IBM Ported Tools for z/OS OpenSSH V1R2

Richard Theis (rtheis@us.ibm.com)
IBM Rochester, MN

Session 9684
August 11, 2011

Trademarks and Disclaimers

- **See http://www.ibm.com/legal/copytrade.shtml for a list of IBM trademarks.**
- **The following are trademarks or registered trademarks of other companies**
  - UNIX is a registered trademark of The Open Group in the United States and other countries
  - CERT® is a registered trademark and service mark of Carnegie Mellon University.
  - ssh® is a registered trademark of SSH Communications Security Corp
  - X Window System is a trademark of X Consortium, Inc
- **All other products may be trademarks or registered trademarks of their respective companies**

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

>> Overview <<

Packaging and installation

Requirements addressed

Service notes

Migration and coexistence

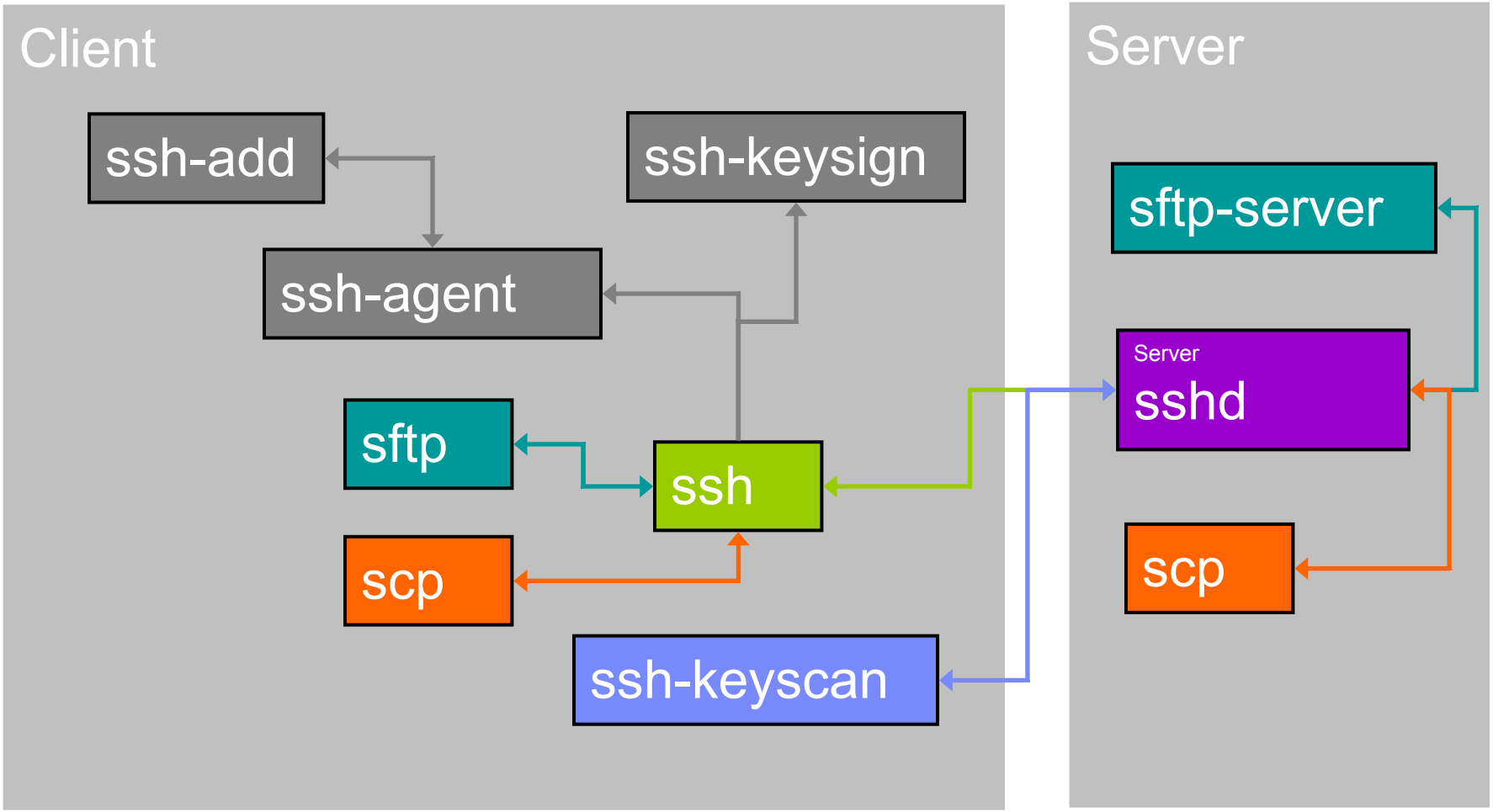
Troubleshooting information

Appendix

Overview: OpenSSH

- **What is OpenSSH?**
  - Suite of network connectivity tools that provide secure encrypted communications between two un-trusted hosts over an insecure network.
- **What security does OpenSSH provide?**
  - Data privacy through encryption
  - Data integrity to guarantee unaltered communications
  - Authentication of users and servers
  - Authorization of user actions
  - Forwarding to protect other TCP/IP-based applications

Overview: OpenSSH



Overview: OpenSSH for z/OS Products

- **"Tools and Toys" OpenSSH for z/OS**
  - Non-priced tool (never an official product)
  - Never officially supported
  - No longer available

Overview: OpenSSH for z/OS Products

- **IBM Ported Tools for z/OS: OpenSSH V1R1**
  - GA Version (May 2004): OpenSSH 3.5p1, OpenSSL 0.9.7b, zlib 1.1.4, x11-ssh-askpass 1.2.4.1
  - APAR OA10315 Version (April 2005): OpenSSH 3.8.1p1, OpenSSL 0.9.7d, zlib 1.1.4, x11-ssh-askpass 1.2.4.1
  - Non-priced program product (not part of z/OS)
  - Supported on z/OS 1.4 and later
  - No longer orderable but still supported

Overview: OpenSSH for z/OS Products

- **(NEW) IBM Ported Tools for z/OS: OpenSSH V1R2**
  - GA Version (July 2010): OpenSSH 5.0p1, OpenSSL 0.9.8k, zlib 1.2.3, x11-ssh-askpass 1.2.4.1
  - Non-priced program product (not part of z/OS)
  - Supported on z/OS 1.10 and later
  - Order from ShopzSeries
  - a.k.a. “OpenSSH for z/OS” throughout this presentation

Agenda

Overview

>> Packaging and installation <<

Requirements addressed

Service notes

Migration and coexistence

Troubleshooting information

Appendix

Packaging and installation

- New release (V1R2 - FMID HOS1120) installs over the previous release (V1R1 - FMID HOS1110)
- Cannot order the previous release now that the new release is available
- New release supported on z/OS 1.10 and later
- z/OS 1.10 and z/OS 1.11 requirement: PTFs for APARs PK86329 and OA29401 must be applied.

