

HP-UX Development Environment for Eclipse

October 2010

Passwordless SSH Setup



Printed in the US

Legal Notices

© Copyright 2010 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation. Intel®, Pentium®, Itanium®, Intel Inside®, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux® is a U.S. registered trademark of Linus Torvalds.

Eclipse® is a trademark of Eclipse Foundation Inc.

Introduction

This document describes the procedure for configuring the public-key authentication for the Passwordless SSH setup of the HP-UX Development Environment for Eclipse. It includes the following:

- [Settings required for the Client](#)
- [Settings required for the Server](#)

Settings required for the Client

To generate the RSA/DSA key pairs:

1. Run the following command on the Client system. The Client system can be either a Windows or Linux desktop. For Windows, you must have a windowing client, such as cygwin.

```
# ssh-keygen -t [rsa|dsa]
```

The following output is displayed:

```
Generating public/private rsa key pair.  
Enter file in which to save the key (//.ssh/id_rsa) : <file name>  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /tmp/hi. Your  
public key has been saved in /tmp/hi.pub. The key  
fingerprint is:  
84: 7d: f5 :dd: 88: f7 :53:88: 8a: 6e: f7 :85:04:28: 6e:ed root@<hostname>
```

NOTE: For the Enter passphrase: and Enter same passphrase fields, press **Enter**.

The HP-UX Secure Shell generates the following key pairs and stores them in the \$HOME/.ssh directory on the client system:

- If the `ssh-keygen -t rsa` command is entered, SSH generates the `id_rsa` and `id_rsa.pub` key pairs.
- If the `ssh-keygen -r dsa` command is entered, SSH generates the `id_dsa` and `id_dsa.pub` key pairs.

2. Set the following configuration directive in the `/opt/ssh/etc/sshd_config` configuration file on the client system:

```
PubkeyAuthentication yes
```

NOTE: If you use Windows as your desktop and cygwin as the windowing client, you might not find the `/opt/ssh/etc/sshd_config` file. Hence, you can ignore this step.

NOTE: For backward compatibility purposes, HP-UX Secure Shell supports the RSA Authentication configuration directive in both the client and server configurations. This directive also enables public-key authentication for the client, but only for the SSH-1 protocol.

3. To ensure that the permissions of the home directory of the client, the `$HOME/.ssh` directories, and all files under the `$HOME/.ssh` directory match the permissions listed in Table 1: Permissions for the Client Files and Directories run the following commands:

```
# ll -d $HOME  
  
# ll -d $HOME/.ssh  
  
# ll $HOME/.ssh/
```

Table 1 lists the specific permissions for these files and directories.

Table 1: Permissions for the Client Files and Directories

File/Directory	Permissions
<code>\$ HOME (home directory)</code>	<code>drwx----- or drwxr--r--</code>
<code>\$HOME/.ssh</code>	<code>drwx----- or drwxr--r--</code>
<code>\$HOME/.ssh/id_rsa and id_dsa</code>	<code>-rw-r--r-- or -rw-----</code>
<code>\$HOME/.ssh/id_rsa.pub and id_dsa.pub</code>	<code>-rw-r--r-- or - rw</code>
<code>\$HOME/.ssh/config</code>	<code>-rwx-----</code>

NOTE: If you use Windows as your desktop and cygwin as the windowing client, the `ll -d` command will not work. You can use the `ls -al` command instead of the `ll -d` command to check the permissions.

4. Copy the public key in the client system to the home directory of the server using the following command:

```
#cat $HOME/.ssh/id_dsa.pub | ssh remoteuser@remotehost 'cat  
- >> $HOME/.ssh/authorized_keys'
```

The following output is displayed:

```
The authenticity of host 'remoteuser.remotehost (15.70.189.130)' can't be  
established  
RSA key fingerprint is 2a:c9: 77 :ad:d5 :d3 :ef:c3 : 1e: 12:12: 9e: 3a: 9f:c0 :38. Are  
you sure you want to continue connecting (yes/no)?
```

Note: Listed below is the alternate for the above command.

I) `scp $HOME/.ssh/id_dsa.pub <username>@<hostname>:`

Add the colon at the end of the command. You will be prompted for the password.

II) Type the password to connect to the remote host.

III) `Telnet <remotehost>.`

IV) Type the command: `mv id_dsa.pub .ssh/authorized_keys`

5. Do one of the following:

- i) Enter `yes` to continue with the connection.

The following message is displayed:

```
Warning: Permanently added 'itanika2.india.hp.com' (RSA) to the list  
of known hosts.
```

- ii) Enter `no` if you do not want to continue with the connection.

Settings required for Server:

To enable public-key authentication:

6. Set the following directive in the server configuration file
`/opt/ssh/etc/sshd_config:`

```
PubkeyAuthentication yes
```

7. Set the directory and file permissions on the server as specified in Table 2.

Table 2: Permissions for Server Files and Directories

File/Directory	Permissions
<code>\$ HOME (home directory)</code>	<code>drwx----- or drwxr--r--</code>
<code>\$HOME/.ssh</code>	<code>drwx----- or drwxr--r--</code>
<code>\$HOME/.ssh/authorized_keys and \$HOME/.ssh/authorized_keys2</code>	<code>-rw-r--r-- or -rw-----</code>

NOTE: The `$HOME` and `$HOME/.ssh` directories and all the files in the `$HOME/.ssh` directories must be owned by the respective users.

9. To connect to the server, run the following command:

```
$ ssh <username>@<hostname>
```

The server does not prompt for the password.

The secure connection is established between the server and the client.