Introduction to HP NonStop SSH
Customer Talk – 01/24/08

Karen Copeland
HP NonStop Product Management

Thomas Burg
comForte Chief Technology Officer

Technology for better business outcomes
HP NonStop SSH
Overview

HP NonStop is offering a new product on the pricebook to enable encryption of data in motion for the NonStop Server.

HP NonStop Secure Shell (SSH) is that product and it is based on technology from comForte™.

This presentation provides information about this new product for customers who wish to know more.
HP NonStop SSH
Agenda

What is ssh?
NonStop SSH function & architecture
NonStop SSH Installation
Product Licensing options & future release plans
What is ssh?
Secure Shell (ssh) protocol

Definition

Quoted from Wikipedia:

- Secure Shell or ssh is a network protocol that allows data to be exchanged over a secure channel between two computers.
- ssh is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding arbitrary TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols.
- See http://en.wikipedia.org/wiki/Secure_Shell for full text
The ssh Encryption Standard

- The ssh standard was created by a Finnish student in 1995
- Initially developed for shell access only, other functionality added later
- Governed by multiple RFC’s today
- Widely popular in Unix world early on (“openssh”)
- Uses Key Pairs *or* username/password for Authentication
- OpenSSH very popular on Unix, available for NonStop (with some limitations)
- Several Commercial solutions for Unix, Windows, i.e.
  - “Tectia”, [www.ssh.com](http://www.ssh.com)
HP NonStop SSH
Architecture

Technology for better business outcomes

© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice
The HP NonStop SSH product is designed to help customers effectively manage security risks and comply with external and internal security policies.

- Fully compliant to the ssh Protocol (Version 2)
- Strong authentication and multiple cipher suites
- Supports full screen terminal access for TACL and OSS
- Built-in user base
- Central key store
- Secure SFTP transfer
- TCP and FTP Port forwarding
- Advanced Auditing capabilities
- Does not require SYSGEN to install
HP NonStop SSH
Overview

− NonStop SSH provides an encryption layer for data transmitted between the NonStop and:
  • Terminal emulator devices
  • Other Servers
  • For File Transfer Protocol (FTP)
− Works in the Guardian Filesystem as well as OSS
− Runs as “daemon process on NonStop” (for remote clients to connect to)
− Has clients on NonStop which are started from TACL and connect to remote systems
HP NonStop SSH
Compared to “openssh”

• General
  – NonStop SSH does not require OSS
  – Optimized performance
    • (Inter-process communication via Guardian IPC, not OSS sockets)
  – Robust solution proven in high-volume business-critical production
  – Professional product and implementation support

• SSH daemon
  – Password authentication (OpenSSH supports only public key authentication)
  – External user-ids mapped to Guardian user-ids, allows customer to keep Guardian user-ids secret
  – Advanced audit capabilities
  – Fault-tolerance (SSH server runs as a NonStop process)
  – Pseudo-terminals support full screen applications such as vi or emacs.
  – Direct TACL command execution without requiring an OSS gtacl process
  – 6530 terminal support (SSH client supports 6530 terminal emulation, such as MR-Win6530)
  – Support of TELSERV-like SERVICE concept (H06.13 and later)
HP NonStop SSH
Compared to “openssh”

• SSH client
  – Guardian SSH client
  – Optimized for batch mode (e.g. remote passwords can be stored in a secure password store, avoiding interactive password prompts)

• File Transfer
  – Guardian SFTP client
  – Supports OSS and Guardian SFTP, as well as SFTP server
  – ASCII mode file transfer
  – Transfer from/to structured files (analogous to HP’s FTP)
  – Support of file create options, both for client and server (analogous to HP’s FTP)
  – Fine-grained access control, restricting individual users to specific Guardian file sets, OSS directories and specific operations (e.g. download only)
  – Tunneling of standard FTP sessions over SSH (i.e. FTP port forwarding)
HP NonStop SSH
Key management