Packaging and installation

- **Important extended attributes settings set during install**
  - NEW: sshd, scp, sftp and sftp-server must have the APF-authorized extended attribute set (i.e. extattr +a)
  - NEW: ssh and ssh-keysign must have the noshareas extended attribute set
    (i.e. extattr –s)
  - sshd must have the noshareas extended attribute set (i.e. extattr –s)
  - sshd must have the program control extended attribute set (i.e. extattr +p)

Packaging and installation

- See the “What you need to verify before using OpenSSH” section in the user’s guide for details
- Xvfb split (separate book and FMID HVFB111) from OpenSSH for z/OS

Agenda

Overview

Packaging and installation

>> Requirements addressed <<

Service notes

Migration and coexistence

Troubleshooting information

Appendix

Requirements addressed: Overview

- Upgrade versions of OpenSSH, OpenSSL and zlib
- Provide SMF support
- Provide SAF key ring support
- Miscellaneous requirements

Requirements addressed: Upgrade

- **Problem statement**
  - OpenSSH for z/OS needs to upgrade the open source versions of OpenSSH, OpenSSL and zlib to address various functional, performance and security requirements.
- **Solution**
  - Upgraded to OpenSSH 5.0p1
  - Upgraded to OpenSSL 0.9.8k
  - Upgraded to zlib 1.2.3
  - Recompiled with XPLINK to improve overall performance

Requirements addressed: Upgrade

- **Benefits**
  - Functional: Compression with privilege separation support
  - Functional and Performance: Connection sharing support **(See illustration #1)**
  - Security: Delayed compression option
  - Security: Restricted environment support for SSH clients **(See illustration #2)**
  - Security: Hashed hostname and address support
  - Security: Support for arcfour128 and arcfour256 ciphers
  - Security: Support for umac64@openssh.com MAC
  - General: Currency with open source enhancements and fixes

Illustration #1: Connection Sharing

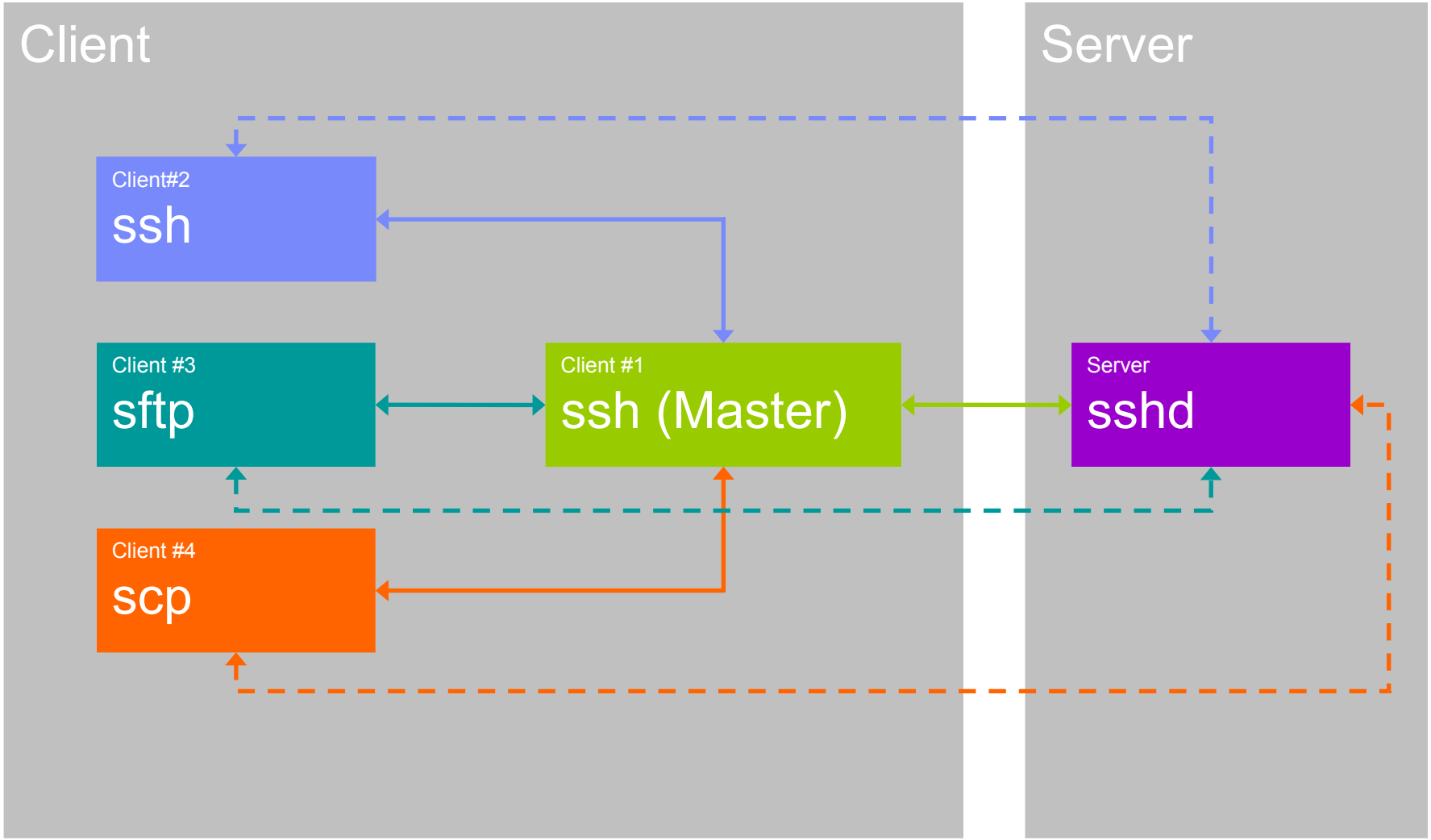
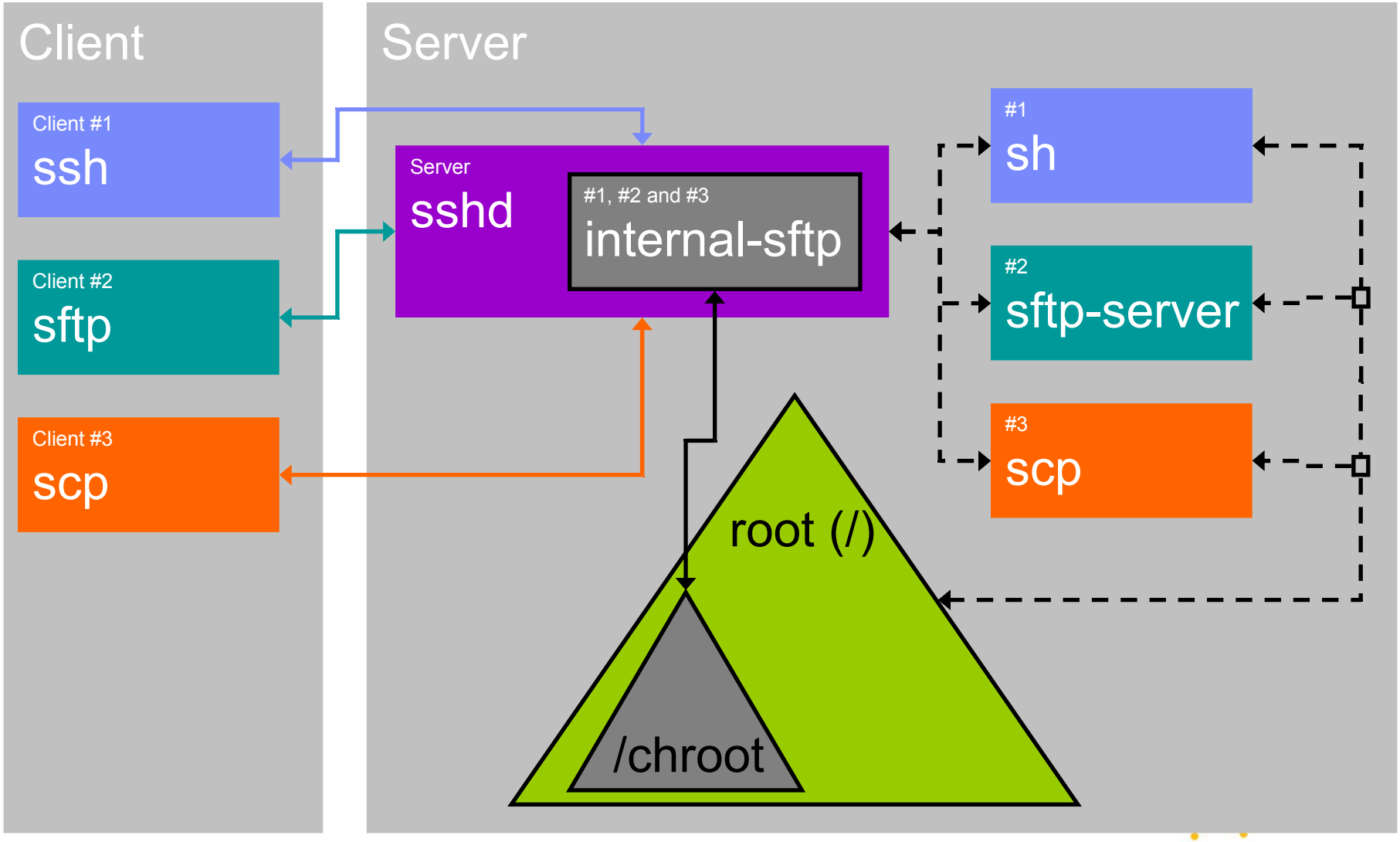


