Release Notes: IBM Aspera HSTS, HSTE, and Desktop Client 3.9.1 for Linux, Windows, and MacOS

Product Release: December 18, 2018
Release Notes Updated: April 8, 2019

This release of IBM Aspera High-Speed Transfer Server, High-Speed Transfer Endpoint, and Desktop Client provides the new features, breaking changes, and other changes listed below. Additional sections cover system requirements and known problems.

WHAT'S NEW (LINUX)

Release 3.9.1 is an update of IBM Aspera High-Speed Transfer Server, High-Speed Transfer Endpoint, and Desktop Client. It provides the new features, fixes, and other changes listed below for Linux since release 3.9.0.

NEW FEATURES

For more information about the new features in this release, see "What's New" in the guides.

Watch Folders and Aspera Watch Service

- You can now use the API to pause a specific Watch Folder.

  Note: When starting a stopped Watch Folder that had a large number of files added while it was stopped, expect a delay and high CPU utilization while Watch Folders rebuilds the file source tree.

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 `sshd_config` file no longer accepts the `ssh-dss` (DSA) public key algorithm. Customers using DSA keys should use RSA keys instead.

DEPRECATION NOTICES

- The "File Pre- and Post-Processing (Prepost)" feature will be deprecated from HST Server and HST Endpoint in versions 4.0 and onward. At that time, customers should use Inline File validation with Lua or an External URL validator for pre-post processing features. For more information on those features, see the *IBM Aspera High Speed Transfer Server Admin Guide*.

DOCUMENTATION UPDATES

Corrected Async `--transfer-threads` option example to use only numeric values in bytes. (CIM-1973)

ISSUES FIXED IN THIS RELEASE

ATT-804 - Ascp crashes in multi-session mode if it tries to copy a symlink.

Ascp crashes when `lua_file_delete` is called in a script.

In some translated versions of the GUI, when canceling the installation process, the cancel confirmation panel is truncated.

Async fails to start while checking the entitlement if the redis database is on a remote host.

WAT-870 - Watch Folders continues to catch changes in subdirectories of a directory which has been moved outside the watched directory.

WAT-869 - When a directory is removed from a watched source directory, the Watch Folder errors and fails to remove the directory from the internal data model, continuing to consuming memory.

WAT-868 - Watch Folders fail to monitor directories with non-ascii chars in the name.

WAT-865 - Watch Folders do not automatically handle server time changes. (CIM-1818)

WHAT'S NEW (Windows and MacOS)

Release 3.9.1 is an update of IBM Aspera High-Speed Transfer Server, High-Speed Transfer Endpoint, and Desktop Client. It provides the new features, fixes, and other changes listed below for Windows and MacOS since release 3.8.1.

NEW FEATURES

For more information about the new features in this release, see "What's New" in the guides.

General

- The products are completely converted to new names; Enterprise Server and Connect Server are now "IBM Aspera High-Speed Transfer Server", Point-to-Point Client is now "IBM Aspera High-Speed Transfer Endpoint", and Desktop Client is now "IBM Aspera Desktop Client". These changes affect installer package names, the GUI, and the display names and descriptions of Aspera services, but not the default paths to Aspera application files.
- A new AES-GCM encryption mode (AES-128-GCM, AES-192-GCM, and AES-256-GCM) offers significantly faster encryption, decryption, and transfer compared to the legacy AES encryption mode, as well as built-in data authentication and FIPS 140-2 compliance. These encryption ciphers can be configured on the server, set in access keys, and requested by the client, including transfers started with ascp, the GUI, Hot Folders (for Windows), Aspera Sync, Watch Folders, and the Node API. Ciphers are reported to management without the suffix.

  Note: Both the client and server must be version 3.9.0 to use AES-GCM, otherwise transfers are refused by the server. To ensure backwards compatibility, set the server to "any" (default) or AES-128, AES-192, or AES-256, and allow the client to request GCM (client must be version 3.9.0).
- An experimental rate control module based on loss-adjusted queueing (LAQ) is now available as a Beta feature. While it has not been exercised in a large-scale production environment, preliminary testing indicates that it rapidly corrects for overdrive conditions when the target rate exceeds available network bandwidth, reducing packet loss and increasing transfer performance.
- JRE upgraded to 8u181 to support strong ciphers. For a highly secure environment, Aspera recommends installing HST Server or Endpoint behind an Nginx proxy that is configured to use strong SSL ciphers (see https://cipherli.st/ for an example). (CIM-1694)
- A cluster of three or more HST Servers can now be configured to use a highly available Redis backend (database) that provides continuous availability and automatic failover. HST Server uses Redis tools and HAProxy (the Redis load balancer tool) to direct Redis requests from the HST Servers to the primary Redis database. If the primary is reported as failing, a replica is automatically promoted.

ascp

- IBM Spectrum Scale (formerly GPFS) NFSv4 ACLs are now preserved by `--preserve-xattrs` and `--remote-preserve-xattrs`.
- Expanded transfer testing capabilities now allow you to specify a faux directory and configure the files that it contains.

Ascp4

- The new `--check-sshfp` argument increases Ascp 4 security by verifying the server's SSH fingerprint before transfer.

