# Release Notes: IBM Aspera High-Speed Transfer Server, High-Speed Transfer Endpoint, and Desktop Client, 4.1

Product Released: April 26, 2021
Release Notes Updated: May 6, 2021

The 4.1 release provides the new features, fixes, and other changes listed below. In particular, the *Breaking Changes* section provides important information about modifications to the product that may require you to adjust your workflow, configuration, or usage. Additional sections cover system requirements and known problems.

## NEW FEATURES

Increased security of local keystores by adding a stash file-encryption layer. (ES-1974)

Watchfolders have the ability to PULL from cluster of transfer server. (WAT-991)

Aspera Sync has new arguments. The --support-resume=[SIZE] argument enables the resume feature and optionally defines the minimum size of files to resume. The --resume-age=DAYS argument defines the number of days after which files that are older than DAYS will be removed from the temporary folder. (WAT-938)

Added support for IMDSv2 endpoints for IAM authorization with Amazon S3 storage types. (TRAP-262)

Updated default trap.properties to retry connection on timeout errors. (TRAP-228)

The API GET call to /ops/transfers will by default return ascp and ascp4 sessions. To limit the transfer sessions to a specific type, use type=ascp or type=ascp4 in the query string of the API call. (NODE-1203)

Access-key configuration now includes a file-checksum option. (NODE-1025)

Google Object Storage support in lib_cloud no longer relies on asperatrapd for object storage support. (ES-1738)

Server side encryption at rest now supports rotating secrets. Up to three secrets can be stored when using the askmscli command line tool. (ES-1637)

Added peer rate calculations for vlink local, vlink_remote in the Sender bl log line for easier interpretations of sender logs. (ATT-1453)

When receiver is a URI based path and file checksum is enabled, the receiver will validate the checksum computed by the source. (ATT-1392)

Added transfer in-out configuration setting to access key based on IP address. (NODE-1165)

Return errors from object storage interaction via asperatrapd to the ascp or ascp4 based log files. (ATT-1144)

Added I/O rate control module for URI based paths. New module will give feedback to sender to slow transfer rates when the sender is sending faster than the receiver can write. (ATT-1127)

ascp4/fasp uses AES-GCM encryption for data transfer. (ATT-1070)

Added --preserve-xattrs to ascp4. (ATT-924)

Install passwd.exe from the cygwin bundle to enable saving credentials with use of OpenSSH. (ES-1203)

Debian 10 is now supported. (ES-1911)

AES-GCM is now the default cipher. (ATT-873)

## BREAKING CHANGES

If you are upgrading from a previous release, the following changes in this release may require you to adjust your workflow, configuration, or usage.

The following platforms are no longer supported:

- Debian 7
- Fedora 26-27
- RHEL/CentOS 6
- Ubuntu 14.04 LTS, 17.10
- MacOS 10.11-10.12

HSTS HA (Redis) cluster configuration has changed. For an upgrade from 4.0 to 4.1 you must apply the aspera.conf configuration changes described in the HSTS Admin Guide (to allow for the direct recognition of the Sentinel protocol) before you run the installer to upgrade to 4.1.

Lua verification options have changed. HSTS 4.x does not recognize Lua settings from 3.x releases, and aspera.conf does not pass verification with them. Lua scripts must conform to the specifications described in the HSTS Admin Guide.

NODE-1209 - Removed HaProxy from product. When using HSTS in an HA Cluster, you now use aspera.conf options to configure Redis Sentinel communication.

ES-1992 - Azure Datalake Gen 1 Java property name prefixes have changed from dfs.adls to fs.adl in /opt/aspera/etc/trapd/adl.properties. For example: dfs.adls.oauth2.client.id changed to fs.adl.oauth2.client.id.

ES-1246 - Install includes Nginx for use as a reverse HTTPS proxy.

ES-1845 - Support for file pre- and post-processing shell scripts has been removed. Use Lua scripting functionality for pre- and post-processing scripts, the Node API to get transfer status or events, and IBM Aspera Orchestrator for more complex processing.

