```
Name setup-ssh – sets up an SSH key on specified hosts
```

```
Synopsis setup-ssh [--help]
[--sshport ssh-port] [--sshuser ssh-user]
[--sshkeyfile ssh-keyfile] [--sshpublickeyfile ssh-public-keyfile]
[--generatekey={false|true}]
host-list
```

Description The setup-ssh subcommand sets up a secure shell (SSH) key on the hosts that are specified as the operand of the subcommand. This key enables GlassFish Server to use public-key authentication for authentication of the user's SSH login on remote hosts.

> SSH enables GlassFish Server clusters that span multiple host machines to be administered centrally. When a subcommand for cluster administration is run, the subcommand is propagated from the domain administration server (DAS) host to remote hosts. To contact remote hosts, GlassFish Server uses SSH. SSH provides confidentiality and security for data that is exchanged between the DAS and remote hosts.

Public-key authentication uses an SSH key pair that comprises the following keys:

- A private key, which is stored in a secure location on the DAS host and is protected with a passphrase
- The public key, which is stored on all the remote hosts with which the DAS communicates

The subcommand sets up SSH connectivity between the DAS host and remote hosts by automating the following tasks:

- **Generating an SSH key pair.** If no SSH key pair exits, the default behavior of the subcommand is to prompt the user to generate an SSH key pair. The SSH key pair is generated without a passphrase. If a passphrase-protected key pair is required, the subcommand must generate the SSH key files without prompting the user. For more information, see the description of the --generatekey option.
- **Distributing the public key.** The subcommand copies the public key file to the *user-home*/.ssh directory and installs the public key in the user-home/.ssh/authorized keys file on each remote host. user-home is the user's home directory on the host. To distribute the public key, authentication of the user's SSH login is required. If public key authentication is not set up, the subcommand uses password authentication. If the subcommand uses password authentication and the --paswordfile option of the asadmin(1M) utility is not specified, the subcommand prompts the user for the password.

The subcommand does not modify the configuration of the DAS.

The prerequisites for using this subcommand are as follows:

- The sshd(1M) daemon is installed and running on the DAS host and on all hosts where an SSH key is to be set up.
- The DAS user has an SSH login on all hosts where an SSH key is to be set up.

- The ssh-keygen(1) utility is installed on the DAS host either at the default location or in a location that is defined in the DAS user's path.
- On Windows systems, the SSH package for Cygwin is installed.

This subcommand is supported in local mode only.

Options --help

--netp

Displays the help text for the subcommand.

--sshport

The port to use for SSH connections to the host where the GlassFish Server software is to be installed. The default is 22.

--sshuser

The SSH user that is to run the process for connecting to the host where the SSH key is to be set up. The default is the user that is running the DAS process. To ensure that the DAS can read this user's SSH private key file, specify the user that is running the DAS process.

--sshkeyfile

The absolute path to the SSH private key file for user that the --sshuser option specifies. This file is used for authentication to the sshd daemon on the host.

The path to the key file must be reachable by the DAS and the key file must be readable by the DAS. The path may contain Java properties of the form \${prop.name}.

The default is the a platform-dependent key file in the user's . ssh directory, for example:

- id rsa
- id dsa
- identitylocation

--sshpublickeyfile

The absolute path to the SSH public key file for user that the --sshuser option specifies. The public key file is copied to the user's .ssh directory on each host where SSH is being set up.

The path to the key file must be reachable by the DAS and the key file must be readable by the DAS. The path may contain Java properties of the form \${prop.name}.

The default is the a platform-dependent key file in the user's .ssh directory, for example:

- id rsa.pub
- id dsa.pub
- identitylocation.pub

--generatekey

Specifies whether the subcommand generates the SSH key files without prompting the user.

Possible values are as follows:

Reference Pages 2

true

The subcommand generates the SSH key files without prompting the user. Even if --generatekey is true, the subcommand generates the SSH key files without prompting the user only if the following conditions are met:

- The --interactive option of the asadmin utility is false.
- The --passwordfile option of the asadmin utility specifies a file in which the AS_ADMIN_SSHPASSWORD entry specifies the SSH user's password for logging in to the specified hosts.

If a passphrase is required, the file that --passwordfile option of the asadmin utility specifies must also contain an entry for AS ADMIN SSHPASSPHRASE.

false

The behavior of the subcommand depends on whether the SSH key files exist:

- If the SSH key files exist, the subcommand does not generate the files.
- If the SSH key files do not exist, the subcommand prompts the user to create the files and to provide the SSH user's password for logging in to the specified hosts.

This value is the default.

Operands host-list

A space-separated list of the names of the hosts where an SSH key is to be set up.

Examples EXAMPLE 1 Setting Up an SSH Key

This example sets up an SSH key for the user <code>gfuser</code> on the hosts <code>sj03</code> and <code>sj04</code>. The key file is not generated but is copied from the user's . ssh directory on the host where the DAS is running.

asadmin> setup-ssh sj03 sj04

Enter SSH password>

Copied keyfile /home/gfuser/.ssh/id rsa.pub to gfuser@sj03

Enter SSH password>

Copied keyfile /home/gfuser/.ssh/id_rsa.pub to gfuser@sj04

Command setup-ssh executed successfully.

EXAMPLE 2 Generating and Setting Up an SSH Key

This example generates and sets up an SSH key for the user gfuser on the hosts sua01 and sua02.

asadmin> setup-ssh --generatekey=true sua01 sua02

Enter SSH password>

Copied keyfile /home/gfuser/.ssh/id_rsa.pub to gfuser@sua01

Enter SSH password>

Copied keyfile /home/gfuser/.ssh/id_rsa.pub to gfuser@sua02 Command setup-ssh executed successfully.

Exit Status 0

command executed successfully

```
\begin{tabular}{ll} $1$ & error in executing the command \\ $See Also$ & $ssh-keygen(1)$ & \\ & asadmin(1M)$ & \\ & sshd(1M)$ & \\ & Cygwin Information and Installation (http://www.cygwin.com/) \\ \end{tabular}
```

Reference Pages 4