Node API

- The Node API /access_keys endpoint no longer supports modifying the content protection secret value in an access key configuration. If you must change the content protection secret, create new access keys with the updated secret. This change makes it more difficult to upload encrypted content to the server with one secret and then download the file and create incorrect file content when it is decrypted with the new secret.
- Access keys can be configured report to the IBM Aspera on Cloud Analytics application. The access key setting overrides the setting on the server.
- The output of a GET request to /files/{id}/files that is sorted by name is now insensitive to case.
- There is faster transfer startup when many transfer sessions are started through the Node API. (CIM-1010)

Watch Folders and Aspera Watch Service

- You can now use the API to pause a specific Watch Folder.

  Note: When starting a stopped Watch Folder that had a large number of files added while it was stopped, expect a delay and high CPU utilization while Watch Folders rebuilds the file source tree.
- Pull Watch Folders no longer require that the remote Watch Service run under the "xfer" domain. Now Watch Folders uses the system user that is associated with the Node API user or access key that is used to authenticate to the remote server. Watch Folders that use the xfer domain are still supported.
- Faster file system scans by the Aspera Watch Service (watchd) by using multiple threads to scan in parallel. The number of threads can be configured with the new `<scan_threads>` option in the `watchd` section of `aspera.conf`.
- When the password of a system user who runs Watch and Watch Folder services changes, you can now update the password for the services by changing the password for one service, and after restarting the Aspera Run Service (asperarund) the change is propagated through all services run by that user. In the GUI, click the services & policies icon, select a service that is run by the user, edit the service and update the password. From the command line, update the Watch Folder configuration with a PUT request to /v3/watchfolders. Restart the Aspera Run Service (asperarund) to activate your change.

Sync

- IBM Spectrum Scale (formerly GPFS) NFSv4 ACLs are now preserved by `--preserve-xattrs` and `--remote-preserve-xattrs`.
- Sync now respects the `files_filelock_enabled` setting in a user's access key, which overrides the server setting in `aspera.conf`.
- Sync now applies `--transfer-threads` arguments in pull mode as well as push mode.
- Dramatically faster synchronization with cloud storage through more efficient file monitoring and multi-threaded transfer handling. New command line options, `--local-fs-threads` and `--remote-fs-threads`, can be used to increase the number of threads for file system operations on the local and remote computers.
- As of version 3.9.0, Aspera Sync transfers start faster because Sync no longer automatically retrieves information about the files (with a file stat) at the start of a session. Performance is particularly improved object storage and storage mounts. To enforce the previous behavior, use `--local-force-stat` or `--remote-force-stat`. (See also Breaking Changes).
- A new Sync option `--clean-excluded` can be used to optimize the Sync snapshot database when using `--exclude-dirs-older-than` or `--exclude` by removing directories from the snapshot as they become excluded. The option applies to all Sync directions and the excluded paths are removed from the snapshot database on both endpoints.
- Continuous synchronization is now supported for macOS file sources.
- The `--preserve-acl` and `--preserve-xattrs` options now synchronize changes to file or directory ACLs when the file or directory is otherwise unmodified.

Object Storage Support

- Faster uploads to large virtual machines in cloud storage by increasing the default number of transfer threads to a maximum of 50. Job threads and the threshold definitions of "large" virtual machines are configurable in `trap.properties`.

OTHER CHANGES

- For security reasons, the token is no longer reported in the file manifest or management output, which might affect some SDK integrations.
- The `asnodeadmin` option `--key-file-path` has been removed. The key file must now be in the Aspera `etc` folder.

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 `sshd_config` file no longer accepts the `ssh-dss` (DSA) public key algorithm. Customers using DSA keys should use RSA keys instead.
- Ascp transfers now fail if the `--tags` or `--tags64` argument exceeds 4 Kb. Previously, the transfer succeeded but the tags were truncated to 4 Kb.
- Access keys for the Aspera on Cloud transfer service (formerly ATS) can no longer be managed in the HSTS, HSTE, or Desktop Client GUI. Instead, use the Aspera on Cloud UI (see https://ibm.ibmaspera.com/helpcenter/admin/nodes/creating-a-new-transfer-service-node) or the ATS API.
- As of version 3.9.0, Aspera Sync transfers start faster because Sync no longer automatically retrieves information about the files (with a file stat) at the start of a session. To run Sync with the previous behavior, use `--local-force-stat` when the local computer is the source, `--remote-force-stat` when the remote computer is the source, or both options for bidirectional synchronization.

DOCUMENTATION UPDATES

- Documented how to address a temporary connectivity issue between the `asperanoded` service and the `asperalee` service by configuring `asperanoded` to depend on `asperalee` to start. (CIM-1874)
- Corrected Async `--transfer-threads` option example to use only numeric values in bytes. (CIM-1973)
- Updated product names. Enterprise Server and Connect Server are now High-Speed Transfer Server, and Point-to-Point Client is now High-Speed Transfer Endpoint.
- "Server Logging Configuration for Ascp and Ascp 4" now includes how to configure logging from the command line with `asconfigurator` commands.
- Instructions for setting filters on Ascp and Watch Folders sources now specify that an include rule must be followed by at least one exclude rule, otherwise all files are transferred. (CIM-1615) Ascp, Sync, and Watch Folders filtering instructions updated and corrected.
- The system requirements and instructions for configuring the HST Server web UI are updated for Apache 2.4 (older Apache versions are no longer maintained and should be upgraded).
- The instructions for changing the TCP port for HST Server and HST Endpoint no longer include the "adjustment phase" setup when both TCP/22 and TCP/33001 are open. They now describe how to switch directly from TCP/22 to TCP/33001. (CIM-1689)

DEPRECATION NOTICES

- The "File Pre- and Post-Processing (Prepost)" feature will be deprecated from HST Server and HST Endpoint in versions 4.0 and onward. At that time, customers should use Inline File validation with Lua or an External URL validator for pre-post processing features. For more information on those features, see the *IBM Aspera High Speed Transfer Server Admin Guide*.

