Release Notes: IBM Aspera HSTS, HSTE, and Desktop Client 3.8.1 for Linux, Windows, and macOS

Product Release: July 3, 2018
Release Notes Updated: July 13, 2018

This release of IBM Aspera High-Speed Transfer Server, High-Speed Transfer Endpoint, and Desktop Client 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.

Desktop Client users: Features and issues that are related to configuration, Watch Folders, and the Node API are not applicable to your product.

Note: Some Aspera product names are in a transition phase. Enterprise Server and Connect Server are changing to "IBM Aspera High-Speed Transfer Server" and Point-to-Point Client is changing to "IBM Aspera High-Speed Transfer Endpoint".

NEW FEATURES

For more information about the new features in this release, see "New Features" in the guides:

Enterprise Server Admin Guide (Linux)
Enterprise Server Admin Guide (Windows)
Enterprise Server Admin Guide (Mac)

General

- Faster directory browsing in the GUI, especially for remote cloud storages.
- Improved reporting for package transfers that are intiated by Aspera Central. (CIM-1327)

Node API

- Faster transfer start up when many transfer sessions are started through the Node API. (CIM-1010)

Sync

- A new async option, `--ignore-mode`, prevents the file mode from being synced from the source to the destination. Use this option to allow the file to have different modes on the source and destination and to prevent Sync from hanging if the destination permissions change.
- Sync now respects the `files_filelock_enabled` setting in a user's access key, which overrides the server setting in `aspera.conf`.
- 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.

Object Storage Support

- Faster authentication to AWS S3 when using AWS assumed roles. Trapd can now get credentials from regional Amazon Security Token Service (STS) endpoints, rather than only the global endpoint. On EC2 instances the regional endpoint is retrieved automatically, otherwise the endpoint can be set in s3.properties or the docroot.
- The TrapD plugin now reports the total bytes to transfer; a new method, `getBytesToTransfer`, is available in the `aspera.trap.plugins.Transfer` interface.

BREAKING CHANGES

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

- 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.

ISSUES FIXED IN THIS RELEASE

ATT-612 - Some Ascp 4 error messages are missing the last letter of the message or are incorrectly parsed. (CIM-1364)

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-511 - When both `--overwrite=never` and `--remove-after-tranfer` are used, source files may be deleted even if no transfer occurred. (CIM-932)

ATT-579 - Persistent `ascp` uploads to a server that is configured to skip symbolic links do not report when symbolic links are skipped.

ATT-492 (#22998) - If the overwrite setting in the server's `aspera.conf` is "deny", a destination file with the same name as the source file is still overwritten.

ATT-433 - [Windows] An `ascp4` transfer that uses the `--file-list` option fails. (CIM-433)

ATT-189 - In rare cases, `ascp` keeps running after it encounters a disk read error. (CIM-233)

ATT-98 - If inline validation is configured on the server side, the server does not honor a session timeout if a transfer includes a skipped file.

ES-798 - Transfers that are started in the GUI do not respect `peer_ip` transfer authorization rules (command line `ascp` transfers follow the rules). (CIM-1290)

ES-771 - [Windows] In 3.8.0, with a push Hot Folder configured to always overwrite and delete the source file after transfer, when the same set of files is added to the source repeatedly, the source files are not always sent and deleted from the source because new-file notifications are occassionally missed if the notification is received while a scan is in process. (CIM-1243)

ES-731 - [Linux] Aspera services may not be able to start if a computer OS upgrade replaced `init` with `systemd` (for example, Debian 7 to Debian 8.10), and then the Aspera server is upgraded to version 3.8.0. **Workaround:** Reboot the computer after upgrading your Aspera server to version 3.8.0.

ES-760 - In the 3.8.0 GUI, when you create a connection to Azure Files, clicking the **Browse** button to select the target directory returns an "Access denied" error.

NODE-653 - The Aspera NodeD service crashes when it receives a POST request to /access_keys for an Azure SAS access key.

NODE-643 - When the content_protection_secret is specified in an access key (that is created with /access_keys), uploads are correctly encrypted but downloads do not use the secret and files are not decrypted.

NODE-635 - The IAM policy of an AWS access key that uses IAM role authentication must include s3:GetObject permission to authorize the user to browse and upload to the storage.

