



OpenSSH Accelerator for z/OS

Tuesday, March 22th 2011

Steve Goetze
Kirk Wolf
Rob Schramm



<http://dovetail.com>
info@dovetail.com



Dovetailed Technologies

We provide z/OS customers world wide with innovative solutions that enhance and transform traditional mainframe workloads:

- Co:Z Toolkit, which includes:
 - *Co:Z Launcher* – remote system cooperative processing
 - *Co:Z Dataset Pipes* – convert datasets to files
 - *Co:Z SFTP* – OpenSSH SFTP with z/OS exploitation
 - *Co:Z Batch* – full featured BPXBATCH replacement
- T:Z Quickstart for Tomcat and z/OS
- JZOS - acquired by IBM in 2005 and now part of the z/OS Java SDK



SECURE FILE TRANSFER: DEEP POCKETS NOT REQUIRED

FREE

Use the Co:Z Co-Processing Toolkit with our Community License and support forum free of charge.

Enterprise license and support agreements start at \$4995. These include commercial SLAs along with friendly, responsive technical support provided directly by the Co:Z development team.

Join the growing number of enterprises that rely on the Co:Z Toolkit for affordable, supported and non-proprietary secure file transfer and distributed processing.



Dovetailed Technologies
www.dovetail.com
+1.636.300.0901

Co:Z SFTP

OpenSSH secure file transfer with support for MVS datasets and SMF logging

Co:Z Launcher

Execute Unix or Windows processes from a batch job with access to MVS datasets

Co:Z Dataset Pipes

Flexible conversion of MVS datasets to/from pipes or Unix files

Co:Z Batch

A better BPXBATCH



Co:Z Co-Processing Toolkit

for z/OS | Dataset Pipes · SFTP · FTP-SSH Proxy · JZDS · DTISpawn



Agenda

- OpenSSH Accelerator for z/OS overview
- OpenSSH Accelerator installation and usage
- Comparing Co:Z SFTP to FTP/SSL
- New Co:Z SFTP service offerings
- Q & A



Terminology used in this presentation

- **SSH** – A draft internet standard defined by a group of related RFCs, aka “SSH-2”
- **SFTP** – SSH file transfer layer. SFTP implementations generally follow “draft-ietf-secsh-filexfer” version 3 or 4.
- **FTPS** – FTP with SSL/TLS; RFC-2228 et al.
- **“Ported Tools”** - IBM Ported Tools for z/OS OpenSSH; a non-chargeable, supported z/OS feature

Note: the old SSH protocol version 1 (“SSH-1”) has known security weaknesses, and should be avoided and disabled in your SSH servers if possible (the default in Ported Tools)

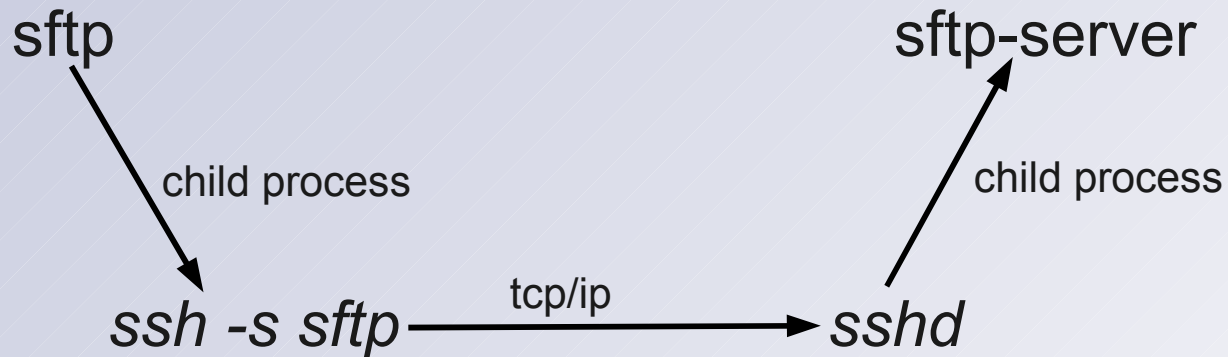


Ported Tools OpenSSH – free or not?

