Release Notes: IBM Aspera High-Speed Transfer Server, High-Speed Transfer Endpoint, and Desktop Client, 4.0

Product Release: November 17, 2020
Release Notes Updated: November 16, 2020

This release of IBM Aspera High-Speed Transfer Server (HSTS), High-Speed Transfer Endpoint (HSTE), and Desktop Client provides new features, fixes, and other changes. In particular, the *Breaking Changes* section provides important information about modifications that may require you to adjust your workflow, configuration, or usage. Other sections cover system requirements and known problems.

NEW FEATURES

- The minimum rate is now locked by default. This prevents changing the minimum rate, which often disables the automatic rate control features of the FASP protocol. (CIM-2694)
- The default installation and upgrade of HSTS and HSTE now uses a non-root user to run daemons. (CIM-2752)
- Added the new command line option --no-log=stats to async, which suppresses the logging of PROG and STATS messages in async. (CIM-2259)
- Added a delete before transfer checkbox to the ScpGUI's File Handling tab. (CIM-2510)
- Added option "Remove Skipped" to ScpGUI remove after transfer configuration options. With this checked any files that were not transferred due to destination file matching source file will be removed.
- aspera_tokenauth_rsa key is now FIPS compliant. (CIM-2152)
- Redis is now started with a systemd/init.d script on Unix platforms.
- Must update to 3.8.0 before updating to 4.0.0 if you use the Aspera High-Speed Transfer GUI (ScpGUI).
- ACL/Xattr preservation can now be set in in the ScpGUI's connection dialog. (CIM-1917)
- Clarified the overwrite options displayed in the File Handling tab of the ScpGUI's Connection dialog. (CIM-2304)
- ScpGUI uses new Node API endpoint /files/page when attempting to browse object storage file systems. This will improve listing object storage directories containing 1,000s of items.
- Keep pvcl_wm library up-to-date with each HSTS release.
- Updated jackson-databind, jsch, and httpclient java dependencies to the latest versions.
- Updated to OpenSSH version 8.4 in HSTS/HSTE for Windows. (CIM-2727)
- Streaming is now supported by the IBM Aspera Enterprise product.
- Added a checkbox for HTTPS connections in ScpGUI to disable hostname verification.
- Multiple Watchfolders can be paused/stoped/started/resumed from the ScpGUI UI.
- Updated Java components to OpenJDK 1.
- Notarized HSTS, HSTE and Desktop Client binaries for macOS. (CIM-2256)

ISSUES FIXED IN THIS RELEASE

ES-1878 - In some cases upgrades fail due to a script failure in a prior installation of HSTS or HSTE. If you see an error with the preun script, then remove the prior package by passing the --nopreun argument to the rpm command. (none)

ES-1833 - Transfers will not start from the GUI if the password includes special characters.

ES-1833 - Transfers will not start from the GUI if the password includes special characters.

ES-1824 - On new installations the default target rate is set to 510 Mbps.

ES-1758 - Updates Windows API calls to NetGetUserInfo to use USER_INFO_4 data structure to fix issues get user details on some Windows Domain controllers.

ES-1682 - Fixed issue with asperalee daemon where it was not able to startup due to an issue with the db.mv.db file. (CIM-3127)

ES-1644 - Fixed an issue for asperacentral, when it did not start any more transfers when a RemoteLocation was not specified in a submission. (CIM-3390)

ES-1643 - ScpGUI only writes its log in text and not HTML.

ES-1513 - Fixed issue where ALEE failed to start because of a permissions issue when attempting to save internal files to root of filesystem.

ES-1450 - Fixed an issue for services files for systemd on Unix systems that did not preserve user modifications on upgrade. (CIM-2702)

ATT-1439 - Fixed issue in ascp4 to allow for -E exclude option to work with delete-before-transfer option.

ATT-1417 - Fixed issue with ascp4 not reporting errors when there is a failure to create a directory and the -d option is specified on the command line.

ES-1417 - Fixed issue in Hot Folders on Windows to the handle case in which there is a trailing slash on a source path and the move-after-transfer option is being specified. (CIM-2663)

ATT-1400 - Fixed issues with ascp4 exclusions with file-lists.

ATT-1387 - Fixed issue with astrap-config.sh script where required ENABLE/DISABLE to be upper case. Will accept upper or lower case now.

