IBM Education Assistance for z/OS V2R2

Item: OpenSSH upgrade to 6.4p1
Element/Component: IBM Ported Tools for OpenSSH V1R3
z/OS OpenSSH V2R2

Material current as of May 2015

Agenda

- Trademarks
- Presentation Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Presentation Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Presentation Objectives

- Explain the benefits of the OpenSSH upgrade
- Explain how to use the major features
- Identify important installation information
- Identify migration and coexistence considerations
- Identify references for additional information
-
- **Reminder:**

  IBM Ported Tools for z/OS is a non-priced program product. It is not part of the
  z/OS operating system. OpenSSH V1R3 and V2R2 have the same level of functionality.

Overview

Problem Statement / Need Addressed :

(1.) z/OS OpenSSH needs to upgrade underlying open source code to more current OpenSSH version to address various functional, performance and security requirements.

Solution:

Upgraded to OpenSSH 6.4p1 (released November 2013). Same versions of OpenSSL 1.0.1c and zlib 1.2.3 will be used. **N.B.:** ssh-rand-helper is no longer supported in 6.4p1, so ICSF is now a hard requirement (more later)

Benefits:
Functional: many (highlights listed later)
Support for many new crypto algorithms are included, so as to be compatible with other OpenSSH or SSH implementations that wish to use these new algorithms.

Overview

Problem Statement / Need Addressed (Continue):

(2.) z/OS OpenSSH needs to support ICSF acceleration of CTR mode AES ciphers. This is important since the defaults in open source OpenSSH have recently changed so that AES-CTR is preferred over AES-CBC. For these connections, ICSF acceleration was not previously available.

Solution:

AES CTR mode support was added to ICSF via APAR OA45548 and support was added to work like existing AES-CBC mode ICSF support. Affected OpenSSH algorithm names: aes128-ctr, aes192-ctr, aes256-ctr.

Benefits:

Performance: reduction in CPU usage over software implementation when using AES-CTR Ciphers.

Overview

Problem Statement / Need Addressed (Continue):

(3.) Improve SMF support. a) sftp client does not currently record target pathname b) ssh client and sshd server do not currently cut SMF records at the beginning of a successful connection.

Solution:

a) Add new triplet to SFTP client transfer SMF record for target pathname
b) Create new SMF 119 records at the beginning of a successful ssh connection, just after user authentication. The ssh client and sshd server will have their own new subtypes. Existing “Common TCPIP” and “SSH Common Security” triplets will be included. **Note:** BPX.SMF access is required in order to record the ssh client connection started record, since the ssh client is not APF authorized.

Benefits:
Better accounting and auditing of ssh connections.

Overview

Problem Statement / Need Addressed (Continue):

(4.) The current ssh, sftp, and scp clients cannot be invoked from a TSO-OMVS (3270) environment. This makes diagnosis of connection and handshake problems more difficult for many customers.

Solution:

Allow the ssh client to be invoked under a TSO/OMVS shell. Entry of password credentials will not be allowed however, to prevent exposure/display of passwords.

Benefits:

The ssh command may be invoked under TSO/OMVS to verify a working network connection, acceptance of server host key, and even a completed connection if a password is not required. Passwords are not required if ssh user keys are used.

Overview

Problem Statement / Need Addressed:

(5.) The IBM-added option “IdentityKeyRingLabel” is complex to use in a shell script since literal double-quotes are required.

Solution:

Relax the syntax of IdentityKeyRingLabel so that double-quotes are optional when entered from an ssh (or sftp, scp) command line. They are still required when the keyword appears in the zos_ssh_config or authorized_keys file. The HostKeyRingLabel is similarly relaxed so that double-quotes are not required when this keyword is used on an sshd command line.

Benefits:

Difficult multiple shell script escape sequences are no longer required. The previous syntax still works.

Usage & Invocation

- **Key Exchange algorithms can now be specified (-oKexAlgorithms).** They are (new **highlighted**):

  diffie-hellman-group1-sha1, diffie-hellman-group14-sha1,
  diffie-hellman-group-exchange-sha1,
  diffie-hellman-group-exchange-sha256,
  ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521

  - NIST Elliptic-curve algorithms added.