ISSUES FIXED IN THIS RELEASE

ATT-804 - ascp crashes in multi-session mode if it tries to copy a symlink.

ATT-765 - Hotfolder with "Automatically delete source files after transfer" setting does not delete transferred files from the source . (CIM-1749)

ATT-709 - Ascp does not stop gracefully when the value for `--file-checksum` is invalid.

ATT-580 - If a server has server-side encryption-at-rest enabled, when a file is uploaded to the server then modified at the source and uploaded again, that file cannot be downloaded from the server and returns error code 27 with the error "Other session error". (CIM-1209)

ATT-531 - When the destination of an `ascp` transfer is a symbolic link that is a relative path to a file (not a directory) and a partial file name suffix is configured on the receiver, the file is transferred into the user's home directory and the symbolic link target is not overwritten.

ATT-451 - Ascp 4 does not respect exclude filters if the file path is specified in the command line.

ATT-395 - When running a persistent `ascp` session, a FaspManager FILEERROR message truncates a filename that is longer than 128 characters to only the first 128 characters.

ATT-360 and NODE-545 - Directory timestamps are not always preserved on the destination during an `ascp` transfer that uses `-p`.

ATT-537 - Downloads that use `ascp --overwrite=always` fail when they are authenticated using ASPERA_LOCAL_TOKEN that specifies a local storage path.

ATT-485 - Persistent session Ascp 4 downloads from object storage do not report a STOP message to management after the transfer completes.

ATT-243 - [Windows] If the Aspera product is installed on Windows, filepaths for source and destination files are limited to 520 characters, even if the remote machine is running a non-Windows operating system. With the fix, Windows paths can now be 4096 characters.

ES-1152 - [Foreign OS] When canceling the installation process, the cancel confirmation panel is truncated.

ES-934, ES-903, ES-846 - As of 3.8.0, some settings in the GUI are not displayed properly, particularly for non-English languages. The setting names are preceded by "!?!" or are blank.

ES-819 - GID is not preserved for files that are transferred using HTTP fallback. (CIM-1382)

ES-742 - As of 3.8.0, some translated versions of the GUI have empty field names for configuration settings.

ES-792 - Very rarely when file checksum reporting is enabled, Ascp uploads to IBM Cloud might fail to close even after all data is successfully transferred.

ES-780 - Renaming files and directories on the server through the GUI errors with the message "Path outside docroot" if the transfer user has a docroot with the format `file:////dir_name`. (CIM-1258)

ES-694 - As of 3.8.0, when you upgrade Connect Server that uses a locally-hosted Connect SDK, the new installation must be manually configured to use the locally-hosted Connect SDK.

ES-675 - As of 3.7.4, in the rare case when a transfer fails with a "Session open failed" error, the status is not updated in the Aspera Central database from "running". As a result, Console continues to report the session as "RUNNING" until the entry in the central database is manually deleted or updated to "ERROR". (CIM-1072)

ES-626 - As of 3.8.0, `ascp` truncates JSON tags if the tags exceed 4 Kb. With this fix, tag length is checked before the transfer is started and an error is returned if the tags exceed 4 Kb.

ES-526 - As of 3.8.0, some translated versions of the GUI have "!?!" in front of labels that are not translated from English.

ES-323 - When doing a dry run of an `asdelete` (by using the `-d` option), the log shows all the files that were scanned, not the files that would be deleted by the `asdelete` command. (CIM-558)

ES-267 - Under rare conditions, `ascp` transfers to cloud object storage may be reported as successful even though Trapd reports an error and the content is not in the storage. (CIM-475)

ES-98 (#34674) - When Japanese language is set in the GUI, the application doesn't respect `aspera.conf` settings; all docroot settings are set to false, and the other settings fail with attached Japanese errors.

NODE-778 - When a Watch Folder is created using `NODE_BASIC` authentication and encryption enabled, the cipher type `AES128` is always applied, regardless of what is in the Watch Folder configuration.

NODE-742 - As of 3.8.0, downloading with Ascp fails when the access key that is used to authenticate to the server does not have `"content_protection_secret"` set, but the access key that is used to authenticate to the client (set with the ASPERA_LOCAL_TOKEN environment variable) does have `"content_protection_secret"` set. With the fix, if either (local or remote) access key has `"content_protection_secret"` set, the content is encrypted and decrypted using the secret in the access key. If both access keys have `"content_protection_secret"` set, each side (local and remote) does its own encryption and decryption.

NODE-726 - Reloading the Aspera Node service does not reload all settings, which can cause the license information to become outdated and transfers to fail. (CIM-1643) **Workaround:** Restart the Aspera Node service. Transfers that were started through the Node API might fail during the restart.

NODE-700 - The Aspera NodeD service returns an error and then stops when the body of a POST request to /files/{id} endpoints contains an invalid value.

NODE-698 - GET requests to /files/{id} return duplicate entries for symbolic links.

NODE-687 - Requests to /files/browse that are started by the Aspera Watch Service are very slow and require high CPU for large directories.