- Stores keys in flat files and its own user/key database
- Two basic ways to use keys
  - To make sure client connects to proper daemon rather than an attacker (“server authentication” – mandatory yet automatic)
  - To replace user names and password with keys (more secure than user name/password – optional, requires generation and configuration of keys)
- As NonStop can be client and server that implies four key pairs (!)
  - Detailed explanation please see Reference Manual, section “Public Key Authentication”
NonStop Data in Motion
without NonStop SSH Installed

HP NonStop Server – Security Encryption without HP NonStop SSH

- TACL
- OSS
- Other Applications
- FTPSERV
- FTP

TELSERV

- MR-Win6530 emulator on the NonStop System Console
- Any 6530 emulation Client
- OSS emulation client
- FTP client
- FTP server
NonStop Data in Motion
with NonStop SSH Installed

HP NonStop Server – Security Encryption including HP NonStop SSH

- TACL
- OSS
- Other Applications
- Filesystem

HP NonStop SSH

- MR-Win6530 emulator on the NonStop System Console
- Any SSH enabled 6530 emulation Client
- SSH OSS emulation Client (MR-Win6530, PuTTY)
- SFTP client
- SFTP daemon
HP NonStop SSH Architecture
Runs as a SSH daemon on NonStop
HP NonStop SSH Architecture
Also runs as an SSH client on NonStop

NonStop Server

SSH[OSS] client
SFTP[OSS] client
FTP/FTPSERV
Any socket client or server

Audit log
SSH CTL

HP NonStop SSH (SSH2)

SSHCOM administration

Partner system

Standard SSH daemon (e.g. OpenSSH SSH Tectia)
HP NonStop SSH
Feature Summary

- Enterprise security solution to provide secure shell connectivity for HP NonStop servers
- File transfer and applications connectivity implementing end-to-end communications security
- Strong authentication replacing passwords with private keys (optional)
- Auditing capabilities
HP NonStop SSH
Installation and set-up Information

• HP NonStop SSH is delivered:
  – For H-Series – it is part of the RVU delivered on the SUT and installed using DSM/SCM
  – For initial delivery on S-series – it is being offered as an independent product until the next G-series RVU.
• The installation subvol for SSH is $SYSTEM.ZSSH
• SSH operation will be configured and started automatically on the default TCPIP stacks ($ZTCP1 and $ZTCP2)
• For each stack an SSH2 process is configured as generic process (managed by $ZZKRN).
• SSH operation on other TCP/IP stacks can be easily enabled
HP NonStop SSH
Installation and set-up Information

SCF entries for SSH are added by DSC/SCM

$SYSTEM ZSSH 3> scf info process $ZZKRN.#SSH*
SCF - T9082H01 - (26SEP05) (12SEP05) - 08/03/2007 20:46:03 System \NPNS01
(C) 1986 Tandem (C) 2005 Hewlett Packard Development Company, L.P.

NONSTOP KERNEL - Info PROCESS \NPNS01.$ZZKRN

<table>
<thead>
<tr>
<th>Symbolic Name</th>
<th>*Name</th>
<th>*Autorestart</th>
<th>*Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH-ZPTY</td>
<td>$ZPTY</td>
<td>10</td>
<td>$SYSTEM.ZSSH.STN</td>
</tr>
<tr>
<td>SSH-ZTCP0</td>
<td>$ZSSP0</td>
<td>10</td>
<td>$SYSTEM.ZSSH.SSH2</td>
</tr>
<tr>
<td>SSH-ZTCP1</td>
<td>$ZSSP1</td>
<td>10</td>
<td>$SYSTEM.ZSSH.SSH2</td>
</tr>
</tbody>
</table>

Total Errors = 0  Total Warnings = 0

$SYSTEM ZSSH 4>
HP NonStop SSH Licensing Options & Release Update
NonStop SSH Delivery

For H-series
- Provided as part of the H06.11 RVU.
- The individual SPR may be applied back to systems running H06.07
- For H-series systems running H06.11 or later, NonStop SSH is now resident on the SUT for use with NonStop Console.
- As HP NonStop delivers new products, many will already incorporate the use of SSH functionality.
- For releases prior to H06.11, customers can get the SSH functionality by downloading T0801AAA from NS-Scout.
- Until G06.32, S-series customers can request a try and buy or purchase the Independent product.