Usage & Invocation

- **Key algorithms** (used for ssh host(server) or user keys; new **hilighted**)

  ssh-rsa,ssh-dss,
  ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,
  ecdsa-sha2-nistp521,
  ssh-rsa-cert-v01@openssh.com,
  ssh-dss-cert-v01@openssh.com,
  ecdsa-sha2-nistp256-cert-v01@openssh.com,
  ecdsa-sha2-nistp384-cert-v01@openssh.com,
  ecdsa-sha2-nistp521-cert-v01@openssh.com,
  ssh-rsa-cert-v00@openssh.com,
  ssh-dss-cert-v00@openssh.com

  - NIST Elliptic-curve DSA w/ SHA-2 algorithms added
  - OpenSSH “certificates” added (more later)
  - Note: non-standard non-RFC names have “@openssh.com”

Usage & Invocation

- **Cipher algorithms** (new **hilighted,** default preference order as shown, ICSF support noted with “*” or “**”(new))

  aes128-ctr**,aes192-ctr**,aes256-ctr**,arcfour256,arcfour128,
  aes128-gcm@openssh.com,aes256-gcm@openssh.com,
  aes128-cbc*,3des-cbc*,blowfish-cbc,cast128-cbc,aes192-cbc*,
  aes256-cbc*,arcfour,rijndael-cbc@lysator.liu.se*

  - AES GCM (Gallois Counter Mode) ciphers added. These are interesting in that they function as both Cipher and HMAC in one.
  - AES CTR mode ICSF support

Usage & Invocation

- **Mac algorithms** (new **hilighted**, default preference order shown, ICSF support noted as "*" or "**"(new))

  hmac-md5-etm@openssh.com*,hmac-sha1-etm@openssh.com*,
  umac-64-etm@openssh.com,umac-128-etm@openssh.com,
  hmac-sha2-256-etm@openssh.com**,**
  hmac-sha2-512-etm@openssh.com**,**
  hmac-ripemd160-etm@openssh.com*,
  hmac-sha1-96-etm@openssh.com*,
  hmac-md5-96-etm@openssh.com*,
  hmac-md5*,hmac-sha1*,
  umac-64@openssh.com**,umac-128@openssh.com,**
  hmac-sha2-256,hmac-sha2-512****,**
  hmac-ripemd160*,hmac-ripemd160@openssh.com*,
  hmac-sha1-96*,hmac-md5-96*
  (continued on next slide)

Usage & Invocation

- **Mac algorithms** (continued from previous slide)
  - SHA-2 algorithm added (with ICSF support)
  - umac algorithm support added
  - "-etm@openssh.com" algorithms are **not** new algorithms! They are variants that indicate that the MAC is calculated **after** encryption ("Encrypt-then-MAC") rather than the other way around. The community now considers this more secure (in theory).

Usage & Invocation

- **Dynamic port assignment for remote port forwarding (ssh -R 0:host:port)**
  A remote port of “0” can be specified in which case a dynamic port will be assigned on the server. The client will report a message with the specific ephemeral port assigned.
- **More flexibility in configuration files.**
  Match blocks have more criteria and can include more options within the block.
- **Support for public key (user and host) certificates.**
  These are not X.509 certificates, but a simpler implementation that is unique to OpenSSH. A single key (“CA key”) may sign (vouch for) the public keys of many users or servers. If a host or user trusts the CA public key, then it implicitly accepts the keys that have been signed by it. For more information, see the User's Guide / man page for the `ssh-keygen` command. These have been available for a few years, and are not used much. We do not have any Key Ring support for these or their associated keys.
- **Multiple user authentication methods.**
  The server (see: sshd_config / AuthenticationMethods) may specify that more than one authentication method is required for a/all user(s). For example: key + password.

Usage & Invocation

- **SFTP enhancements**
  - support for recursively transferring files in a directory tree (get/put -r)
  - sftp server read-only mode
  - sftp "`df`" command. (Display filesystem attributes)
  - improved performance of directory listings
  - "`ls -h`" option – human readable file attribute units

Usage & Invocation

- **Elimination of `ssh-rand-helper`**

  z/OS OpenSSH now requires a working `/dev/random` UNIX device.
  - `ssh-rand-helper` was slow, not as secure, and often timed out.
  - ICSF /dev/random support is now **required** to start ssh or sshd. Setup is as before. Note that with HCR77A0, a crypto card is not required. Also, CSFRNG check can be skipped by defining resource `CSF.CSFSERV.AUTH.CSFRNG.DISABLE` in class `XFACILIT`
  - If `/dev/random` is not available, then ssh/sshd will fail with:

    ```
    FOTS1949 PRNG is not seeded.  Please activate the Integrated
    Cryptographic Service Facility (ICSF).
    ```

Usage & Invocation

- **SMF record**
  - New algorithms are added into the related SMF record
  - sftp client records target path name in subtype 97
    - An additional triplet (section) was added to this record which contains the target (remote) path name for a SFTP client file transfer.
    - For SCP, this triplet will be present, but the count (SMF_119SSH_S6Num) and length (SMF_119SSH_S6Len) will be zero.