NODE-686 - GET requests to /files/{id} return duplicate file entries for files with mixed-case file names (for example, aspera.txt is not duplicated, Aspera.txt is duplicated).

NODE-553 - The "proxy" value in POST requests to /ops/transfers is not passed on to the Ascp session.

NODE-442 - Requests to /ops/transfers can return a value of "null" for `files_failed`, which can prevent transfers from being displayed in Console. (CIM-864)

TRAP-126 - [Azure Data Lake Storage] When setting the docroot for a server in ADLS, special characters in query values are incorrectly processed by Trapd.

TRAP-123 - [S3-compatible storage] Custom ports that are specified in the URI docroot are not respected. For example, if the docroot is `s3://s3.xyz.ingest.xyz.net:9090/staging`, port 9090 is not respected.

WAT-870 - Watch Folders continues to catch changes in subdirectories of a directory which has been moved outside the watched directory.

WAT-869 - When a directory is removed from a watched source directory, Watch Folder errors and fails to remove the directory from the internal data model, continuing to consuming memory.

WAT-865 - Watch Folder does not automatically handle server time changes. (CIM-1818)

WAT-830, WAT-465 - Sync does not close during shutdown following a TCP impairment that produces a libssh2 timeout or error.

WAT-828 - Files might be incorrectly skipped by Watch Folders when the ascp session receives a large number of files in one drop.

WAT-826 - The default database that is used by `asrun` is `redis:localhost:31415` and not the value for `db_spec` in the `rund` section of `aspera.conf`.

WAT-821 - During a continuous Sync session to cloud storage, when a directory is renamed while a file in that directory is being transferred, Sync reports a conflict.

WAT-818 - `aswatchadmin` always uses `redis:localhost:31415` and not the value for `db_spec` in the `watchd` section of `aspera.conf`.

WAT-814 - Watchd can timeout when under heavy loads, such as when scanning for multiple Watch Folders in large file systems.

WAT-812 - A pull Watch Folder becomes inactive when the remote Watch service hangs and cannot recover because the Watch service does not have a timeout.

WAT-810 - As of 3.8.1, when a Watch Folder is configured to pull from cloud storage, the Watchd service that is associated with it can crash under heavy transfer loads.

WAT-808 - A file can be marked as in conflict when Sync is run in non-continuous, bidirectional mode with preserve timestamps (`-t` or `--preserve-time`) enabled and the timestamp is changed on the remote server.

WAT-768 /ES-455 - A continuous Sync session might log several error messages stating "add watch failed" because it tries to access the service when one is already in use. This issue does not affect file synchronization. (CIM-806)

WAT-742 - When filelocks are enabled on the server and a push or bidi Sync session is run with basic token authentication, a local file deletion is not propagated to the server.

WAT-737 - Sync can hang on a fatal error, such as if the disk with the Sync database runs out of space, rather than aborting the session. (CIM-1075)

WAT-644 - If the local directory to synchronize is a symbolic link, the Sync session succeeds the first time but then fails the second time with the error, "ERROR: Error reading from peer (disconnected)". (CIM-897)

WAT-573 - Under rare conditions, Sync crashes after reporting the error message, "ERROR: Failed to reconcile with peer snap db".

WAT-550 (#29686) - A continuous Sync push to S3 storage does not update the object in S3 when the source file is renamed or deleted while it is transferred.

SYSTEM REQUIREMENTS

Enterprise Server, Connect Server, Point-to-Point Client, and Desktop Client

- **Linux 64-bit**: Ubuntu 14.04 LTS, 16.04 LTS, 17.10; RHEL 6-7; CentOS 6-7; SLES 11-12; Debian 7-9; Fedora 26-27; Kernel 2.4 or higher and Glibc 2.5+
- **Windows 64-bit**: Windows 7 with service pack 1, 8.1, 10, or Windows Server 2008 R2 with service pack 2, 2012 R2, 2016
- **Mac**: OS X 10.11, macOS 10.12 (Sierra), 10.13 (High Sierra)

Client Browsers for High-Speed Transfer Server UI

- Linux: Chrome 64-71, Firefox 58-64, Firefox ESR 52-60
- Windows: Chrome 64-71, Microsoft Edge 41-44, Internet Explorer 11, Firefox 58-64, Firefox ESR 52-60
- macOS: Chrome 64-71, Firefox 58-64, Safari 11-12, Firefox ESR 52-60

KNOWN ISSUES

Note: This release contains tickets that were created from different issue-tracking systems. For this reason, the list below uses two different formats for issue numbers.

General

ATT-245 (#22726) - Successful transfers might log the error, `Failure Event: -34 - libssh2_channel_wait_closed() invoked when channel is not in EOF state`, particularly downloads in FIPS mode. The error can be safely ignored. (CIM-329)

ATT-107 - The file count that is reported in the GUI under session statistics is incorrect when the user has an exclude filter.

ES-1088 - Folders that are symbolic links cannot be directly downloaded (the directory set as the source) by using HTTP fallback. Folders that are symbolic links are processed correctly when their parent folder is the source. (CIM-1679)

ES-1061 - Opening the Aspera logs from the GUI (**Tools > View Log**) does not work unless the macOS Console utility is already running.

ES-1040 - Support for ECDSA-type SSH keys is deprecated in OpenSSH 7.0 and some operating systems require that ECDSA keys are passphrase-protected. **Workaround:** To use ECDSA keys, edit the `sshd_config` file.