For G-series
- Provided as an Independent Product today
- Will be resident on the next G-series RVU (target is G06.32)
NonStop SSH – NS-Integrity (H-series)
Summary of ordering options

Installation Guidance:

Available starting with H06.11 RVU
(Or can be downloaded from SCOUT)

T0801AAA

Apply to systems running H06.07 or later.

INSTALL using DSM/SCM

For full or FTP-Only, install license file received from license.manager@hp.com after purchase or request for trial use

Ordering Options:

Basic SSH capability on the NonStop System Console:

• Nothing to order -- comes on the SUT
• Use an SSH capable Terminal Emulator on the NSC like MR-Win6530 (provided since H06.10)

For full SSH Capability:

• Order HSSH01V1 through NonStop Sales rep.
• Contact License.Manager@hp.com to receive license file.
• Install license file and run

For FTP Only Capability:

• Order HSSH02V1 through NonStop Sales rep.
• Contact License.Manager@hp.com to receive license file.
• Install license file and run
NonStop SSH – S-series (G-series)
Summary of ordering options

Installation Guidance:

Available as an Independent product
(Updates can be downloaded from Scout)

T0801G06

Apply to systems running G06.21 or later.

INSTALL CD using IP SETUP

For full or FTP-Only, install license file received from license.manager@hp.com after purchase or request for trial use

Ordering Options:

Basic SSH capability on the NonStop System Console:

• Order as SSH01V1 as “Trial”
• Use an SSH capable Terminal Emulator on the NSC like MR-Win6530 (provided since H06.10)

For full SSH Capability:

• Order SSH01V1 through NonStop Sales rep.
• Contact License.Manager@hp.com to receive license file.
• Install license file and run

For FTP Only Capability:

• Order SSH02V1 through NonStop Sales rep.
• Contact License.Manager@hp.com to receive license file.
• Install license file and run
NonStop SSH
Upcoming Release Plan – Calendar 2008

|-----------|-----------|-----------|-----------|-----------|

**H-series NonStop Integrity Platforms**

<table>
<thead>
<tr>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Delivery</td>
<td>H06.11 ( T0801AAA )</td>
</tr>
<tr>
<td>Participation in</td>
<td>H06.12 ( T0801AAB )</td>
</tr>
<tr>
<td>Participation in</td>
<td>H06.13 ( T0801AAC )</td>
</tr>
<tr>
<td>Early Delivery as TCF for H-series</td>
<td>( T0801AAC )</td>
</tr>
<tr>
<td>Participation in</td>
<td>H06.14</td>
</tr>
<tr>
<td>Participation in</td>
<td>H06.15</td>
</tr>
</tbody>
</table>

**G-series NonStop S-series Platforms**

<table>
<thead>
<tr>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Delivery As Independent Product</td>
<td>( T0801G06 )</td>
</tr>
<tr>
<td>TCF for G-series</td>
<td>( T0801AAD )</td>
</tr>
<tr>
<td>Participation in</td>
<td>G06.32</td>
</tr>
</tbody>
</table>

Note: Future product plans, dates, and functionality are subject to change without notice.
NonStop SSH
Upcoming Release Plans

We’ll be releasing a TCF SPR for both the H-series and the G-series versions of the product in January 2008 for existing customers. These SPRs correct the following known problems:

> lack of TELSERV-like SERVICE concept
> Display issues when using MR-Win6530 and SSH in OSS.
> OSS “man” and “more” commands failed
> Port param override issue
> Backspace issue in OSS when also using XYPRO XAC

Most problems reported have been found during OSS usage. All known OSS problems will be rolled into the upcoming H06.13 release and in the next G-series release.

H-series SPR will be available in Scout – T0801AAC.
G-series SPR will be available in Scout – T0801AAD.
NonStop SSH
Where to get more information

Questions?

Contact your NonStop Sales rep for quotes and more information about the product.

http://www.hp.com/go/nonstop/security/datainmotion