Illustration #2: Restricted Environment



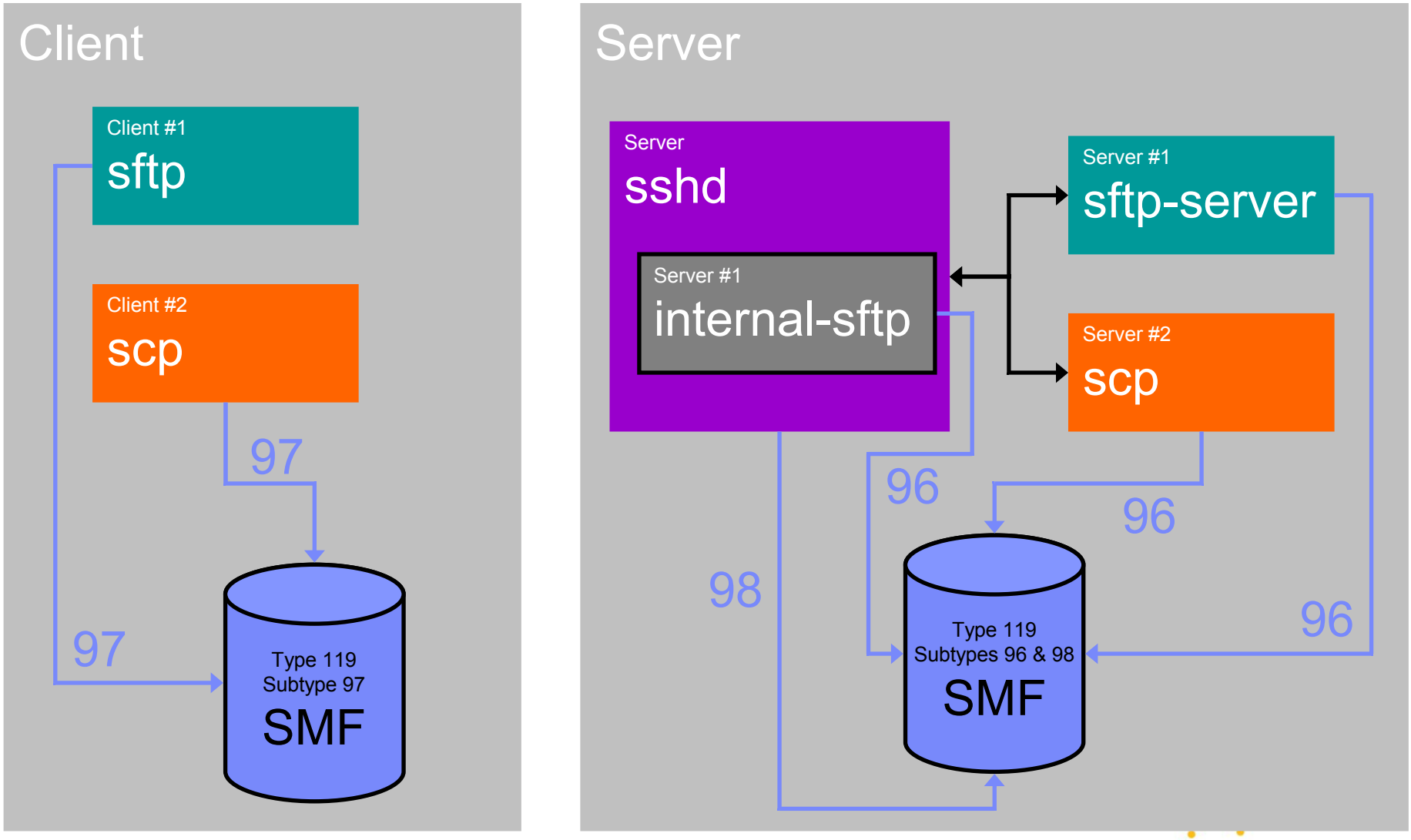
Requirements addressed: SMF

- **Problem statement**
  - OpenSSH for z/OS needs to audit file transfers and login failures.
- **Solution**
  - SMF records generated for both client & server file transfers
  - SMF records generated for login failures
  - New SMF server transfer completion record (Type 119 - Subtype 96)
  - New SMF client transfer completion record (Type 119 - Subtype 97)
  - New SMF login failure record (Type 119 - Subtype 98)

Requirements addressed: SMF

- **Benefits**
  - SMF records audit scp, sftp, sftp-server and sshd activity **(See illustration #3)**
  - New SMF records are customized for OpenSSH for z/OS
  - Support for SMF record exit IEFU83 or IEFU84

Illustration #3: SMF Records



Requirements addressed: Key Rings

- **Problem statement**
  - OpenSSH for z/OS needs to support getting OpenSSH keys (RSA and DSA) from SAF key rings.
- **Solution**
  - OpenSSH for z/OS keys can be stored in a digital certificate connected to a SAF key ring
  - New features available for ssh, scp, sftp, ssh-add, ssh-keygen and sshd to get keys from a SAF key ring

Requirements addressed: Key Rings

- **Benefits**
  - SAF (e.g. RACF) control of OpenSSH for z/OS keys for SSH protocol version 2
  - Supports server authentication when keys are stored in key rings **(See illustration #4)**
  - Supports user authentication when keys are stored in key rings **(See illustration #5)**
  - Supports mixing key storage – key rings and UNIX files **(See illustration #6)**
  - Supports real or virtual key rings
  - Additional features available (e.g. expired certificate, signing, etc.)