ES-1031 - Some text and images in the GUI are truncated when the display uses high (>175%) DPI.

ES-793 - If an HTTP connection cannot be established or errors for another reason, HTTP fallback transfers can take 3 minutes or longer to stop and report the error.

ES-780 - Renaming files and directories on the server through the GUI errors with the message "Path outside docroot" if the transfer user has a docroot with the format `file:///dir_name`. (CIM-1258)

ES-779 - When IBM Aspera Faspex is run with High-Speed Transfer Server version 3.8.0, if a package is created from a remote source with "enable linking" selected and the package is a symbolic link, then the package size that is reported is the size of the symbolic link, not the symbolic link's target. (CIM-1267)

ES-664 - As of 3.7.4, `asconfigurator` no longer returns a warning to reload the Aspera Central service in order to activate a change in the server's configuration. (CIM-1037)

ES-610 - The Connect Server web UI displays duplicate headers and does not display symbolic link files if a symbolic link in the same directory is broken. **Workaround:** Correct the broken symbolic link and all files and symbolic links are shown correctly.

ES-526 - Some translated versions of the GUI have "!?!" in front of labels that are not translated from English.

ES-357 - If the user language is set to Spanish (`user.language=es` in `aspera.prop`) and global configuration settings are changed in the GUI (**Configuration > Global**), the GUI displays the default values after it is restarted even though the updated settings are saved in `aspera.conf`. (CIM-638)

ES-249 - The aggressiveness setting is applied to Vlinks, rather than only the network rate controller. (CIM-399)

ES-248 - While an `ascp` or `ascp4` transfer of many files is in progress, skipped files are reported as complete. The counters are correct once the entire session is complete. (CIM-398)

ES-216/ASCN-705 - If the Aspera Connect is unable to connect to the server through SSH, a misleading error message, "Failed to authenticate," is reported rather than indicating that it is a connection problem. (CIM-72)

ES-215 - If Aspera Connect is unable to connect to the server by SSH, HTTP fallback is attempted but only after a 15 minute delay. (CIM-320)

ES-166 - To set a combination of symbolic links actions besides the default, `aspera.conf` must be manually edited. Selecting **any combination of the above delimited by commas** in the GUI sets that invalid text string as the value.

ES-42 - When you retrieve the entitlement status by using `alee-admin status`, confusing error messages are returned even if the entitlement was registered successfully.

#35952 - `asunprotect` cannot decrypt a re-protected file.

#34811 - You are unable to download encrypted files with an incorrect decryption passphrase when you are using HTTP fallback.

#32934 - If the Internet accountability software Covenant Eyes is installed, some HTTP fallback transfers appear to complete but then lose connection with the server and then attempt to re-transfer. Covenant Eyes captures the entire HTTP transmission before forwarding it to the server. If the file is so large that this process takes longer than about 20 seconds, the server times out and cancels the session. **Workaround:** Reduce the probability of timeout by increasing the server timeout length. Set `Session Activity Timeout` in `aspera.conf` by running the following command:

```
$> asconfigurator -x "http_server;session_activity_timeout,time_in_seconds"
```

#32517 - Retransfer requests are unencrypted when transfers are encrypted. This change in encryption can cause transfer failures in some scenarios, such as when a network device drops the re-transfer request because it detects a bit sequence it considers malicious.

#31791 - Files with the file extension `.aspx` are not transferred. **Workaround:** Edit the `resume_suffix` setting in `aspera.conf` on the client.

#30690 - `ascp` fails with an inaccurate message-`Error: failed to authenticate`-when the server is configured to accept only unsupported ciphers.

#28679 - In some cases, the fallback server cannot accept additional connections, possibly due to too many 'incomplete' requests.

#27056 - `ascmd` does not respect server-side symbolic link configuration.

#21629 - Connect Server `aspera-dirlist.pl` does not accurately reflect file permissions for user actions.

Ascp

ATT-657 - Multi-session transfers that use `-k1`, or multi-session transfers from cloud storage to local storage, can result in files on the destination that are missing bytes. This occurs when a file is split between sessions; the first session creates matching attributes for the source and destination (partial) file, and the other sessions do not recognize that there are more bytes for transfer. **Workaround:** For multi-session downloads from cloud storage, use `--overwrite=always` (to prevent resuming file transfers) or `--multi-session-threshold=0` (to prevent file-splitting across sessions).

ATT-613 - When uploading files to a HST Server on a Windows computer, if the file name contains a carriage return character ("\r"), then the transfer fails. (CIM-1205)

ATT-435 - `save-before-overwrite` is not supported for URI.

ATT-361 - `ascp` transfers to S3 fail when the `--symbolic-link=copy` or `--symbolic-link=copy +force` option is used.

ATT-226 - If the docroot is a URL path, `ascp` reports incorrect bytes for the sessions that are involved in a multi-session transfer.

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

ES-645 - The `ascp -@` option is not supported when the destination is `stdio://`.

ES-359 - `ascp` downloads from SoftLayer do not support `--move-after-transfer`.

ES-177 - The `range_low` value of a `-@` argument is not respected.

#35010 - If the source path in an `ascp` transfer is a file that is named \ (which is not supported by Aspera), the file is not transferred and an error is generated, but the folder then contains the file and all other files in that folder are transferred.

#34322 - [Linux CentOS 7.2] `ascp` fails to authenticate SSH with a large banner file size (approximately 2000 bytes).

