SSH-SSH-SSH-SSH-SSHANGES

(Tom Conley)

SSHANGES

- After upgrading to z/OS V2R4, you may see SSH failures
- SSH won't accept client connections
- z/OS V2R4 comes with a big upgrade to OpenSSH
- ssh -V output
  - z/OS V2R3 - OpenSSH_6.4p1, OpenSSL 1.0.2h 3 May 2016
  - z/OS V2R4 - OpenSSH_7.6p1, LibreSSL 3.0.2
- According to OpenSSH: Release Notes:
  - OpenSSH_6.4p1 was released on 2013/11/08
  - OpenSSH_7.6p1 was released on 2017/10/03
  - That's a jump of four years and 12 releases of OpenSSH
- A few things sshanged…

SSHANGES

- Deprecated ciphers and key exchange (Kex) methods removed
- You eliminate deprecated methods on the server side
- But what about the client side?
- OpenSSH will allow support for deprecated methods
- In ssh_config, specify the following (use these only if you must):
  - PubkeyAcceptedKeyTypes +ssh-dss
  - HostKeyAlgorithms +ssh-dss
- This will fix some issues, but not all

SSHANGES

- IBM created the following APARs to help:
  - OA61535 - REMOTE HOST IDENTIFICATION HAS CHANGED may occur after enabling DSA support for host keys
  - OA60340 - WHEN CPACF OR ICSF IS AVAILABLE AND CONFIGURED FOR USE BY Z/OS OPENSSH SOFTWARE (OPENSSL) CIPHERS MAY FAIL WHEN SELECTED
- Even after these APARs, you may still have SSH failures
- Buried in the OpenSSH: Release Notes is this blurb:
  - * ssh(1), sshd(8): increase the minimum modulus size supported for diffie-hellman-group-exchange to 2048 bits.
  - This happened in OpenSSH 7.2/7.2p1 (2016-02-29)
- OpenSSH no longer accepts 1024-bit keys (modulus 1024) for Kex

SSHANGES

- Encourage your SSH clients to eliminate deprecated methods
- In ssh_config, specify the following for KexAlgorithms:
  - diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha256,(and if you must) diffie-hellman-group14-sha1
  - Remove diffie-hellman-group1-sha1
  - Do this for both client and server sides of connection
- For z/OS V2R3 sites, extremely difficult to pre-determine scope
- Lacking instrumentation to identify SSH clients using outdated Kex
- Some tools available
  - SMF data
  - Wireshark with packet filtering

BOTTOM LINE…

- Stop using deprecated algorithms!
- Institute procedures reviewing your SSH connections to ensure use of secure algorithms
- SHA-1 was officially deprecated in 2011
- The major browsers removed SHA-1 in 2017
- Yet somehow SHA-1 is still in widespread use today
- We must eradicate SHA-1 and other deprecated methods
- Make it your mission in life!