Illustration #4: Server authentication

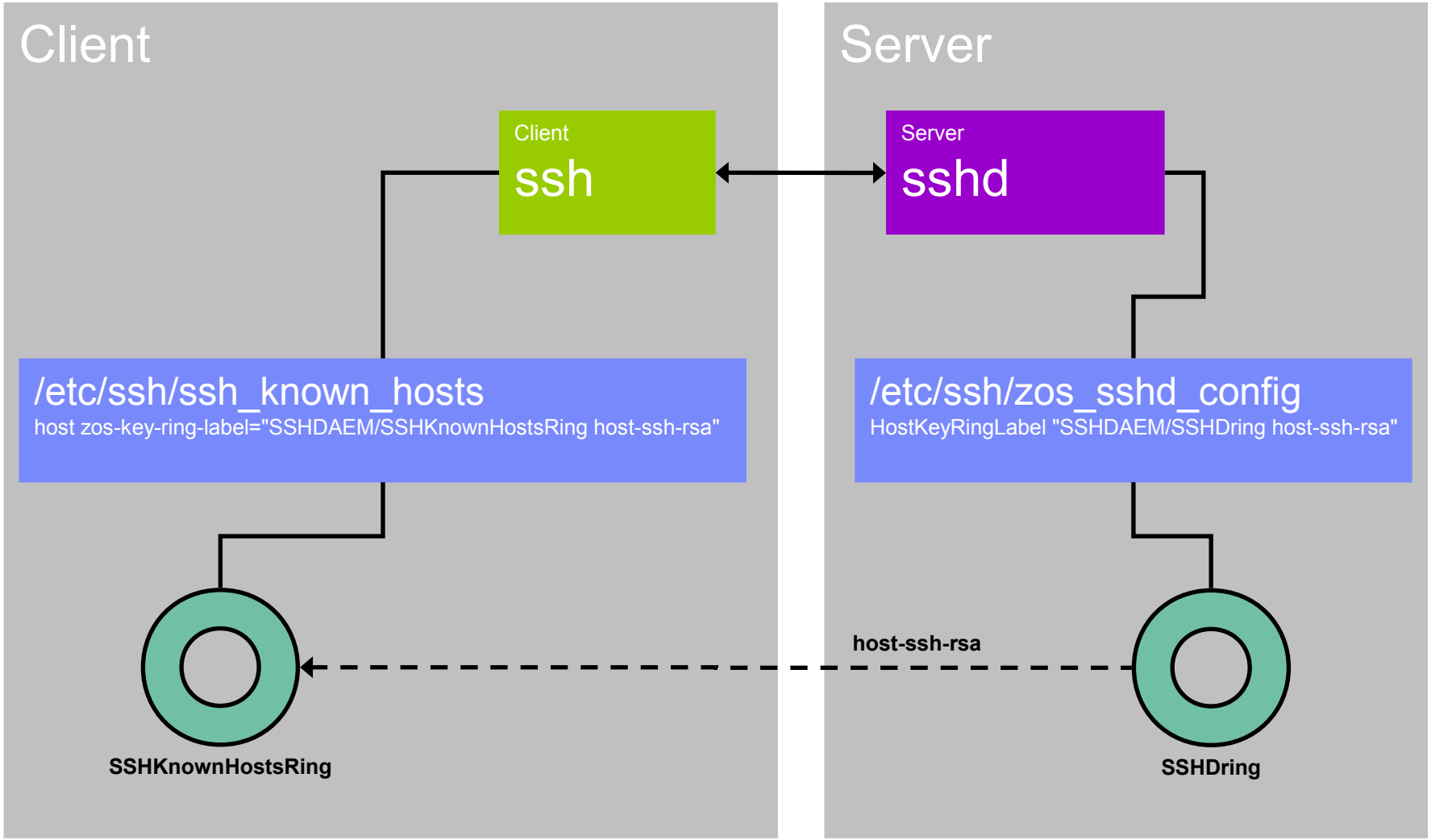


Illustration #5: User authentication

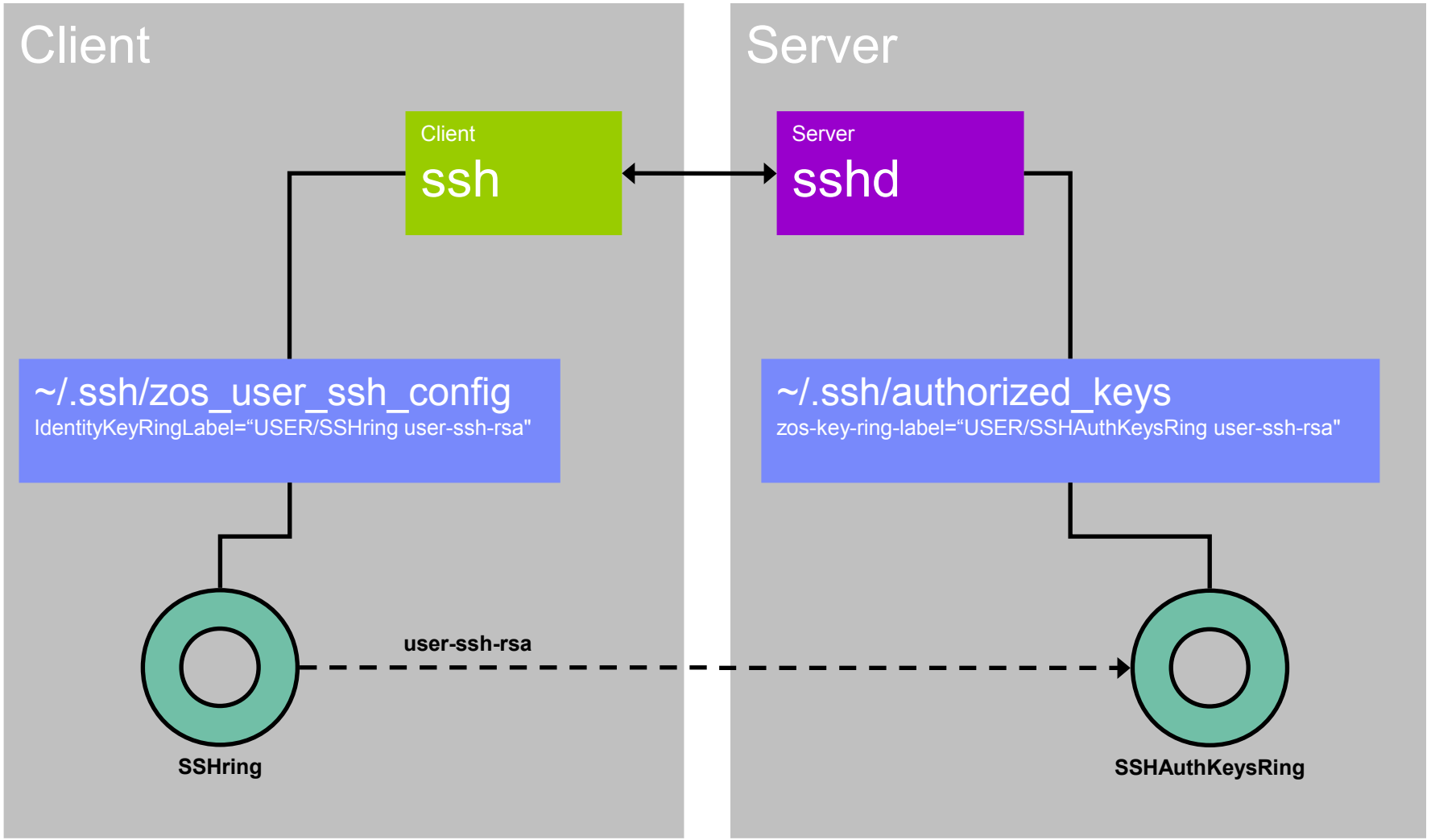
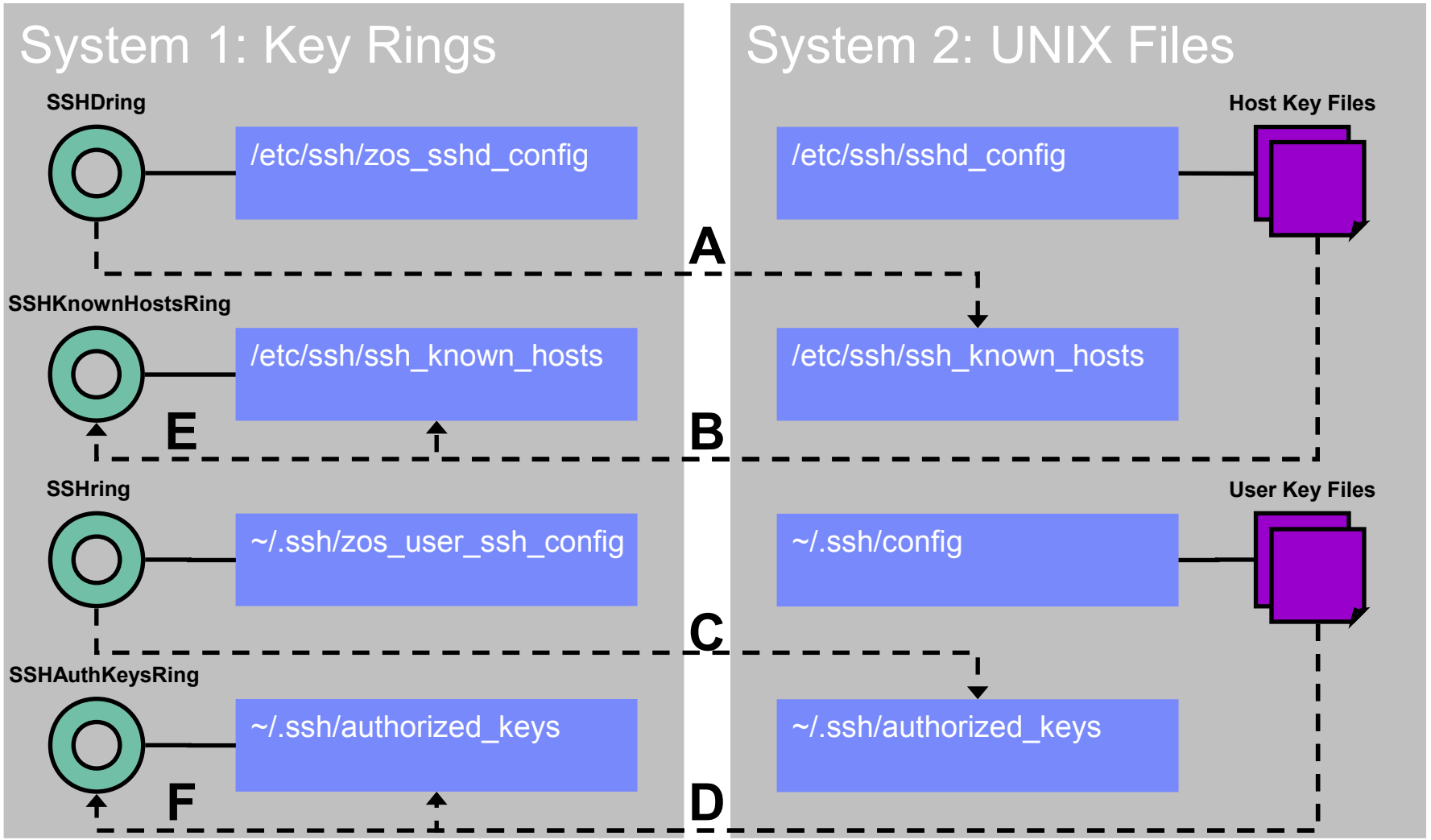