NODE-633 - In 3.8.0, when creating an AWS access key through the Node API, the value for "server_side_encryption_aws_kms_key_id" is not respected and the default master encryption key is used instead.

TRAP-83 - Using the default configuration of the Java Heap size, Trapd might be unable to recover enough memory after a full garbage collection, resulting in an out-of-memory error.

WAT-802 - In 3.8.0, Sync database updates might be slower than previous versions.

WAT-784 - If a Hot Folder is set up with a connection to a server over HTTP/S, such as to Shares, and the connection password is changed without updating the Hot Folder connection, then the connection to that Hot Folder fails and any other Hot Folders stop transferring until the problem Hot Folder is stopped. (CIM-1386)

WAT-775 - Incorrect host format described in the instructions for creating a Watch Folder from the command line. (CIM-1299)

WAT-771 - When upgrading to 3.8.0, if you have multiple existing Hot Folders, they no longer work.

WAT-765 - When upgrading from 3.7 to 3.8.0, Watch Folders that are configured to use SSH key authentication no longer work after the upgrade.

WAT-762 - When `async` is run in continuous mode and no initial scan (with `-C --no-scan`), `async` does not receive notifications of new files and directories. (CIM-1238)

WAT-706 - Pull Watch Folders might hang if a request to the remote WatchD API times out.

WAT-606/WAT-557 - If Sync does not receive a notification that a new folder is created, files in that folder are not synchronized during a continuous Sync session. As a result, a continuous Sync push that is run with the `--scan-dir-rename` option does not synchronize files if the directory is created and then renamed after the Sync session has started.

WAT-594, WAT-589 (#13645), WAT-362 (#24812) - During a Sync session, if `ascp` fails to transfer a file, such as if a file is resized or a directory is renamed, Sync keeps the file as pending rather than as errored and the session does not stop. (CIM-814)

SYSTEM REQUIREMENTS

High-Speed Transfer Server, High-Speed Transfer Endpoint, 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
- **macOS**: OS X 10.11, macOS 10.12 (Sierra), 10.13 (High Sierra)

Client Browsers for High-Speed Transfer Server Web UI

- **Linux:** Chrome 62-64, Firefox 56-58, Firefox ESR 52
- **Windows:** Chrome 62-64, Microsoft Edge 39-41, Internet Explorer 11, Firefox 56-58, Firefox ESR 52
- **macOS:** Chrome 62-64, Firefox 56-58, Safari 11, Firefox ESR 52

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-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.

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

ES-930 - [Mac] When a node user is associated with a transfer user who is not assigned to aspshell and attempts to transfer by using the Aspera RSA key `aspera_tokenauth_id_rsa.pub`, transfers fail because the path to aspshell in `aspera_tokenauth_id_rsa.pub` is incorrect. **Workaround:** Either assign the transfer

user to aspshell (see "Setting up Users" in the admin guide) or edit /Library/Users/*username*/.ssh/ authorized_keys, changing the first line:

```
command="/bin/aspshell -t",...
```

to

```
command="/Library/Aspera/bin/aspshell -t",...
```

ES-893 - [Windows] As of 3.8.0, the product cannot be silently installed by using the instructions in https:// support.asperasoft.com/hc/en-us/articles/216127388-How-to-do-a-Silent-Installation-of-Enterprise-Server-Point-to-Point-Client-or-Connect-Server-2-6-0-or-higher (CIM-1459).

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

ES-796 - [Windows] As of 3.8.0, your Aspera application does not appear in "Programs and Features" after a silent installation from the command line. (CIM-1304)

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-770 - 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. (CIM-1239) **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.

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

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

ES-443 - [Windows] As of 3.7.4, local users cannot access a UNC shared folder ("Access is Denied") in a domain environment when the docroot is set to a network share. (CIM-854)

ES-408 - [Windows] Inconsistent transfer UDP use when bind source address is configured for multiple network interfaces. (CIM-702)

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-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-291 - [Windows 10 with Java 8] - The Aspera GUI is displayed in a small font on high-resolution displays. This issue is a Java bug that causes applications that use Swing to not scale correctly. **Workaround:** Right-click the Aspera application icon and click **Properties > Compatibility**. Select **Override high DPI scaling behavior**. Click the drop-down menu for **Scaling performed by**, and select **System**. Click **OK** to apply your changes and start the application. (CIM-505)

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-145 (#36083) - [Windows] On non-English operating systems, two **File Handling** tabs are displayed in the GUI, one in English and one in the language of the operating system.