ATT-1384 - Fixed issues with --delete-before-transfer removing internal temporary ascp destination files causing resume transfers to transfer the entire file rather than continuing from the last data transferred.

ES-1371 - Improved error reporting with expired tokens and incorrect source paths. ascp will only report an error with an expired token, and it will not report an error about a source path. (CIM-2539)

ATT-1370 - Allow for the -E exclude option to be used with the --delete-before-transfer option to ascp.

ATT-1352 - ascp4 will return error code 1 if there is a license failure.

ATT-1349 - Fixed issue with ascp4 and process uris in the docroot path configuration.

ES-1329 - Improved the handling of tags to allow for a maximum size of any value to 1 KB. The maximum size of the tags argument is 4 KB. (CIM-2346)

ATT-1320 - Fixed issue with ascp4 where it failed to process a file-list file if the file had an empty line as the last file in the file.

ES-1317 - Corrected HSTS documentation for redis.conf.

ATT-1316 - ascp4 now supports the -E exclude argument.

ATT-1298 - Allowed ascp4 to make use of the <logging> directive in aspera.conf.

ES-1295 - Updated documentation to specify that entitlement licensing is only possible with HSTS. (CIM-2243)

ES-1285 - Permissions of node_id.conf and cluster_id.conf files are now more restrictive. (CIM-2209)

ATT-1270 - ascp4 will now support server side encryption at rest if configured in an access key configuration.

ATT-1243 - Added a timeout to the SSH handshake used by the ssh client library in ascp. This will help resolve issues where an initial TCP connection is made to a server, but the client never receives an SSH banner response. (CIM-3223)

ATT-1241 - Fixed ascp4 issue in which the --preserve-creation-time argument was not handled properly. (CIM-3333)

ATT-1240 - ascp4 can now use the "copy+force" option for symbolic links which will allow for ascp4 to overwrite destination symbolic links with the contents of the source symbolic link. (CIM-3332)

ATT-1236 - ascp4 now has the ability to preserve the user_id and group_id on symbolic links on Unix platforms. (CIM-3323)

ES-1220 - ascp can use ssh-agent to connect to remote servers via ssh.

ES-1208 - Improved ascp4's ability to recognize when a receiver's disk is full and will give an appropriate error message. (CIM-1950)

ES-1207 - Improved ascp4 use of tokens generated by the Node API's upload_setup and download_setup API calls. (CIM-1960)

ATT-1199 - ascp4 is now prevented from using multiple read/write threads for streaming, to avoid potential size or md5 mismatches.

ATT-1186 - ascp (sender) accepts a folder path for stdio-tar based download.

ES-1183 - The `<chunker_max_mem>` configuration element is provided for situations in which you have a high transfer rate, a significantly lossy or slow network between the sender and receiver, are sending large files (in the Gigabyte range), and the sending host does not have a generous amount of RAM to spare. The `<chunker_max_mem>` element limits the amount of memory (defined in bytes) that the sender will use to hold on to data that has yet to be acknowledged by the receiver. This means that the sender will temporarily stop reading data that it will send as for as long as that limit is reached. (CIM-1702)

ES-1182 - Improved the use of Lua scripting to allow scripts to be run as session start, session stop, file start and file stop. (CIM-1880)

NODE-1169 - Added an Accept-version to allowed headers in the Node API for CORS.

ATT-1164 - Now allow include/exclusion of files in the aspera.conf of HSTS or HSTE. This allows administrator to define rules to allow or deny specific types of incoming files. (CIM-1776)

NODE-1130 - Added support for different cipher options in POST to /ops/transfers for ascp4.

NODE-1113 - ascp4 Gen3 transfer with AK fails to initiate when authenticating with aspera_tokenauth_id_rsa keypair.

ATT-1111 - Fixed issue with ascp4 reporting network bytes rather than file bytes when using tcp or udp endpoints and usage licensing is enabled.

ATT-1105 - Improved HA Redis and sentinel documentation. (CIM-2891)

NODE-1096 - Fixed issue with ascp4 to allow the Node API to specify an ssh_private_key in the payload to /ops/transfers to allow ascp4 to initiate an ssh transfer using the private key.

NODE-1092 - Fixed an issue where an ascp client could transfer to the wrong folder when using a sub-access key for authorization.

