Release Notes: IBM Aspera Proxy 1.4.4

Product Release: November 4, 2019
Release Notes Updated: November 3, 2019

This release of IBM Aspera Proxy provides the new features, fixes, and other changes listed below. Additional sections cover system requirements and known problems.

NEW FEATURES

- The version of NGINX included with Proxy has been upgraded to 1.14.2 to address several security vulnerabilities: CVE-2018-16844, CVE-2018-16845, CVE-2018-16843, and CVE-2019-7401.
- Proxy can now be run by a non-root user. For instructions, see the appendix "Running Proxy as a Non-Root User" in the Proxy guide.

BREAKING CHANGES

ES-1468 - A new vulnerability in `sudo` affects the usage of the Runas `(ALL)` keyword when granting sudo access to users. For further information, see https://www.sudo.ws/alerts/minus_1_uid.html and http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14287. Aspera recommends users discontinue using the `(ALL)` keyword. Instructions in the Proxy guide have been updated and no longer suggest using it.

ISSUES FIXED IN THIS RELEASE

ATT-775 - Proxy `enable-routing.sh` needs to support newer SuSE versions and Debian.

ATT-896, ATT-897 - Ascp running on proxy server hangs when incoming address is NAT64.

ES-1468 - Instructions in the Proxy guide have been updated to no longer suggest using the `(ALL)` keyword when granting sudo access to users.

ES-1433 - Issue with `$user` in `aspera.conf` for `ssh` key path.

SYSTEM REQUIREMENTS

Linux 64-bit: RedHat 6-7, CentOS 6-7, Fedora 15-20, Ubuntu 12-14, Debian 6-7, SLES 11-12, Suse 15, Kernel 2.6 or higher, and libc version GLIB 2.5+.

KNOWN ISSUES

ATT-779 - Aspera Proxy shows a disable-routing.sh error, even when Proxy is handling all transfers correctly.

ES-225 - Aspera clients using `ascp` version 3.1.1 or earlier are mapped by Reverse Proxy to the first domain rule specified in `aspera.conf` if only a `host_domain` rule is set. **Workaround:** Set a `host_ip` rule for the desired domain rule. (CIM-337)

#34615 - When you configure Forward Proxy in the Aspera server GUI (**Preferences > Proxy > Enable transfer proxy**), the GUI applies TCP and UDP rules from Forward Proxy to the Aspera server GUI connections.

#19185 - If you specify a directory for `<log_dir>`, the log file is created with 0640 permissions. As a result, not all transfers will be logged. **Workaround:** Once the log file has been created, change its permissions to 0660.