Illustration #6: Mixing key storage



Requirements addressed: Miscellaneous

- **Problem statement**
  - OpenSSH for z/OS needs to provide a configurable timeout value for ssh-rand-helper.
- **Solution**
  - New _ZOS_SSH_PRNG_CMDS_TIMEOUT environment variable
- **Benefits**
  - Improved ssh-rand-helper support on heavily loaded systems

Requirements addressed: Miscellaneous

- **Problem statement**
  - OpenSSH for z/OS needs to improve message support.
- **Solution**
  - New _ZOS_OPENSSH_MSGCAT environment variable
  - All error-related messages are now documented
- **Benefits**
  - Enables quicker identification of problems

Requirements addressed: Miscellaneous

- **Problem statement**
  - OpenSSH for z/OS needs to improve support for users that share a UID.
- **Solution**
  - Current MVS identity used to determine user name and initial working directory
- **Benefits**
  - Improves ssh, ssh-add, ssh-keygen, ssh-rand-helper and sshd functionality for users that share a UID

Agenda

Overview

Packaging and installation

Requirements addressed

>> Service notes <<

Migration and coexistence

Troubleshooting information

Appendix

Service notes

- **V1R2: DOC APARs OA34819, OA34378 and OA33914**
  - Document 3 new migration actions.
  - Update documentation for 1 migration action.
- **V1R2: PER APAR OA34210**
  - Fixes SMF Type 119 subtype 97 record problem when using “sftp user@ host:file1 file2” file transfer syntax.
- **V1R2: UR1 APAR OA36257**
  - Noise error message when using nested ssh client after enabling SMF to collect Type 119 subtype 96 records.

Service notes

- **V1R2: sftp –b //DD:FTP and APF authorized problem**
  - OpenSSH for z/OS (V1R1 or V1R2) doesn't support MVS data sets.
  - Turning off sftp APF-authorized bit may provide unsupported circumvention but sacrifices SMF support.
- **V1R1 and V1R2: Packet problems "Bad packet length" and "Corrupted MAC on input"**
  - Affects SSH protocol version 2
  - Check hardware, firewalls, network, inetd, etc.
  - See the following website for details: http://blogs.oracle.com/janp/entry/ssh_messages_code_bad_packet

Service notes

- **V1R1 and V1R2: Loop when using SSH_ASKPASS in batch**
  - Affects OpenSSH in general
  - Running in batch and telling OpenSSH that you aren't can cause an infinite loop (i.e. sftp -oBatchMode=no).
  - Circumvent by changing StrictHostKeyChecking to yes or no depending on how much you trust the host.
- **V1R1 and V1R2: OpenSSH for z/OS isn't a FIPS 140-2 compliant application.**

Agenda

Overview

Packaging and installation

Requirements addressed

Service notes

>> Migration and coexistence <<

Troubleshooting information

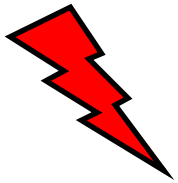
Appendix

Migration and coexistence

- Migration actions
- Coexistence considerations
- See the “Migrating to Version 1 Release 2 of IBM Ported Tools for z/OS: OpenSSH” chapter in the user’s guide.

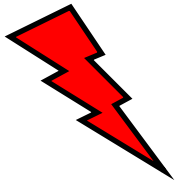
Take special note of the migration actions with this symbol

Migration action: sftp batch mode



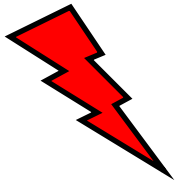
- **What changed**
  - When the sftp command is run with the –b option, the -oBatchMode=yes argument is now passed to the ssh command.
- **When is a migration action needed**
  - If you use the sftp command with the –b option and require password, passphrase or host key prompts during authentication. For example, if you use the SSH_ASKPASS environment variable for user authentication, this migration action is required since using SSH_ASKPASS requires a passphrase prompt.

Migration action: sftp batch mode (Continued)



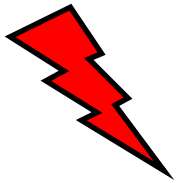
- **Migration action**
  - Run the sftp command with -oBatchMode=no as the first option.
- **Commands, options or keywords affected**
  - sftp –b command-line option
- **References**
  - Migration action updated with DOC APAR OA33914.

Migration action: OpenSSH heap management



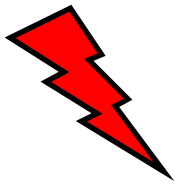
- **What changed**
  - OpenSSH changed how it manages user heap storage for data transfers.
- **When is a migration action needed**
  - If you limit the amount of storage available to the processes running OpenSSH commands.
- **Migration action**
  - Refer to the “OpenSSH heap management” section in the user’s guide for details on action options: _CEE_RUNOPTS=“HEAP(,,,FREE)”, _CEE_REALLOC_CONTROL=“256K,25” or increase storage available to OpenSSH.