NODE-1091 - Node API changed it return values for auth_types for the /ops/transfers GET request. The returned values are now. bearer_token basic_token auth_token access_key_auth_token

ATT-1085 - Added error code to err logging in ascp4 when there is a failure with a sparse file. (CIM-2790)

NODE-1085 - Fixed issue in Node API GET /ops/transfers response where a cancelled transfer still had a "transferring" status in the files section.

ATT-1083 - Gave ascp the ability to report file-checksum when using multi-session as long as multi-session-threshold=0.

NODE-1078 - Fixed issue in Node API where an access key could not be created if it had a UNC path (\\server\path\)

ATT-1029 - Added the command line argument to ascp --fail-bad-pass that causes ascp to fail its transfer session if an incorrect passpharse is given to files protected by client side encryption at rest.

WAT-1004 - Fixed a very specific issue in the async shutdown process where under unique conditions async would enter a deadlock resulting in an async session never completing until it was forced quit. (TS004214524)

NODE-1002 - Fixed issue in asperanoded to allow it to reconnect to Redis. This resolves an issue with the HA implementation that occurred when there was a failover that required asperanoded to make a new TCP connection to Redis.

ATT-999 - Added --keepalive to the hidden help (-hh) of ascp4. (CIM-2410)

NODE-982 - Improved asperanoded handling of errors codes from ALEE to help support newer backend systems API with different return codes.

ATT-982 - Fixed issue with ascp4 on Windows where docroots can now be specified with backslahes or forward slashes.

WAT-979 - Fixed issue in async where Unix file permissions were not synced after a reset of the snap.db database and a source file mode was changed.

WAT-973 - Fixed issues in Hot Folder configuration dialog where enable/disable checkboxes did not always register changes in sync-conf.xml file.

WAT-972 - Improved watchfolder logging configuration to be able to set watchfolder logger per user as seen in aspera.conf. (CIM-3382)

WAT-971 - asperawatchfolder can now use restrictions without a docroot to give administrators the ability to watch multiple directories within a UNC mount, on Windows operating systems. (CIM-3394)

WAT-963 - Fixed issue in ScpGUI where a NULL Pointer Exception would not allow for a watchfolder to be edited through the GUI. (CIM-3180)

NODE-957 - Improved memory usage with the Node API upload/download_setup endpoints.

WAT-951 - Transfers initiated with watchfolderd now pass dsa and rsa based ssh keys when interacting with older HSTS instances that have dsa based ssh keys enabled. (CIM-3019)

NODE-946 - Fixed issues in asperanoded in which management messages were mishandled.

WAT-926 - When async is running in continuous mode it will not retry files that no longer exist on disk.

WAT-925 - Fixed issue when async encountered a parent directory that was not found in the snap.db database.

ATT-887 - macOS clients now properly log UDP recv got "Network is unreachable" rather than "unrecognized error". (CIM-2167)

WAT-881 - Updated aswatchfolderadmin man pages to be more accurate.

WAT-879 - async now provides a better error message when it cannot change the permissions mode of a directory. (CIM-2020)

ATT-874 - Improved checking of NAT64 IPv6 networks with SSH connections to allow for ascp transfers to work correctly on these networks. (CIM-1673)

NODE-851 - Fixed issue in Node API where upload_setup or download_setup endpoint failed to create a transfer spec if a directory contained multiple . (dot) characters in a row. (CIM-2198)

ATT-829 - When using client-based encryption at rest, ascp now has the ability to resume uploads that were interrupted. Before this fix ascp would always upload from offset 0. (CIM-1980)

ATT-813 - ascp4 now writes an error to the management stream when it encounters an error writing a file to disk. This will allow applications like Console to be able to report session errors. (CIM-1902)

ATT-762 - Improved transfer reporting of ascp4 with the /ops/transfers endpoint.

NODE-988 - Added a new /files/page endpoint to the Node API to allow for paged browsing through directory lists. This is especially helpful when listing contents of object storage directories. The new endpoint will be used by ScpGUI to help display results of large directories view on object storage.

ATT-1059 - Fixed issue in ascp where certain combination of arguments and missing directories made ascp bypass the mkdir permissions.

NODE-1108 - Changed the Node API to be able to accept files posted to the files/id endpoint to be greater than 4KB.