Usage & Invocation

- **SMF record (Continue)**
  - Two new SMF 119 records were added:
    - type 94(x'5E') Client connection started record
    - type 95(x'5F') Server connection started record
  - If SMF recording is configured (in zos_ssh_config / zos_sshd_config), they will be written just after the user has been authenticated by the server.
  - The content of these records is identical, and a subset of other 119 SSH records:
    - standard SMF 119 header
    - Common 119 TCP/IP identification section
    - SSH common security section (identifies which algorithms were used)
  - **Note:** BPX.SMF permission is now required for ssh client users if SMF recording is enabled, since the “ssh” command is not APF authorized.
  - Updated the C-level mapping macros in /samples/ssh_smf.h and the assembler mapping macros in SYS1.MACLIB(FOTSMF77)

Usage & Invocation

- **Run under OMVS**
  - ssh client command is enabled to run under TSO OMVS (3270), but prompting for passwords or pass phrases is not allowed.
- **IdentityKeyRingLabel**
  - double-quotes are optional when entered from an ssh (or sftp, scp) command line.
  - Example

  A key ring named SSHring that is owned by KeyRingOwnerID and a certificate labeled 'my label with blanks' is as follows:
  IdentityKeyRingLabel="KeyRingOwnerID/SSHring my label with blanks"

  If the option is specified as a command-line option, you might issue:
  -o IdentityKeyRingLabel="\"KeyRingOwnerID/SSHring my label with blanks\""

Interactions & Dependencies

- **Hardware Dependencies**
  - None.

- **Software Dependencies**
  - ICSF HCR7780 or later MUST be running.
    See “Installation” information for details

Migration & Coexistence Considerations

- As in previous releases, protocol 1 is disabled by default.
- Version 6.4 of OpenSSH changes sftp so that non-error messages are not printed to stdout if running a batch file (-b). In effect, the -q (quiet mode) option is turned on with -b and cannot be turned off. Since this will impact many customers, it has been changed in the z/OS port so that -b does not force -q. The -q option can be specified in addition to -b. Therefore this is not actually a migration action, but the behavior will not be consistent with other implementations.

Migration & Coexistence Considerations

- Default value/order changes for ssh_config and sshd_config (Continue)
  - Ciphers (ssh_config/sshd_config)

    aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,
    aes128-gcm@openssh.com,aes256-gcm@openssh.com,
    aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,
    aes256-cbc,arcfour
  - MACs (ssh_config/sshd_config)

    hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,
    umac-64-etm@openssh.com,umac-128-etm@openssh.com,
    hmac-sha2-256-etm@openssh.com,hmac-sha2-512-
    etm@openssh.com, hmac-ripemd160-etm@openssh.com,hmac-sha1-
    96-etm@openssh.com, hmac-md5-96-etm@openssh.com, hmac-
    md5,hmac-sha1,
    umac-64@openssh.com,umac-128@openssh.com, hmac-sha2-256,
    hmac-sha2-512,hmac-ripemd160,hmac-
    ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96.

Migration & Coexistence Considerations

- Default value changes for ssh_config and sshd_config (Continue)
  - GlobalKnownHostsFile (ssh_config)
    /etc/ssh/ssh_known_hosts, /etc/ssh/ssh_known_hosts2
  - HostKeyAlgorithms (ssh_config)
    ecdsa-sha2-nistp256-cert-v01@openssh.com ,
    ecdsa-sha2-nistp384-cert-v01@openssh.com,
    ecdsa-sha2-nistp521-cert-v01@openssh.com ,
    ssh-rsa-cert-v01@openssh.com , ssh-dss-cert-v01@openssh.com,
    ssh-rsa-cert-v00@openssh.com,ssh-dss-cert-v00@openssh.com,
    ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,
    ssh-rsa,ssh-dss
  - IdentityFile (ssh_config)
    For protocol version 2, the default is ~/.ssh/id_rsa, ~/.ssh/id_dsa, and ~/.ssh/id_ecdsa.
  - UserKnownHostsFile (ssh_config)
    ~/.ssh/known_hosts, ~/.ssh/known_hosts2.

