z/OS 3.1 IBM Education Assistant

Solution Name: Upgrade OpenSSH to 8.4
Solution Element(s): z/OS OpenSSH

July 2023

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

- A new release of OpenSSH 8.4p1 ported to z/OS, replacing the older release 7.6p1.

Overview

- Who (Audience)
  - System Programmers, z/OS OpenSSH users
- What (Solution)
  - Providing a newer level of OpenSSH
- Wow (Benefit / Value, Need Addressed)
  - Support for many new functions and crypto algorithms are included, so as to be compatible with other OpenSSH or SSH implementations that wish to use these new functions and algorithms.
  - Certain security vulnerabilities are resolved

Usage & Invocation

Support “FIDO2 / SK” authentication.

- OpenSSH 8.2 introduced support for FIDO/U2F hardware authenticators.
  - Details can be found in the release notes here: OpenSSH 8.2 (www.openssh.com/txt/release-8.2).
- z/OS 3.1 OpenSSH is based on OpenSSH 8.4p1 and supports the server (SSHD) verification of FIDO/FIDO2 based keys for authentication of remote ssh clients. It does not support:
  - Use of z/OS attached FIDO/U2F hardware tokens
  - Generation (by using ssh-keygen) of keys on FIDO/U2F tokens.
  - z/OS ssh client authentication (by using either ssh or ssh-agent) using a FIDO token.

Usage & Invocation

An example illustrates how z/OS sshd can verify a FIDO-based key that was generated on a remote platform:

1. On a remote system such as Linux, which has an attached FIDO hardware token, generate a FIDO key:

   ```
   linux> ssh-keygen -t ecdsa-sk
   ```

2. Add the ECDSA-SK public key to $HOME/.ssh/authorized_keys on z/OS in the same manner as with other SSH public key types.
3. Connect to z/OS OpenSSH with the FIDO-based key:

   ```
   linux> ssh -i ~/.ssh/id_ecdsa_sk user@zos.myco.com
   ```

Usage & Invocation

- The “FIDO2 / SK” algorithms are added to default support list of:
  - sshd_config option “HostbasedAcceptedKeyTypes” and “PubkeyAcceptedKeyTypes”
  - ssh_config option “HostbasedKeyTypes” and “HostKeyAlgorithms”
- The added “FIDO2 / SK” algorithms are:
  - sk-ecdsa-sha2-nistp256-cert-v01@openssh.com
  - sk-ecdsa-sha2-nistp256@openssh.com
  - sk-ssh-ed25519-cert-v01@openssh.com
  - sk-ssh-ed25519@openssh.com

Usage & Invocation

- Besides the above sk keytypes are added, the following keytypes are also supported in 3.1:
  - rsa-sha2-512-cert-v01@openssh.com
  - rsa-sha2-256-cert-v01@openssh.com
  - rsa-sha2-512
  - rsa-sha2-256

- The related options are:
  - sshd_config: CASignatureAlgorithms, HostbasedAcceptedKeyTypes, HostKeyAlgorithms, PubkeyAcceptedKeyTypes
  - ssh_config: CASignatureAlgorithms, HostbasedKeyTypes, HostKeyAlgorithms, PubkeyAcceptedKeyTypes

Usage & Invocation

- The support Cipher, MAC and Key Exchange algorithms are as the same as on V2R5.
- To obtain the supported algorithms on system, user could use command “ssh -Q”.
  - “ssh -Q cipher” - obtain the list of available Cipher algorithms
  - “ssh -Q mac” - obtain the list of available MAC algorithms
  - “ssh -Q kex” - obtain the list of available kex algorithms
  - “ssh -Q key” - obtain the list of available key algorithms

- Support “^” syntax to easily place specified algorithms at the head of the default lists.
  - For example: “MACs=^hmac-md5”, “Ciphers=^3des-cbc”

Usage & Invocation

- Less-secure algorithms have been deprecated and removed from default support:
  - diffie-hellman-group14-sha1 remove from **default** KexAlgorithms list.
  - when using ssh-keygen to create new OpenSSH certificates with an RSA key, the rsa-sha2-512 algorithm will be used **by default**.
  - The ssh-rsa (sha1) key algorithm is still supported and available as a **default** key algorithm, but is deprecated. It will be removed as a default in a future release.

- Using LibreSSL 3.0.2 as statically linked cryptographic library, to replace OpenSSL 1.0.2.

- Extensive internal changes to the code to perform more checking and validation to enhance security.

Usage & Invocation

- Support URI format of the target address in ssh, scp and sftp command:
  - scp://[user@]host[:port][/path]
  - sftp://[user@]host[:port][/path]
  - ssh://[user@]hostname[:port]

- New option CASignatureAlgorithms supported in both ssh_config and sshd_config, which specifies which algorithms are allowed for signing of certificates by certificate authorities (CAs). The default is:
  - ecdsa-sha2-nistp256
  - ecdsa-sha2-nistp384
  - ecdsa-sha2-nistp521
  - ssh-ed25519
  - rsa-sha2-512
  - rsa-sha2-256

Usage & Invocation

- New option GSSAPIKexAlgorithms supported in both ssh_config and sshd_config, which specifies the key exchange algorithms that are accepted by GSSAPI key exchange. This option only applies to connections using GSSAPI.
- The support values are:
  - gss-group14-sha256-,
  - gss-group16-sha512-,
  - gss-nistp256-sha256-,
  - gss-curve25519-sha256-,
  - gss-group14-sha1-,
  - gss-gex-sha1-,
  - gss-group1-sha1-
- The default is:
  - gss-group14-sha256-,
  - gss-group16-sha512-,
  - gss-nistp256-sha256-,
  - gss-curve25519-sha256-,
  - gss-group14-sha1-,
  - gss-gex-sha1-

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - N/A

Upgrade & Coexistence Considerations

- z/OS 3.1 OpenSSH does not support:
  - SSH Version 1 protocol (also referred to as SSH-1).
  - Running without privilege separation for sshd (SSH Daemon).
  - Support for the legacy v00 OpenSSH cert format.
  - Support for pre-authentication compression by sshd (SSH Daemon). SSH clients will either need to support delayed compression mode or otherwise compression will not be negotiated.

Installation & Configuration

- No special considerations

- Verifying version:

  $ ssh -V

  OpenSSH_8.4p1, LibreSSL 3.0.2

Summary

- The following z/OS OpenSSH enhancement has been explained:
  - Upgrade OpenSSH 8.4

- Upgrade to OpenSSH 8.4p1 provides various functional, performance and security requirements.

Appendix

- z/OS OpenSSH User's Guide
- Open source reference guide:
  - OpenSSH http://www.openssh.org/
  - LibreSSL http://www.libressl.org/