Migration action: OpenSSH heap management (Continued)



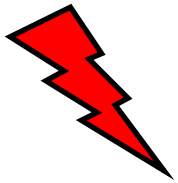
- **Commands, options or keywords affected**
  - All OpenSSH commands
- **References**
  - Migration action new with DOC APAR OA34819.

Migration action: sftp special characters



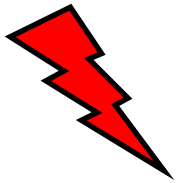
- **What changed**
  - Previously, sftp subcommand parsing handled certain special characters (for example, '#' and glob characters) differently. Now sftp subcommand parsing is more consistent with shell command parsing.
- **When is a migration action needed**
  - If you use special characters on sftp subcommands.
- **Migration action**
  - Escape special characters with the backslash character.

Migration action: sftp special characters (Continued)



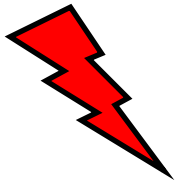
- **Commands, options or keywords affected**
  - sftp command
- **References**
  - Migration action new with DOC APAR OA34819.

Migration action: ssh-rand-helper ~/.ssh/ directory creation



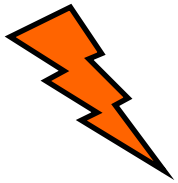
- **What changed**
  - The ssh-rand-helper command now fails if a user's ~/.ssh/ directory does not exist and can not be created.
- **When is a migration action needed**
  - If you use ssh-rand-helper to generate random numbers for OpenSSH and an OpenSSH user doesn't have and can not create a ~/.ssh/ directory.
- **Migration action**
  - Ensure that all OpenSSH users have or can create a ~/.ssh/ directory.

Migration action: ssh-rand-helper ~/.ssh/ directory creation (Continued)



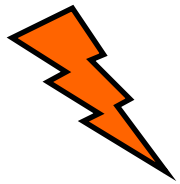
- **Commands, options or keywords affected**
  - All OpenSSH commands
- **References**
  - Migration action new with DOC APAR OA34378.

Migration action: ~/.ssh/config owner and permissions check



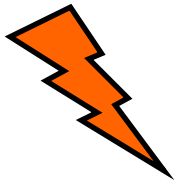
- **What changed**
  - Previously, if the user was using the default configuration file (~/.ssh/config), the owner or permissions on the file was not checked. Now ssh issues an error message and exits if the file is not owned by the user or if the file is writable by the world or the file's group.
- **When is a migration action needed**
  - If your file has incorrect owner or permissions.
- **Migration action**
  - Correct the settings so they adhere to the new requirements.
- **Commands, options or keywords affected**
  - ssh command

Migration action: sshd full path name



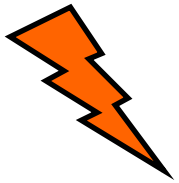
- **What changed**
  - Previously, the sshd daemon could be started using a relative path name (for example, ./sshd). Now a full path name must be used instead of the relative path name.
- **When is a migration action needed**
  - If you use a relative path name when starting the sshd daemon.
- **Migration action**
  - Change the startup process to use the full path name instead of a relative path name.
- **Commands, options or keywords affected**
  - sshd command

Migration action: Address parsing changes



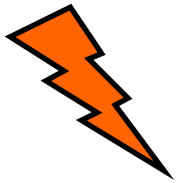
- **What changed**
  - Previously, addresses containing a colon (:) character could be parsed using the forward slash (/) character and vice versa. Now addresses containing delimiter characters (: or /) must be enclosed in square brackets.
- **When is a migration action needed**
  - If you use an address that contains delimiter characters.
- **Migration action**
  - Enclose the address in square brackets.

Migration action: Address parsing changes (Continued)



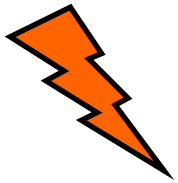
- **Commands, options or keywords affected**
  - ssh –L and –R command-line options
  - ssh_config LocalForward and RemoteForward keywords
  - permitopen authorized_keys file format option

Migration action: Default value change for AllowTcpForwarding



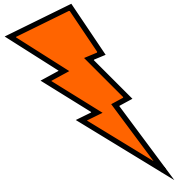
- **What changed**
  - Previously, the default value was "yes". Now it is "no".
- **When is a migration action needed**
  - If you want to continue to allow port forwarding. This default was changed to reduce exposure to a vulnerability reported as CVE-2004-1653.
- **Migration action**
  - Set AllowTcpForwarding to "yes".
- **Commands, options or keywords affected**
  - sshd_config AllowTcpForwarding keyword

Migration action: Input value changes for ssh-keygen –b



- **What changed**
  - Previously, the minimum RSA key size on the ssh-keygen -b option was 512 bits and the default was 1024 bits. Now the minimum RSA key size is 768 bits and the default is 2048 bits. The maximum remains 32768 bits.
  - Previously, the DSA key size on the ssh-keygen –b option was allowed to be between 512 and 32768 bits. Now the DSA key size must be 1024 bits.

Migration action: Input value changes for ssh-keygen –b (Continued)



- **When is a migration action needed**
  - If you are using ssh-keygen to generate RSA keys with a size that is less than 768 bits.
  - If you are using ssh-keygen to generate DSA keys with a size that is not equal to 1024 bits.
- **Migration action**
  - Use ssh-keygen to generate new RSA and DSA keys based on the new size requirements.
- **Commands, options or keywords affected**
  - ssh-keygen –b command-line option

Migration action: XPLINK environment

- **What changed**
  - Beginning in Version 1 Release 2, IBM Ported Tools for z/OS: OpenSSH is an XPLINK application. XPLINK (Extra Performance Linkage) is a type of call linkage that can improve performance in an environment of frequent calls between small functions.
- **When is a migration action needed**
  - If the XPLINK environment is not set up.

Migration action: XPLINK environment (Continued)

- **Migration action**
  - To set up the XPLINK environment (that is, to initialize the resources necessary to run an XPLINK application), do the following:
    - Put the Language Environment run-time library SCEERUN2 in the LNKLST member of SYS1.PARMLIB.
    - Put the XPLINK modules in SCEERUN2 in the dynamic LPA.
- **Commands, options or keywords affected**
  - All OpenSSH commands

Migration action: Message numbers

- **What changed**
  - Previously, to associate message numbers (for example, FOTSnnnn) with OpenSSH error messages, the NLSPATH environment variable had to include the following path: /usr/lib/nls/msg/%L/%N.cat. Starting in Version 1 Release 2, message numbers for IBM Ported Tools for z/OS: OpenSSH are associated with OpenSSH error messages by default.
- **When is a migration action needed**
  - If you do not want message numbers to be associated with OpenSSH error messages.

Migration action: Message numbers (Continued)

- **Migration action**
  - Set environment variable _ZOS_OPENSSH_MSGCAT="NONE" before running an OpenSSH command. If you have previously modified the NLSPATH environment variable, you do not need to make any changes to it.
- **Commands, options or keywords affected**
  - All OpenSSH commands

Migration action: Default value change for ciphers list

- **What changed**
  - Previously, the default cipher list did not contain arcfour128 and arcfour256. Now the default cipher list contains arcfour128 and arcfour256. The order was also changed to prefer ciphers that are not susceptible to security vulnerability CVE-2008-5161.
- **When is a migration action needed**
  - If you used the previous default list and do not want to allow the new ciphers or the new order of the preferred ciphers.
- **Migration action**
  - Specify the previous default list.

Migration action: Default value change for ciphers list (Continued)

- **Commands, options or keywords affected**
  - ssh –c command-line option
  - ssh_config Ciphers keyword
  - sshd_config Ciphers keyword

Migration action: Default value change for MACs list

- **What changed**
  - Previously, the default MACs list did not contain umac64@openssh.com. Now the default MACs list contains umac64@openssh.com.
- **When is a migration action needed**
  - If you used the previous default list and do not want to allow the new MAC.
- **Migration action**
  - Specify the previous default list.