Migration & Coexistence Considerations

- Default value changes for ssh_config and sshd_config
  - AuthorizedKeysFile (sshd_config)
    .ssh/authorized_keys, .ssh/authorized_keys2
  - HostKey (sshd_config)
    /etc/ssh/ssh_host_rsa_key, /etc/ssh/ssh_host_dsa_key and /etc/ssh/ssh_host_ecdsa_key

Migration & Coexistence Considerations

Changes to the ssh_config file for new enhancements

What Changed	Customization action needed?
The ControlPath keyword Previously, %l in the path was substituted by the local host name. Now, %l in the path is substituted by the local host name(including any domain name).	Yes, if you want to use substitute character to substitute the local host name without any domain name. Action: Use the %L in the path to substitute the first component of the local host name.
The **RhostsAuthentication** keyword Previously, this option was supported for protocol version 1. Now this option is no longer supported for protocol version 1 on z/OS Unix.	Yes, if you use RhostsAuthentication for protocol version 1 in your application. When setting it, message "*filename* line *line_number*: Deprecated option *keyword" is returned.* **Action:** Update your application.

Migration & Coexistence Considerations

Changes to the sshd_config file for new enhancements

What Changed	Customization action needed?
The **RhostsAuthentication** keyword Previously, this option was supported for protocol version 1. Now this option is no longer supported for protocol version 1 on z/OS Unix.	Yes, if you use RhostsAuthentication for protocol version 1 in your application. When setting it, FOTS2374 "*filename* line *line_number*: Deprecated option *keyword" is returned.* **Action:** Update your application.
The ServerKeyBits keyword Previously, the default number of bits in the ephemeral protocol version 1 server key was 768. Now the default number of bits in the ephemeral protocol version 1 server key is 1024.	Yes, if you use the ephemeral protocol version 1 server key which is 768 bits. **Action:** Start the sshd daemon with specifying -b 768, if you want to use the old default.

Migration & Coexistence Considerations

Changes to the sshd command for new enhancements

What Changed	Customization action needed?
The -b option Previously, the default number of bits in the ephemeral protocol version 1 server key was 768. Now the default number of bits in the ephemeral protocol version 1 server key is 1024.	Yes, if you use the ephemeral protocol version 1 server key which is 768 bits. **Action:** Start the sshd daemon with specifying -b 768.

Migration & Coexistence Considerations

Changes to the ssh-keygen command for new enhancements

What Changed	Customization action needed?
-d option Previously, -d option as alias of '-t dsa' was supported. Now it is not supported.	Yes, if you use ssh-keygen command with -d option. If specifying -d option, error message "unknown option -- d" is returned. Action: replace -d by '-t dsa' .
-b option (for RSA) Previously, the maximum RSA key size on the ssh-keygen -b option was 32768. Now the maximum size is 16384.	Yes, if you are using **ssh-keygen** to generate RSA keys with a size that is between 16384 and 32768 bits. If specifying the RSA key size which is larger than 16384, error message "key bits exceeds maximum 16384" is returned. **Action:** Use **ssh-keygen** to generate new RSA keys based on the new size requirement.

Migration & Coexistence Considerations

Changes to the ssh-keyscan command for new enhancements

What Changed	Customization action needed?
The -t option Previously, If the -t option was not specified, ssh-keyscan searches only for SSH protocol version 1 keys ("rsa1") by default. Now If the -t option is not specified, ssh-keyscan searches only for SSH protocol version 2 “rsa” and “ecdsa” keys by default.	Yes, if you search protocol version 1 keys ("rsa1") without specifying -t option. **Action:** Search protocol version 1 keys ("rsa1") with specifying -t rsa1.

Migration & Coexistence Considerations

Changes to the sftp command for new enhancements

What Changed	Customization action needed?
The -P option Previously, this option was used to specify the sftp_server_path. Now, this option is used to specify the port to connect to on the remote host.	Yes, if you specified the sftp_server_path. If specifying the -P sftp_server_path, FOTS1401 "*filename* line *line number*: Bad number *number*" is returned. Action: Use the -D option to specified the sftp_server_path.
Ln subcommand Priviously, the ln subcommand created a symbolic link from oldpath to newpath on the remote host. Now, If the -s flag is specified the created link is a symbolic link, otherwise it is a hard link.	Yes, if you create a symbolic link. Action: Run the sftp ln subcommand with the -s flag to create a symbolic link or create a hard link without flag.