- ❏ Ported Tools OpenSSH includes OpenSSL software crypto algorithms which are statically linked into the “ssh” and “sshd” commands.
 - Ciphers: aes, 3des, blowfish, etc.
 - MACs: md5, sha-1, etc.
- ❏ ssh/sshd are used by several clients/subsystems:
 - Ported Tools sftp, sftp-server, scp
 - Co:Z sftp, sftp-server
 - Co:Z Launcher, remote Dataset Pipes via ssh
 - Interactive ssh “shell” sessions
- ➔ It is typical for ssh to use 80-90% of the CPU time for a sftp job.
 - When invoked by sftp/cozsftp, ssh is run in a forked BPXAS address space.



ssh / sshd process structure





1GB transfer using Co:Z SFTP - Costs

Job	Type	Elapsed	TCB Time
CPACOFF	JES2	162.1	6.1
CPACOFF1	OMVS	159.9	54.1



CPACF - Introduction

- A no-charge hardware feature (#3863) available on z machines.
- General CP instructions for ciphers (KM), block ciphers (KMC), and MACs (KIMD, KLMD)
- (depending on model) supports aes-128, aes-192, aes-256, 3des, sha1, sha256
- Test your machine's features using our “cpacf_info” command.
- Can be used through ICSF or directly
- Can be exploited on Linux on z using the open source “OpenSSL” engine written by IBM.



OpenSSH Accelerator for z/OS

- Allows customers to create accelerated versions of Ported Tools “ssh” and “sshd” commands.
- Uses CPACF instructions if available for OpenSSH algorithms with fall back to original software routines.
- Exploits the highly modular OpenSSL architecture to install hooks into the internal “EVP” engine interfaces using the z/OS program binder.
- May reduce ssh CPU time by 67%; overall time for sftp by > 60% (YMMV)
- Not supported by IBM.
 - Instructions included for selecting the original or accelerated versions in your jobs. Original versions should be used when obtaining IBM service for Ported Tools OpenSSH.
- Free Evaluation download; currently no cost to Co:Z “Gold” support customers

OpenSSL Accelerator for z/OS - Installaion



Demo...



OpenSSH Accelerator for z/OS - Using

Demo...



1GB transfer using Co:Z SFTP - with OpenSSH Accelerator for z/OS

Job	Type	Elapsed	TCB Time
CPACOFF	JES2	162.1	6.1
CPACOFF1	OMVS	159.9	54.1
CPACON	JES2	85.8	6
CPACON1	OMVS	85.1	15.1



Comparison: Co:Z SFTP vs FTPS

Feature	Co:Z SFTP + Ported Tools 1.2	IBM FTPS
Ciphers, MACs via CPACF	yes; with OpenSSH Accelerator	yes
Host and user keys in SAF / ICSF	yes	yes
ICSF secure random number generation	yes; if /dev/random is configured	yes
Direct MVS dataset support	yes	yes
SMF 119 records	yes; compatible with FTP	yes
User exits	yes; compatible with FTP	yes
Firewall / NAT router friendly	yes; single socket/port	no ¹
Compatibility	Based on OpenSSH which is installed by default on nearly all Unix/Linux systems	FTP SSL/TLS often requires significant coordination with each partner ¹

¹ See: <http://share.confex.com/share/116/webprogram/Session8239.html>



Service Offerings

- ❏ Co:Z SFTP Discovery
 - Free web-based offering to explore the suitability of Co:Z SFTP for your enterprise.

- ❏ Co:Z SFTP Quickie
 - One day engagement to install and verify Co:Z SFTP in your test environment. Delivered on-site or via the Web. No commitment for Co:Z Support contract required.

- ❏ Co:Z SFTP Custom Offerings

Q and A





Legal...

- Co:Z® is a registered trademark of Dovetailed Technologies
- SSH® is a registered trademark of SSH Communications
- z/OS® is a registered trademark of IBM Corporation