special Note on Encryption at Rest: If the customer's workflow permits the Aspera Cloud service can require client side encryption at rest (user protects content using a secret and communicates the secret out of band to the intended final recipient) in addition to server side encryption at rest (secret is managed on the server side). (Aspera's client side and server side encryption at rest utilize the same FASP encryption pipeline as encryption in transit as described in the FASP Security Model).

Securing the Cloud Infrastructure

The Aspera Cloud Services are designed to run on public cloud infrastructure that provides the compute, network and storage for the Service. The Aspera Operations Team ensures that these infrastructure capabilities are hardened to secure the host computers and storage; to ensure

service availability and integrity; to secure access, authorization and audit capabilities throughout the infrastructure and application stack; and to secure all network flows and firewalls. The specific requirements and implementation policies used are detailed below.

General Security of Host Computers and Storage: All hosts are configured to use Aspera Operational Support Systems (OSS) for ntp synchronization and DNS. Syslog from all hosts is collected and aggregated in an OSS cluster for indexing and search. All non-essential OS accounts are removed, and all system level passwords are strong, randomly generated and securely stored and rotated via a password vault. All unnecessary services are disabled or removed, and all Aspera application databases are configured to bind only localhost interfaces (no extraneous external interfaces). All unnecessary packages, modules, scripts and drivers are removed from system services. All Aspera application services are configured to run as non-root / unprivileged users with credentials rotated periodically.

Service Availability and Integrity: Automated configuration management is used end-to-end to ensure integrity of all critical services: for managing the Aspera application code repositories, for software package build and deployment to staging, and for application and OS configuration management in the Cloud Service. All OS and application service packages are kept up to date.

Secure Authentication: All Aspera applications are set to authenticate administrators via SAML or OAuth2. All Aspera applications are designed such that each user authenticates under a unique account, and all major user activities are recorded to the application logs, which are aggregated for audit review in an OSS cluster and actively monitored for suspicious events. All Aspera applications are configured to prevent brute force attacks against credentials including a) SAML/Oauth2 for end user authentication (customer permitting); and b) for any local users, requiring passwords with strong complexity, a limited number of failed password attempts, an adequately long time period for account lockout, and forced reset of passwords periodically. All Aspera applications also provide the ability to display a managed disclaimer (configurable by the customer) that informs the end-users that only authorized users of the system are permitted access and any business specific policies assumed.

Audit Logging: All major user activities are recorded to the application logs, which are aggregated for audit review in an OSS cluster and actively monitored for suspicious events. Event logging includes all authentication attempts (credentials are not logged), application start-up and shut-down, Aspera Application and Enterprise Server configuration changes, client requests and server responses, and all content transfer activities with details of client/server IPs, source and destination pathnames, transfer statistics, status, etc. Logging is severity classified, and includes the service component performing the operation, the event type, event specific information, and timestamps. Error messages displayed to users are sanitized to ensure no sensitive information is displayed.

Secure Operator and End User Credential Management: All Aspera applications provide secure self-service reset of local user passwords requiring the user to provide the previous password before applying a new one. Service account credentials are also automatically rotated periodically. Customers are encouraged to configure any SAML or Oauth2 provider configured with the Aspera Cloud Service application to expire second factor keys, certs, and pins periodically. Any local user credentials and service account credentials required by the Aspera applications are stored securely using secure salted hash functions.

Secure Authorization: All Aspera applications are designed to authorize users under a specific role-based access control in which only an administrator role can view and configure audit logs, end user access policies, etc. All Aspera application services are designed to meet the principle of least privilege such that each module is granted the minimum set of privileges and system resources needed for its primary operations. For example Aspera management services cannot be used to modify customer content protected by the secure aspshell, and the access key authentication option ensures that Aspera Files and other 3rd party applications require no access to customer storage credentials.

Secure Network Flows and Firewall: The Aspera Cloud Services are configured using the features of the cloud service provider's best practices for host and application firewalls, and Aspera software best practices for secure network flows. All network configuration is also completely automated for predictability and verification.

Firewall: All flows are denied by default and configured to allow only the Aspera required authorized flows, to only authorized source and destination IPs for the Aspera applications (Shares, Faspex, Files). Specific whitelists for specific Aspera client IPs can also be configured. Firewall administrative control is limited to only Aspera Network Operations staff, and is read-only for other Aspera support and engineering.

Network Flows: All Aspera Cloud Services are configured to enforce specific hardened secure transport and authentication protocols using current best practices. As of the date of this document these include:

- Encryption of all HTTP traffic using TLS v1,1.1,1.2.
  - All HTTPS services maintain a Qualys score of 'A+'
- Encryption Algorithms for FASP and SSH - AES128 (default) with options for AES 192/256 (encryption), RSA 2048 (asymmetric encryption, digital signatures) and DSA 2048 (digital signatures), SHA-2* (one-way hash and message digest)

All Aspera Applications (Shares, Faspex and Files) are configured to enforce SSL certificate validation including hostname, expiration date, CA signature, etc. and require explicit certificate installation (no Trust on First Use). Automated deployment removes all self-signed certificates.