#32890 - During an `ascp` transfer that uses the `--preserve-xattrs= metafile --remote-preserve-xattrs=metafile` options, the metafile is not transferred.

#32680 - The option to create a directory (`ascp -d`) may create a directory at a destination before an expected session failure.

#30324 - During an `ascp` upload to cloud storage, if a mid-file read failure occurs on the sending computer (which is rare) it can cause the server-side `ascp` to crash and possibly fail to report transfer completion. This read failure can be caused when a source file is truncated during transfer, a drive or file system fails, or a transfer is canceled with `Ctrl+C` or other means.

#28939 - If command line `ascp` neglects to specify a destination host, then the failed transfer (error: "no remote host specified") gets recorded in `SQLite` with `client_node_id NULL`, instead of being populated with the `uuid` of the node. This database error causes an issue with Console.

#26281 - If you run approximately 100 (or a similarly high number) concurrent uploads to S3, intermittent transfer session failures can occur.

#26185 - During an upload to S3 storage, an error may result if `ascp` reports a successful file transfer before the transfer to S3 completes.

Ascp 4

ATT-717 - Persistent Ascp4 sessions do not report SSH errors (such as an invalid hostname, username, password, port, or file list) to management.

ATT-637 - As of 3.7.4, an empty folder is created on the destination even when the source folder is excluded from the transfer (by using `-E /folder/pathname`).

ATT-621 - As of 3.8.0, Ascp 4 is not backward compatible.

ATT-583 - Ascp 4 does not automatically create a destination folder when the source is a file list and the destination does not exist. Instead, it writes all the files in the file list into one file. (CIM-1198)

ATT-582 - Ascp 4 sessions run with `-d` and a file list do not report an error if the destination already exists and is not a folder. (CIM-1199)

ATT-545 - Ascp 4 downloads all content from an AWS S3 docroot, rather than the specified content, if the docroot contains `?storage-class=REDUCED_REDUNDANCY`.

ATT-515 - When `ascp4` is used by the GUI and transfers are encrypted with AES-128, the GUI incorrectly shows that encryption is "none". (CIM-953)

ATT-477 - When files are transferred to a server with an S3 docroot and quickly retransferred with the `--delete-before-transfer` enabled, some files are deleted from the destination.

ATT-473 - Ascp 4 uploads to object storage that specify `-k 1` (resume if file sizes match) are also sensitive to checksum, such that if a file transfer is resumed and the file has the same size but a different checksum then the entire file is retransferred, rather than resumed from the last successful chunk.

ATT-451 - Ascp 4 does not respect exclude filters if the file path is specified in the command line.

ATT-438 - Ascp 4 downloads from object storage fail if the source filename contains special Unicode characters, such as Japanese font.

ATT-432 - [Linux Ubuntu] When downloading files from a server by using `ascp4`, if a docroot is configured for the transfer user and multiple source files are specified on the command line then only the first file is downloaded.

ATT-428 - During a persistent `ascp4` session, when it a file transferred to a non-existent path and `-d` is used, the file transfers successfully and the destination path is created but the file is renamed to the last element of the destination path instead of being placed inside.

ATT-409 - If a file list contains an invalid path, no error is reported or logged.

ATT-338 - Parallel uploads of several large (>1 GB) files to object or HDFS storage may fail with the error "Peer aborted session" if the number of threads that are specified in the `ascp4` command exceeds the number of jobs that are allowed to run by Trapd. **Workaround:** Open `/opt/aspera/etc/trapd/trap.properties` and set the value for `aspera.session.upload.max-jobs` to one larger than the number of `ascp4` threads. For example,

```
# Number of jobs allowed to run in parallel for uploads.
# Default is 15
aspera.session.upload.max-jobs=50
```

ATT-191 - [Linux] Symbolic links are not updated on the destination when the symbolic link option is `follow` (the default value when none is set) or `copy`.

ATT-186 - An `ascp4` multicast session does not fail if the multicast IP address and port is already in use on the receiver.

ATT-29 - Files that are transferred to S3 storage with `ascp4` retain a `.partial` extension when viewed in the GUI.

ATT-2 (#32295) - The default minimum transfer rate set in `aspera.conf` is not respected.

ES-247 - Console-initiated `ascp4` transfers fail if the docroot on the source is a UNC path (for example, `\\localhost\SHARE`), returning the error `ERR Source base/path is not a valid directory/file (doesn't match any source path).` (CIM-397)

ES-151 - `ascp4` does not recognize the UNC-path docroot of a Console transfer user. (CIM-197)

Node API

ES-505 - If the Aspera Central database cannot be reached by a Reliable Query request to `/services/rest/transfers/v1/sessions`, the response only includes a 500 Internal Server error and does not describe the error. (CIM-895)

NODE-776 - In cluster environments, the server can report a transfer session as "partially_completed" when the session is actually still running. The client correctly reports the session as "running".

NODE-711 - Backing up a master access key with `asnodeadmin --access-key-backup` does not backup the transfer activity that is associated with sub-access keys.

NODE-674 - `asnodeadmin`, `ascp`, and `asperanoded` hang when the Redis database schema is not up-to-date, rather than closing with an error.

NODE-626 - The response to a GET request to /ops/transfers does not return all stream-specific information for a transfer that is started by a POST request to /streams. The response also includes parameters that are not relevant to streams transfers.