Migration & Coexistence Considerations

Changes to the ssh-rand-helper command for new enhancements

What Changed	Customization action needed?
ssh-rand-helper Now the ssh-rand-helper is not supported.	Yes. If no migration action, FOTS1949 message “PRNG is not seeded. Please activate the Integrated Cryptographic Service Facility (ICSF)” is returned. Action: The new OpenSSH requires that a working /dev/random device be available to all OpenSSH client and server jobs. This requires that ICSF be configured to support /dev/random and that users have SAF authority to the CSFRNG service.

Migration & Coexistence Considerations

Changes to the /samples/ssh_smf.h and FOTSMF77 in SYS1.MACLIB for new enhancements

What Changed	Customization action needed?
/samples/ssh_smf.h and SYS1.MACLIB(FOTSMF77) For more information, see "SMF Type 119 records for OpenSSH".	Yes, if you use ssh_smf.h and FOTSMF77. Action: Update your application.

Installation

- **z/OS Ported Tools OpenSSH V1R3 is supported on z/OS 1.13 and later.**

  OpenSSH V2R2 is packaged as a base element of z/OS V2R2.

- **New release installs over the previous release.**

- **ICSF FMID HCR7780 or later is required with PTF for APAR OA45548. OpneSSH V1R3 and V2R2 will not run without ICSF started, since /dev/random is now required.**
  - **Note:** HCR77A0 or later will support /dev/random without a crypto card.
  - **Note:** HCR77A1 allows for SAF checking of CSFRNG to be disabled

- **Verifying version:**

```
$ ssh -V
OpenSSH_6.4p1, OpenSSL 1.0.1c 10 May 2012

$ /usr/sbin/sshd -d -t
…
debug1: sshd version OpenSSH_6.4p1, OpenSSL 1.0.1c 10 May 2012
```

Installation

- **Updated OpenSSH for z/OS V1R3 parts:**
  - /bin/ssh
  - /bin/scp
  - /bin/sftp
  - /bin/ssh-add
  - /bin/ssh-agent
  - /bin/ssh-keygen
  - /bin/ssh-keyscan
  - /usr/lib/ssh/ssh-keysign
  - ~~/usr/lib/ssh/ssh-rand-helper~~ (**removed**!)
  - /usr/lib/ssh/sftp-server
  - /usr/sbin/sshd
  - /usr/lib/nls/msg/C/openssh.cat
  - /usr/man/C/man1/fotz200.book
  - /samples/ssh_smf.h
  - SYS1.MACLIB(FOTSMF77)
- extended attributes unchanged from previous release.

Presentation Summary

- Many features and enhancements provided by this upgrade
- Resolved several customer requirements
- Important migration and coexistence considerations

Appendix

- See the updated *IBM Ported Tools for z/OS: OpenSSH User's Guide* for more information (Order Number: SA23-2246-03)
- Website References:
  - IBM Ported Tools for z/OS
    http://www-03.ibm.com/servers/eserver/zseries/zos/unix/ported/
  - IBM Ported Tools for z/OS: OpenSSH
    http://www-03.ibm.com/servers/eserver/zseries/zos/unix/ported/openssh/index.html
  - OpenSSH http://www.openssh.org/
  - OpenSSL http://www.openssl.org/

Appendix

- **ICSF Reference Guides:**
  - *z/OS Cryptographic Services ICSF Overview* (Order Number: SA22-7519)
  - *z/OS Cryptographic Services ICSF Administrator's Guide* (Order Number: SA22-7521)
  - *z/OS Cryptographic Services ICSF System Programmer's Guide* (Order Number: SA22-7520)
  - *z/OS Cryptographic Services ICSF Application Programmer's Guide* (Order Number: SA22-7522)
  - *z/OS Cryptographic Services Writing PKCS #11 Applications* (Order Number: SA23-2231)
  - ftp://public.dhe.ibm.com/s390/zos/icsf/pdf/OA45548.pdf
- **Other Reference Guides:**
  - *Program Directory for IBM Ported Tools for z/OS* (Order Number: GI10-0769)