NODE-1183 - A sub-access_key can access file_ids outside of its directory structure if, and only if, the top-level directory's path relative to the master access_key's storage_root starts with the same exact characters as the root_file_id's path.

SYSTEM REQUIREMENTS

Linux 64-bit:
Ubuntu 14.04 LTS, 16.04 LTS, 17.10. RHEL 6-8. CentOS 7-8. SLES 11-12. Debian 7-9. Fedora 26-27. Kernel 2.4 or higher and Glibc 2.5+
PowerLinux:
Ubuntu 16.04.2 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. Red Hat Enterprise Linux Server (RHEL) 6-7.3. SUSE Linux Enterprise Server (SLES) 11-12

Windows 64-bit:
Windows Server 2012, 2016, and 2019.

macOS: OS X 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.13 (High Sierra), macOS 10.14 (Mojave), macOS 10.15 (Catalina).

AIX: 7.1, 7.2.

KNOWN ISSUES

ATT-185 - ascp does not reconnect to Redis db when asperanoded is restarted.

NODE-857 - sconfigurator can set a negative value for activity_files_max.

NODE-906 - Fixed issue in Node API post to /ops/transfers where an incorrect value for the multi_session parameter caused problems.

ES-1194 - asconfigurator should not display !?! for non-translated fields.

ES-1453 - The nft firewall on CentOS 8 causes problems with incoming udp data. Must set the a firewall rule similar to:

```
#nft insert rule inet firewalld filter_IN_public_allow position 67 udp dport 33001 accept
```

To allow incoming udp traffic on the default udp port 33001.

ES-1534 - asperacentral reports a job_id with each transfer session reported.

ES-1844 - The ScpGUI's demo.asperasoft.com server might have authentication issues. Use the password "demoaspera" if there is a problem connecting.

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:
  - CentOS 6
  - Isilon
  - Solaris SPARC
  - Solaris x86
- The HST Server Web UI (Connect Server) is no longer supported.
- Added feature to asperanoded to be able to recognize Redis sentinel commands for automatic failover in HA redis configurations.
- Use askms to secure sensitive data in watchfolder configuration.

- Fixed file reporting issue in ascp4, when source files have illegal characters like \ in the names, ascp4 will generate an appropriate error message to management to allow for integrated applications to be able to report on the file errors.
- Node API will return transfer ciphers with cfb or gcm depending on the cipher being used.
- On Windows OS as of 3.7.4, updates to the Cygwin OpenSSH implementation that is used by High-Speed Transfer Server and High-Speed Transfer Endpoint cause transfers to error when: - the OpenSSH service is run by an Active Directory domain user, and - the transfer user is a different Active Directory domain user who has a docroot on a CIFS or SMB share. In this case, the transfer user cannot use SSH key authentication for uploads or downloads because they do not get the proper credentials to access the mounted storage. Workaround: Open a command prompt as an administrator and run the following command: > C:\Program Files\Aspera\Enterprise Server\bin\passwd.exe -R domain\username Where domain is the Active Directory domain and username is the transfer user's username. Then add the transfer user as a Remote Desktop user. Additionally you may configure HTTPS session initialization which can access Windows Credential Manager to be able to login users and allow for access to SMB/CIFS mounts in their transfer sessions. (CIM-1239)
- watchfolder Redis configuration must be set in the aspera.conf and in the aspera_redis.31415 file in order to access redis databases hosted on different servers.
- The file pre- and post-processing script support has been deprecated. Support will be removed in a future release.
- ASPERA_SCP_PASSWORD environment variable will only be used as a ssh key passphrase if the -i (ssh key) argument is used with ascp. If there is no -i argument, the ASPERA_SCP_PASSWORD will only be used as the ssh user password.
- The alee-admin tool can now be run only as the root user (or with the sudo command).
- ascp uses a newer version of libssh2, which makes use of new ssh host keys. If you have host key checking enabled, you should update your aspera.conf to use the newer host key.

OTHER CHANGES

The "File Pre- and Post-Processing (Prepost)" feature is deprecated, and will be removed with a future release.

Streaming capabilities are only provided with the IBM Aspera Enterprise and IBM Aspera Endpoint products. Streaming is not provided with, or supported by, the HSTS and HSTE standalone products.

PREVIOUS RELEASE NOTES

For release note for earlier releases, see the IBM Knowledge Center.

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.