Migration action: Default value change for MACs list (Continued)

- **Commands, options or keywords affected**
  - ssh –m command-line option
  - ssh_config MACs keyword
  - sshd_config MACs keyword

Migration action: Minimum value change for RekeyLimit

- **What changed**
  - Previously, the minimum value was 0. Now the minimum value is 16.
- **When is a migration action needed**
  - If you use a RekeyLimit value that is less than 16.
- **Migration action**
  - Change the value so that the RekeyLimit value is greater than or equal to 16.
- **Commands, options or keywords affected**
  - ssh_config RekeyLimit keyword

Migration action: ProxyCommand shell

- **What changed**
  - Instead of running ProxyCommand with the /bin/sh shell, the user's shell as set in the SHELL environment variable is used.
- **When is a migration action needed**
  - If you use a shell other than /bin/sh (e.g. /bin/tcsh).
- **Migration action**
  - Make sure that ProxyCommand conforms to your shell's syntax.
- **Commands, options or keywords affected**
  - ssh_config ProxyCommand keyword

Migration action: ssh-keygen -r

- **What changed**
  - Previously, if the file name was not specified, a prompt for the file name was issued. Now the default file names for RSA and DSA keys are used instead.
- **When is a migration action needed**
  - If you did not specify a file name.
- **Migration action**
  - Specify the file name on the ssh-keygen command.
- **Commands, options or keywords affected**
  - ssh-keygen –r command-line option

Migration action: ssh-keygen -f

- **What changed**
  - Instead of truncating a long file name at 1023 characters, a message is issued.
- **Migration action**
  - None.
- **Commands, options or keywords affected**
  - ssh-keygen –f command-line option

Migration action: ssh-keygen without the –d or –t options

- **What changed**
  - Previously, if ssh-keygen was issued without the –d or –t options, a message was issued. Now RSA is used as the default key type.
- **Migration action**
  - None. Previously successful ssh-keygen commands will continue to be successful.
- **Commands, options or keywords affected**
  - ssh-keygen

Coexistence considerations

- **Coexistence considerations**
  - In a sysplex environment, some systems might share the same configuration. They might also share the ssh_known_hosts or authorized_keys files. However, those systems might have different versions of ssh or sshd. In that situation, the previous version of the command might exit with an error message because it does not support the new features.
  - When a newer version of the SSH client is trying to connect to a previous version of the sshd daemon, connection might not be established due to incompatibility of the new configuration options.

Coexistence considerations (Continued)

- **Options to avoid sharing the files affected**
  - ssh_config: ssh –F command-line option
  - sshd_config: sshd –f command-line options
  - ssh_known_hosts: ssh_config GlobalKnownHostsFile or UserKnownHostsFile keywords
  - authorized_keys: sshd_config AuthorizedKeysFile keyword

Agenda

Overview

Packaging and installation

Requirements addressed

Service notes

Migration and coexistence

>> Troubleshooting information <<

Appendix

Troubleshooting information: Upgrade

- Verify upgrade installed

```
> ssh -V
OpenSSH_5.0p1, OpenSSL 0.9.8k 25 Mar 2009
```

- Tracing added for z/OS additions and changes (e.g. `debug1: zsshSmfSetConnSmfStatus: SMF status is 0`)
- See the “Troubleshooting” and “OpenSSH vulnerabilities” chapters in the user’s guide for general OpenSSH for z/OS service information.

Troubleshooting information: Upgrade

- **Common "restricted environment support for SSH clients" problems**
  - Insecure components of the sshd_config ChrootDirectory
    - Must be owned by UID 0
    - Must not have write permission for group or others
  - Missing files or directories to support the client's session (e.g. /bin/sh)
  - Confusion as to when the chroot occurs (refer to the "Login process" section under the sshd command description in the user's guide for more information)

Troubleshooting information: Upgrade

- **Common “restricted environment support for SSH clients” problems (Continued)**
  - ssh and scp clients will hang if server forces sftp (e.g. ForceCommand internal-sftp) - this is working-as-designed
  - See the “Limiting file system name space for sftp users” section in the user’s guide for more information on setting up a restricted environment for SSH clients.

Troubleshooting information: SMF

- **Incomplete setup often cause of "problems" (refer to the "Setting up OpenSSH to collect SMF records" section in the user's guide)**
  - Update the SMFPRMxx parmlib member
  - Enable OpenSSH for z/OS SMF recording (i.e. ClientSMF and ServerSMF keywords)
  - z/OS 1.10 and z/OS 1.11 only: Verify the PTFs for APARs PK86329 and OA29401 are applied
- Subtype 98 records are for user authentication failures (e.g. bad password, key problems, etc.) and not for general problems connecting to the sshd daemon.

Troubleshooting information: Key Rings

- Incorrect authority or ownership setup for key rings or certificates often cause of “problems”
- Certificate “not found” errors could also be the result of an authority failure
- ssh-keygen –e, –l, and –B command-line options can be useful service tools for debugging public keys problems
- ssh-agent and ssh-add can be useful service tools for debugging private key problems

Agenda

Overview

Packaging and installation

Requirements addressed

Service notes

Migration and coexistence

Troubleshooting information

>> Appendix <<

What's new or changed: Upgrade

- **Connection sharing support**
  - New ssh –M, -O and –S command-line options
  - New ssh_config ControlMaster and ControlPath keywords
- **Restricted environment support for SSH clients**
  - New sshd_config ChrootDirectory, ForceCommand and Match keywords
  - New "internal-sftp" support (see sshd_config ForceCommand and Subsystem keywords)

What's new or changed: Upgrade

- **Hashed hostname and address support**
  - New ssh-keyscan –H command-line option
  - New ssh-keygen –F, -H and –R command-line options
  - New ssh_known_hosts file format support for hashed hostnames and addresses
  - New ssh_config HashKnownHosts keyword

What's new or changed: Upgrade

- **Security enhancements**
  - New arcfour128 and arcfour256 ciphers supported on the ssh –c command-line option, ssh_config Ciphers keyword and sshd_config Ciphers keyword
  - New umac64@openssh.com MAC supported on the ssh –m command-line option, ssh_config MACs keyword and sshd_config MACs keyword
  - New default list for the ciphers and MACs
  - New "delayed" value (also the new default) for the sshd_config Compression keyword
  - Compression can now be enabled with privilege separation

What's new or changed: SMF

- **Client transfer completion record**
  - scp and sftp write client transfer completion records
  - Enabled via the new ClientSMF keyword in the new zos_ssh_config configuration file
- **Server transfer completion record**
  - sftp-server, scp and sshd (via "internal-sftp") write server transfer completion records
  - Enabled via the new ServerSMF keyword in the new zos_sshd_config configuration file

What's new or changed: SMF

- **Login failure record**
  - sshd writes login failure records
  - Enabled via the new ServerSMF keyword in the new zos_sshd_config configuration file
- **Programming support**
  - New FOTSMF77 member of SYS1.MACLIB that contains assembler mapping macros for OpenSSH SMF Type 119 records
  - New /samples/ssh_smf.h file that contains C mapping macros for OpenSSH SMF Type 119 records

What's new or changed: Key Rings

- **User authentication with SAF key rings**
  - ssh enabled via the new IdentityKeyRingLabel keyword in the new zos_user_ssh_config configuration file
  - ssh-add enabled via the new _ZOS_SSH_KEY_RING and _ZOS_SSH_KEY_RING_LABEL environment variables
  - ssh-keygen enabled via the new _ZOS_SSH_KEY_RING_LABEL environment variable
  - sshd enabled via the new zos-key-ring-label option for authorized_keys file format