Continuous Operation Security and Incident Response

Aspera Operations and Engineering follow a continuous (24x7x365) and disciplined practice to proactively detect and respond to any potential or real vulnerability in the Aspera Application Software or Cloud Services infrastructure. Key practices include the following:

Comprehensive Security Scan Pre-release and Periodically:

Before every major and minor release and upgrade, all Aspera Applications and Enterprise Server software are validated with IBM AppScan and validated for A+ rating for Qualys. On every major release, key components are tested by 3rd party audit firms hired by Aspera. On every infrastructure upgrade, the Aspera Cloud Services infrastructure is scanned using the nmap framework. Periodically (once per month) the infrastructure is re-scanned using the nmap framework.

Continuous Monitoring for Potential Software and Infrastructure Vulnerabilities:

The Aspera Release Team and Security Teams (reporting to the VP Engineering/CTO) subscribe and are continuously notified by the IBM PSIRT system (http://www-03.ibm.com/security/secure-engineering/process.html) and the National Vulnerability Database (CVE) of any vulnerabilities in open source software used in the Aspera Application or Enterprise Server software. Aspera Operations implements continuous host and application log analysis that inspects the infrastructure and application logs and automatically blocks IP addresses causing suspicious activity (logins) and alerts Operations management of unusual activity or potential attacks. Alerting conditions are automatically notified by monitoring software and reviewed continuously by Aspera Operations engineers. Finally, the Aspera Operations team is also subscribed to the cloud infrastructure provider's vulnerability bulletins and responds continuously to any infrastructure concerns to protect against potential vulnerabilities or to respond to any actual vulnerabilities as described in our Incident Response.

Security Incident Response:

For any **Vulnerability that is Potentially Exploitable** in the Aspera Application or Enterprise Server Software or in services used in the Infrastructure, Aspera announces the vulnerability typically within two hours (and always within 24 hours) of discovery to the Aspera customer base using an Aspera software security bulletin (details available at https://support.asperasoft.com/hc/en-us/sections/203780098-SecurityBulletins) and as an IBM Security Bulletin. Aspera makes software updates available within 24 hours to correct the vulnerability and notifies the designated technical contacts of all Aspera Cloud services customers by email of the corrective maintenance schedule. Customers of single tenant Cloud Services may request Aspera to delay maintenance updates to a commonly agreed upon schedule. Multi-tenant Cloud Services are upgraded immediately.

For any **Vulnerability that is Not Exploitable** in Aspera Application or Enterprise Server software, an Aspera software security bulletin is published to all relevant Aspera Customers explaining how the vulnerability is not exploitable in the Aspera software. Corrective updates are pushed to production infrastructure as part of regular updates, typically occurring every 2-6 weeks

For any **Incident where Aspera Operations suspects that the Infrastructure Environment could be Compromised,** Aspera Operations immediately disconnects the production environment from public access, notifies Cloud Services Customer designated technical contacts the details of the

incident, and if deemed safe will provide the Client a backup instance of the Aspera Cloud Service on new infrastructure (typically available within 24 hours). Any risk to Customer's content will be clearly and thoroughly communicated and available to the Customers designated technical contacts and management, and any new environment set up will be deeply monitored by Aspera Operations until the Customer and Aspera are fully satisfied that no vulnerability remains.

For any **Incident where the Aspera Operations suspects the Aspera Application Environment is Compromised,** Aspera Operations immediately disconnects the production environment from public access and notifies Cloud Services Customer designated technical contacts the details of incident. If deemed safe, Aspera Operations will recreate a full clean environment for the customer and re-establish the production environment in collaboration with the Customer. Any risk to Customer's content will be clearly communicated to the Customer designated technical contacts and management. Any new environments set up will be deeply monitored by Aspera Operations until the Customer and Aspera are fully satisfied that no vulnerability remains.

Conclusion

Aspera Cloud Services are delivered with a comprehensive approach to protect Aspera Customers' content by using the rich security capabilities of the Aspera transfer platform and by following disciplined, automated, and state-of-the-art security processes. These processes secure the Application Software and the Cloud Services Infrastructure on which the software runs up to the best practices possible on the particular public cloud infrastructure, and make the highest effort to efficiently detect and correct any potential or real vulnerability in the software or infrastructure. For any questions or additional information on Aspera Cloud Services, please contact info@asperasoft.com or see www.asperasoft.com.

For more information

For more information on IBM Aspera solutions, please visit www.ibm.com/cloud/high-speed-data-transfer.

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
December 2018

Please Recycle

86014386USEN