ES-2020 - HSTS no longer installs on RHEL/CentOS 6. HSTS only supports Red Hat/CentOS version 7 and higher.

## ISSUES FIXED IN THIS RELEASE

ES-1961 - leveldb created in root directory.

NODE-1242 - An access key POST returns exact same cipher as specified in the payload.

ATT-1543 - ascp will abort session if disk returns error "stale file handle" errno 116.

ES-2031 - Fixed issue where asperacentral was not finalizing transfer status. Resulted in Faspex servers having the wrong status on uploaded packages.

ES-1768 - Fixed an issue with asperacentral sometimes leaving zombie processes as a result of starting ascp transfers.

ES-1608 - ScpGUI will now import ssh key generated with newer ssh-keygen.

ATT-1525 - Fixed issue where management stats were not produced while waiting on writes against object storage to complete. Helps to solve cases where transfers were incorrectly marked as timed out because of lack of management messages.

ATT-1524 - Server side log location no longer revealed when there is a log failure.

ATT-1523 - User name no longer revealed on token failure.

ATT-1522 - ascp will reject using file-checksum with MD5 when FIPS mode is enabled.

ATT-1519 - Made ascp mark a failed rename of a partial file an error which results in the entire session being marked in an error state.

ATT-1455 - Improved ascp4 to report an error on bad symlinks.

ATT-1364 - Made --delete-before-transfer a bad argument when used with multi-session in ascp.

ATT-1337 - Fixed management output of the source in ascp4 when source and destination where streaming endpoints.

ATT-1336 - Fixed issue in ascp4 where stream session was not failing when there is a docroot and both endpoints are sockets.

ATT-1334 - Fixed issue in ascp4 where data was not reported with a file as a source and destination was a UDP stream.

ATT-1263 - ascp does not report a file error when a session fails due to lack of disk space.

NODE-1236 - asperanoded /ops/transfers GET does not return all files that were associated with a transfers.

NODE-1233 - asperanoded crashed when there was a self-referencing loop in the database.

ATT-1142 - Ascp --no-read and --no-write options not working with URI-based paths.

ATT-1067 - Fixed issue in ascp4 with encryption at rest (EAR) conflicting with FIPS support due to an unsupported algorithm being used for hashing data.

NODE-913 - Transfer top-level status is marked as failed after timeout even if it is still in the queue.

NODE-828 - /ops/transfers is not returning all files for a session when using count and max_files in query string.

ATT-1442 - Fixed issue with cyclical link causing ascp to hang in precalc.

ES-1944 - ascp fingerprint incompatibility between versions 3 and 4 (now documented).

ATT-1433 - ascp4 with encryption at rest (EAR) conflicting with FIPS support due to an unsupported algorithm being used for hashing data.

## SYSTEM REQUIREMENTS

**Linux 64-bit:** Ubuntu 16.04 LTS. Ubuntu 18.04 LTS. RHEL 7-8. CentOS 7-8. SUSE Linux Enterprise Server (SLES) 12. Debian 8-10. Fedora 32. Kernel 3.10 or higher and Glibc 2.17+.

**Windows:**Windows Server (64-bit) 2012, 2016, and 2019. For client use only, you may also use Windows 10 (36-bit or 64-bit).

**macOS:** 10.13 (High Sierra), 10.14 (Mojave), 10.15 (Catalina), macOS 11.0 and 11.1 (Big Sur).

**PowerLinux:** Ubuntu 16.04.2 LTS, Ubuntu 18.04 LTS. Your OS version must support little-endian (LE) ordering, and it must run on IBM Power hardware that supports LE ordering. Kernel: Linux 4.4.0-116-generic. Architecture: ppc64-le.

**zLinux:** Linux on z Systems s390, 64-bit. RHEL 7-7.3. SUSE Linux Enterprise Server (SLES) 12.

**AIX:** 7.1, 7.2.

## PRODUCT SUPPORT

For online support, go to the IBM Aspera Support site at https://www.ibm.com/mysupport/. To open a support case, log in with your IBMid or set up a new IBMid account.