NODE-619 - The Node API does not clean up transfer session information if the session was submitted with an invalid SSH port. **Workaround:** Clean the jobs manually by running the following command on the server:

```
$> asnodeadmin --transfer-log-del transfer_id
```

NODE-610 - The response to a GET request to /ops/transfers does not include the key-value pair `"use_ascp4":"boolean"`.

NODE-572 - As of 3.8.0, when you try to create an access key with a path to a subdirectory that does not exist, the error response does not report the invalid path.

NODE-571 - The Aspera NodeD service cannot process more than 4,000 tags in a transfer request, which limits the number of files that can be moved and copied between folders in Aspera Files to about 50. (CIM-925)

NODE-557 - When updating access key storage settings with a PUT request to /access_keys, all required settings must be provided, not just the value to update.

NODE-492 - For transfers started by the Node API, the target directory is always created if it is not present, even when `"create_dir"` is set to false. (CIM-995)

NODE-481 - The Node service sometimes returns invalid JSON when Console polls `async` jobs. **Workaround:** Recreate the Redis database to resolve the issue. (CIM-988)

NODE-469 - When managing files with a request to `/files/{id}/files`, if the system user under whom the Node service runs does not have write permissions to the docroot, a 500 internal error is returned, even if the node user is attached to a system user who has write permissions.

NODE-466 - A POST request to `/ops/transfers` that contains an invalid hostname returns "waiting for 300 seconds" rather than an accurate error message.

NODE-463 - `ascp` transfers that use `--remove-after-transfer` do not report `file.deleted` events to the Node service.

NODE-460 - The Redis database grows large quickly when reporting Sync sessions to Console that frequently synchronize large directories. (CIM-936) **Workaround:** Reduce the number of files that are reported to Console or the retention time of data in the database.

NODE-437 - Transfers with object storage, particularly with buckets that contain a lot of data, become slow when `<files_filelock_enabled>` in `aspera.conf` is set to **true** (in order to enable the filelock feature in the Node API `/files` endpoint). The default setting is **false**.

NODE-433 - The value for `xfer_retry` that is submitted in a `POST` request to `/ops/transfers` is not respected. Transfers that retry but ultimately fail take a long time to be reported as inactive.

NODE-405 - The `max_rate_kbps` in the output of a `/events` call is incorrectly reported as zero.

NODE-392 - PUT requests to `/access_keys/id/storage` cannot locate the specified access key. **Workaround:** Submit updated storage specifications as a PUT request to `/access_keys/id`.

NODE-257 - Reports sometimes fail if the Node API temporarily reports an impossibly large value for `bytes_transferred`.

NODE-236 - Transfers with a status of "waiting" cannot be canceled.

NODE-231 - When a node-to-node transfer fails due to a transfer authentication error, the `GET /ops/transfers` response does not provide error information.

NODE-139 - The `--token-key-length` option in `asnodeadmin` allows invalid token key lengths.

NODE-137 - A Node API `/ops/transfers` call reports the incorrect values for `files_completed` and `files_failed`.

#33206 - `/ops/transfers` might briefly report pending transfers as `failed` when transfers are retried.

#32669 - When a directory is symbolically linked from a subdirectory, it does not appear in the search result for a `/files/search` request in the Node API.

Watch Folders and Aspera Watch Service

AC-517 - Pull Watch Folders are not visible in IBM Aspera Console because it uses an older version of the Watch Folder API.

WAT-857 - When you try to create a Watch Folder with an incorrect password for the system user, the GUI returns an incorrect error message "Service creation failed: Failed to set token for *username*". Additionally, the services are actually created but are unusable until the password is corrected.

WAT-856 - As of version 3.8.0 when you create a Watch Folder with the API, the default version in the header is set to 2016_09_14 and conversion to the updated Watch Folder configuration (available as of 3.8.0) fails. **Workaround:** Set the version to the latest by adding `"X-aspera-wf-version: 2017_10_23"` as a header to the Watch Folder setup request. (CIM-1678)

WAT-804 - If `db_spec` is set in both the `<watch>` and `<rund>` sections of `aspera.conf`, the setting for `rund` is not respected and the one for `watch` is used instead.

WAT-758 - The transfer token that is used for pull Watch Folders expires and is not automatically replaced, causing transfers to error. **Workaround:** Restart (disable and enable) the Aspera Watch Folder service (asperawatchfolderd) that is associated with the Watch Folder user.

WAT-674 - As of 3.8.0, some Watch Folder API endpoints still use "local" and "remote" terminology instead of "source" and target", which are used in the 3.8.0 Watch Folder configuration.

WAT-567 - A Watch Folder configured for growing files reports a "Healthy" state and shows bytes are written at the destination despite having an invalid password and no transfer occurring.

WAT-559 - Watchd allows users to create a watch on the root folder, which can overload the Redis database and cause Watchd to core dump. (CIM-662)

WAT-501 - Some `ascp` sessions started by a Watch Folder may not stop running after synchronization is complete when many (50) large (1000 files of 2 KB to 1 MB) Watchfolders are started at the same time.

WAT-314 - `asperawatchfolderd` must be running in order to delete a Watch Folder.

WAT-174 - Watch Folders uses excessive memory when it watches 10 million files.

WAT-159 - If one file in a Watch Folder transfer fails or a drop is aborted, the other files in the package are reported as aborted but `ascp` is not stopped and the transfer continues.