What's new or changed: Key Rings

- **Server authentication with SAF key rings**
  - ssh enabled via the new zos-key-ring-label option for ssh_known_hosts file format
  - sshd enabled via the new HostKeyRingLabel keyword in the new zos_sshd_config configuration file

What's new or changed: Miscellaneous

- **Improved ssh-rand-helper support**
  - New _ZOS_SSH_PRNG_CMDS_TIMEOUT environment variable
- **Improved message support**
  - New _ZOS_OPENSSH_MSGCAT environment variable
  - All error-related messages are now documented in the user's guide

What's new or changed: Details

- **ssh**
  - New –M, –O and –S command-line options
  - New bind address for the –D, –L and –R command-line options
  - New "arcfour128" and "arcfour256" ciphers for the –c command-line option
  - New "umac64@openssh.com" MAC for the –m command-line option
  - New –KR, –h and !*command* escape command-line options
  - Default value changed for the –c and –m command-line options

What's new or changed: Details

- **ssh (continued)**
  - Supports the new _ZOS_USER_SSH_CONFIG environment variable
  - Supports the new zos_ssh_config and zos_user_ssh_config configuration files

What's new or changed: Details

- **ssh_config**
  - New bind address for the DynamicForward, LocalForward and RemoteForward keywords
  - New ControlMaster, ControlPath, ExitOnForwardFailure, HashKnownHosts, LocalCommand, PermitLocalCommand, RekeyLimit and SendEnv keywords
  - New "arcfour128" and "arcfour256" ciphers for the Ciphers keyword
  - New "umac64@openssh.com" MAC for the MACs keyword
  - Default value changed for the Ciphers and MACs keywords

What's new or changed: Details

- **sshd**
  - New no-user-rc and zos-key-ring-label options for the authorized_keys file format
  - New zos-key-ring-label option for the ssh_known_hosts file format
  - New [host]:port formatting and hashed hostname and address support for the ssh_known_hosts file format
  - Supports the new _ZOS_SSHD_CONFIG environment variable
  - Supports the new zos_sshd_config configuration file
  - Supports writing SMF login failure and server transfer completion records

What's new or changed: Details

- **sshd_config**
  - New AcceptEnv, AddressFamily, ChrootDirectory, ForceCommand, HostbasedUsesNameFromPacketOnly, Match, MaxAuthTries and PermitOpen keywords
  - New "delayed" value for the Compression keyword
  - New "clientspecified" value for the GatewayPort keyword
  - New "arcfour128" and "arcfour256" ciphers for the Ciphers keyword
  - New "umac64@openssh.com" MAC for the MACs keyword
  - New "internal-sftp" value for the Subsystem keyword
  - Default value changed for the AllowTcpForwarding, Ciphers, Compression and MACs keywords

What's new or changed: Details

- **scp**
  - Supports writing SMF client and server transfer completion records
- **sftp**
  - New options added for the ls command (–a –f –n –r –S –t)
  - Supports writing SMF client transfer completion records
- **sftp-server**
  - New –f, –l, –e and –h command-line options
  - Supports writing SMF server transfer completion records

What's new or changed: Details

- **ssh-keyscan**
  - New –H command-line option
- **ssh-keygen**
  - New –F, -H and –R command-line options
  - Supports the new _ZOS_SSH_KEY_RING_LABEL environment variable

What's new or changed: Details

- **ssh-add**
  - Supports the new _ZOS_SSH_KEY_RING and _ZOS_SSH_KEY_RING_LABEL environment variables
- **ssh-rand-helper**
  - Supports the new _ZOS_SSH_PRNG_CMDS_TIMEOUT environment variable

What's new or changed: Details

- **(NEW) zos_ssh_config**
  - New z/OS-specific system-wide OpenSSH client configuration file used by ssh
  - Provides ClientSMF keyword for SMF support
  - File location: /etc/ssh/zos_ssh_config
  - Sample provided: /samples/zos_ssh_config

What's new or changed: Details

- **(NEW) zos_user_ssh_config**
  - New z/OS-specific per-user OpenSSH client configuration file used by ssh
  - Provides IdentityKeyRingLabel keyword for SAF key ring support
  - Default File Location: ~/.ssh/zos_user_ssh_config
  - Override default file location via the new _ZOS_USER_SSH_CONFIG environment variable
  - Sample provided: /samples/zos_user_ssh_config

What's new or changed: Details

- **(NEW) zos_sshd_config**
  - New z/OS-specific OpenSSH daemon configuration file used by sshd
  - Provides ServerSMF keyword for SMF support
  - Provides HostKeyRingLabel keyword for SAF key ring support
  - Default File Location: /etc/ssh/zos_sshd_config
  - Override default file location via the new _ZOS_SSHD_CONFIG environment variable
  - Sample provided: /samples/zos_sshd_config

What's new or changed: Details

- **Changed samples**
  - /samples/ssh_config
  - /samples/sshd_config
  - /samples/moduli
- **New samples**
  - /samples/zos_ssh_config
  - /samples/zos_user_ssh_config
  - /samples/zos_sshd_config
  - /samples/ssh_smf.h
  - FOTSMF77 in SYS1.MACLIB

What's new or changed: Details

- **New environment variables**
  - _ZOS_OPENSSH_MSGCAT (Supported by all OpenSSH commands)
  - _ZOS_SSH_PRNG_CMDS_TIMEOUT (ssh-rand-helper)
  - _ZOS_SSHD_CONFIG (sshd)
  - _ZOS_SSH_KEY_RING (ssh-add)
  - _ZOS_SSH_KEY_RING_LABEL (ssh-add and ssh-keygen)
  - _ZOS_USER_SSH_CONFIG (ssh)
  - _ZOS_SMF_FD (internal use only)
  - _ZOS_OPENSSH_DEBUG (internal use only)

What's new or changed: Details

- See the "What's new or changed in Version 1 Release 2 of IBM Ported Tools for z/OS: OpenSSH" chapter in the user's guide for more information.

Appendix

- **Website References**
  - IBM Ported Tools for z/OS:
    http://www.ibm.com/systems/z/os/zos/features/unix/ported/
  - IBM Ported Tools for z/OS: OpenSSH:
    http://www.ibm.com/systems/z/os/zos/features/unix/ported/openssh/
  - OpenSSH: http://www.openssh.org/
  - OpenSSL: http://www.openssl.org/
  - zlib: http://www.zlib.net/

Appendix

- **Website References (Continued)**
  - IETF: http://www.ietf.org/
  - US-CERT Vulnerability Notes Database: http://www.kb.cert.org/vuls
  - National Vulnerability Database: http://nvd.nist.gov/nvd.cfm
  - ShopzSeries: https://www14.software.ibm.com/webapp/ShopzSeries/ShopzSeries.jsp
  - Tools and Toys: http://www.ibm.com/systems/z/os/zos/features/unix/tools/

Appendix

- **See the new "IBM Ported Tools for z/OS: OpenSSH User's Guide" for more details on OpenSSH for z/OS V1R2.**
  (Order Number: SA23-2246-00)
- **RACF Reference Guides**
  - z/OS Security Server RACF Security Administrator's Guide (Order Number: SA22-7683-12)
  - z/OS Security Server RACF Callable Services (Order Number: SA22-7691-12)
  - z/OS Security Server RACF Command Language Reference (Order Number: SA22-7687-12)

Appendix

- **Other Reference Guides**
  - Program Directory for IBM Ported Tools for z/OS (Order Number: GI10-0769-05)
  - z/OS MVS System Management Facilities (SMF) (Order Number: SA22-7630-19)
  - z/OS MVS Initialization and Tuning Reference (Order Number: SA22-7592-18)
  - z/OS Communications Server: IP Configuration Reference (Order Number: SC31-8776-15)