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.

ES-69 - [Windows] In the GUI, Chinese characters overlap in some **Configuration** settings.

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.

#36109 - [Windows] The GUI license display for ALEE-enabled Windows (click **Help > About > View License**) does not show relevant license information, such as what components are enabled.

#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 retransfer. 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 retransfer 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.

#30082 - [Windows] When the upload of a source file to the remote server fails because the file has the same name as a folder, no error message appears in the GUI.

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

#27879 - [Mac] In Connect Server, `always_set_home` does not work if the user's home directory does not exist.

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

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

#16390 - [Windows] Unicode file names appear incorrectly in pre-processing and post-processing email notifications.

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

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

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

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

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-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-624 - [Windows] No files are transferred if the argument for `--src-base` includes a semicolon (";") but the transfer is reported as successful.

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

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

ES-96 (#33091) - [Windows] Downloading files or folders that have names that end in a trailing space fail.

#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.

#30231 - [Windows] If a pre-post script includes a path that contains ".." and the client is running on Windows, `ascp` fails with the following message:

```
Cannot open -e pre-post command: Unknown error
```

#29043 - [Windows] Under serious WAN impairment, Hot Folder push transfers with a prepost script intermittently report an `asssh` error approximately 10-15 seconds after Transfer Statistics are reported to the log. This delay in process shutdown can hold the handle to the file list such that subsequent `ascp` processes fail.

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

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 part of 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-existant 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-298 - [Windows] When the destination has several million files, the source has few files, and `<worker_threads>` is set to 64 in `aspera.conf`, a download run with the `--delete-before` or `--delete-after` option can take several hours to delete files and might time out before finishing the deletion.

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-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-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-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-442 - `/ops/transfers` can return a value of "null" for `files_failed`, which can prevent transfers from being displayed in Console. (CIM-864) **Workaround:** Enable the Console database to handle the "null" value by logging into the Console database and running the following command:

```
ALTER TABLE fasp_sessions CHANGE COLUMN files_failed files_failed INTEGER
null;
```

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.

Watchfolder 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-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-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 coredump. (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-431 - [Windows] Watch Folder services cannot be listed or updated by the API if the user running the Aspera Run Service is changed.

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

WAT-246 - [Mac OS X] Watches cannot be created on symlinked directories.

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

Async on AIX, Solaris, Mac OSX, does not support continuous PUSH or BIDI modes.

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

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-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-644 - If the local directory to synchronize is a symlink, 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.

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-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.

#13826, #13827, #13833 - [Windows] Limited support for Unicode file names on Windows. If you create a directory with a name containing Unicode characters (for example, Japanese) and then create a file in that directory, the following errors may occur:

1. Running with an `-N` set to a string with non-English characters (such as Japanese) causes an error message.
2. After a sync, the UI displays an inaccurate directory name and path separator.
3. After syncing, using the `asyncadmin -M` option does not allow you to delete the file from the database.

#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-126 - [Azure Data Lake Storage] When setting the docroot for a server in ADLS, special characters in query values are incorrectly processed by Trapd. **Workaround:** URL-encode special characters in the refresh URL and client credentials. For example, replace

```
adl://trapstage.azuredatalakestore.net/?dfs.adls.oauth2.refresh.url=https://
login.windows.net/xyz/oauth2/token
```

with

```
adl://trapstage.azuredatalakestore.net/?dfs.adls.oauth2.refresh.url=https:%2F
%2Flogin.windows.net/xyz/oauth2/token
```

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. **Workaround:** Specify the port as a query in the URI. For example, `s3://s3.xyz.ingest.xyz.net/staging?s3service.s3-endpoint-http-port=9090`.

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.

#34954 - [Windows] When stopping and starting Aspera services, including asperalee, asperanoded, and asperacentral, from the command line on ALEE-enabled Enterprise Server on Windows, the error "System error 5 has occurred. Access is denied." is returned even though the services have successfully stopped and started.

#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.