Sync

WAT-850 - Continuous mode on macOS (supported as of 3.9.0) does not handle directory and file moves the same way as Linux and Windows. Instead of renaming the file for directory on the target, macOS treats moves as a delete and recreate action, and the content is re-transferred from the source. When a directory is moved and a file in the target directory is modified, the modifications are overwritten.

WAT-848 - Sync does not synchronize the removal of ACLs or extended attributes from a source file.

WAT-847 - Sync in continuous mode on macOS (supported as of 3.9.0) does not synchronize a modified file from source to destination when the source directory is a symbolic link.

WAT-844 - When running a bidirectional, continuous mode synchronization on macOS (supported as of 3.9.0), when a file is deleted and then recreated, Sync performs multiple deletes and transfers before the file is successfully synchronized.

WAT-838 - During pull or bidi Sync sessions, compression is not applied to transfers from the remote to local computer. (CIM-1638)

WAT-832 - When running a continuous Sync session to cloud storage, the client Sync session can be stuck in "Pending" if a file is moved while it is being transferred.

WAT-821 - As of version 3.6.0, when running a continuous Sync session to cloud storage, if a directory is renamed while a file in that directory is being transferred, Sync does not report a conflict. Instead, the file is transferred and the directory rename is not synchronized to the cloud storage.

WAT-819 - As of version 3.8.0, when a user starts a "push" async session to a destination directory that is owned by a different user and creates a new directory in the source directory, then async reports an error. The new directory is created on the destination, but any files within the source directory are not synchronized to the destination.

WAT-790 - When Sync is run in continuous mode using `--scan-interval`, `--exclude-dirs-older-than`, and `--clean-excluded`, directories that are older than the exclusion threshold are not cleaned from the database.

WAT-759 - In continuous synchronization mode, the UID and GID are not preserved even when `--preserve-uid` and `--preserve-gid` are used.

WAT-715 - The initial synchronization of directories in object storage is very slow.

WAT-700/ES-92 - Sync reports incorrect counts for 'deleted_paths', 'deleted_bytes', and 'cumulative_deleted_bytes'.

WAT-465 - Sync hangs following a TCP impairment that produces a libssh2 timeout or error.

WAT-377 (#27391) - [Linux] A continuous `async` session that is configured to follow symbolic links does not sync a symbolic link target after it is modified.

WAT-376 - A continuous `async` session that is configured to follow symbolic links returns an error for a symbolic link that is created after the `async` session starts and that links to a directory that was created after the `async` session starts.

WAT-355 (#34793) - [Windows] Hard-linked files are not resynchronized. A file that is a hard link to another file is kept in sync until the original file is modified, then only the original file is synced.

WAT-9 - When the `scan-file-rename` option is used with `asperawatchd`, moved files should be detected and renamed at the destination, not deleted and replaced by a transferred, renamed file.

#29038 - Using `overwrite=always` when you sync with cloud storage does not overwrite the file. The default checksum behavior with S3 (as with any cloud storage) is "none". An existing file on S3 is considered identical to the local file when their sizes are equal. Therefore, the file on S3 is not overwritten even when the content of S3 differs from the content of the local file.

#28817 - The Sync log entry for SYNCERROR_DELAY does not include information that describes the file name and path.

#27621 - Hidden, temporary, or transient files, such as temporary files created by Microsoft Office products, can cause Sync to report conflicts.

#25915 - [Linux] If a source file is overwritten during a continuous Sync in push mode, the corresponding file on the destination might be deleted. **Workaround:** Run a one-time push Sync of the overwritten file to restore it on the destination.

#25631 - When you transfer from Windows to Mac and use `preserve-acls=native` and `remote-preserve-acls=native`, ACL data are saved as `xattr`. **Workaround:** Do not use the `native` setting when you transfer or sync across platforms.

#23400 - [Linux] As of Sync version 1.5+ the user is permitted to sync to the root directory.

#20906 - `async` cannot create a watch on an unreadable directory; therefore, it does not get notified when permissions change. In addition, `async` treats an unreadable directory as "skip" rather than reporting an error or conflict.

#20767 - If you use the `-R log dir` from Linux to Windows and there are spaces in the directory path, the path is truncated at the first space in the path.

#19945 - `asyncadmin` creates SHM and WAL files for read-only operations. Once asyncadmin is run as the root, `async` run by the user does not have permission to access the existing SHM and WAL files and thus `async` fails. This issue is due to a bug in SQLite.

#16911 - Characters in the `async` session option that are not preceded by a "`-`" or "`--`" are ignored and no error message is reported. Any session options that are specified (such as `-l` or `-a`) after the string of characters that are not preceded by a "`-`" or "`--`" are also ignored. The session runs using the default values, and does not notify you that the command line settings were ignored.

#13761 - If file names contain "\" or new line, `async` transfer fails, causing the internal transfer queue to become full and the synchronization to stall.

Object Storage Support

TRAP-59 - If an incorrect DNS nameserver is set in `/etc/resolve.conf` and then corrected, TrapD must be restarted for the correct nameserver to be used by TrapD. If TrapD is not restarted, TrapD fails to connect and retries indefinitely. (CIM-469)

TRAP-27 - In some cases, stopping Trapd while an `ascp` transfer is still running may cause a restart of Trapd to fail.

#36067 - Deleting folders from a Limelight directory is slow.

#33214 - Transfers to and from cloud storage using authorization tokens with URIs that do not have a docroot specified are not supported.

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.