InterWorx Server Administrator SSH Guide

by InterWorx LLC

Contents

Chapter 1

SSH guide

1.1 History

Historically, before the implementation of SSH (Secure Shell), computers on the Internet were controlled remotely through such insecure protocols as rsh, rexec, and telnet (which sends data in plaintext). This obviously caused massive security issues as data such as passwords were sent via plaintext and could be intercepted via packet analysis. SSH fixed this vulnerability by providing a cryptographically secure public-key cryptography protocol to control remote computers on the Internet.

InterWorx provides an graphical control for SSH to make life easier for the server administrator.

1.2 Shell Users graph

At the top, you can see a graph of the number of active SSH sessions by time. This can be useful for the server administrator who wants to track how many shell users are active at specific times. This graph can be toggled on and off, and updated via the buttons below.

1.3 SSH Server Control

1.3.1 Status

This table shows the status of the SSH server and allows you to stop, start or restart the SSH server.

1.3.2 Start on boot-up

If set to “Yes”, SSH will be automatically started when the server starts up. This is recommended to be set to Yes so that if your server dies or is rebooted, you will have remote shell access available, rather than having to physically be at the server to control it.

1.3.3 Auto-restart SSH

With this option on you can have SSH restarted automatically if SSH goes down unexpectedly.

1.4 SSH Server Info

1.4.1 Version

The version of SSH installed on this system.

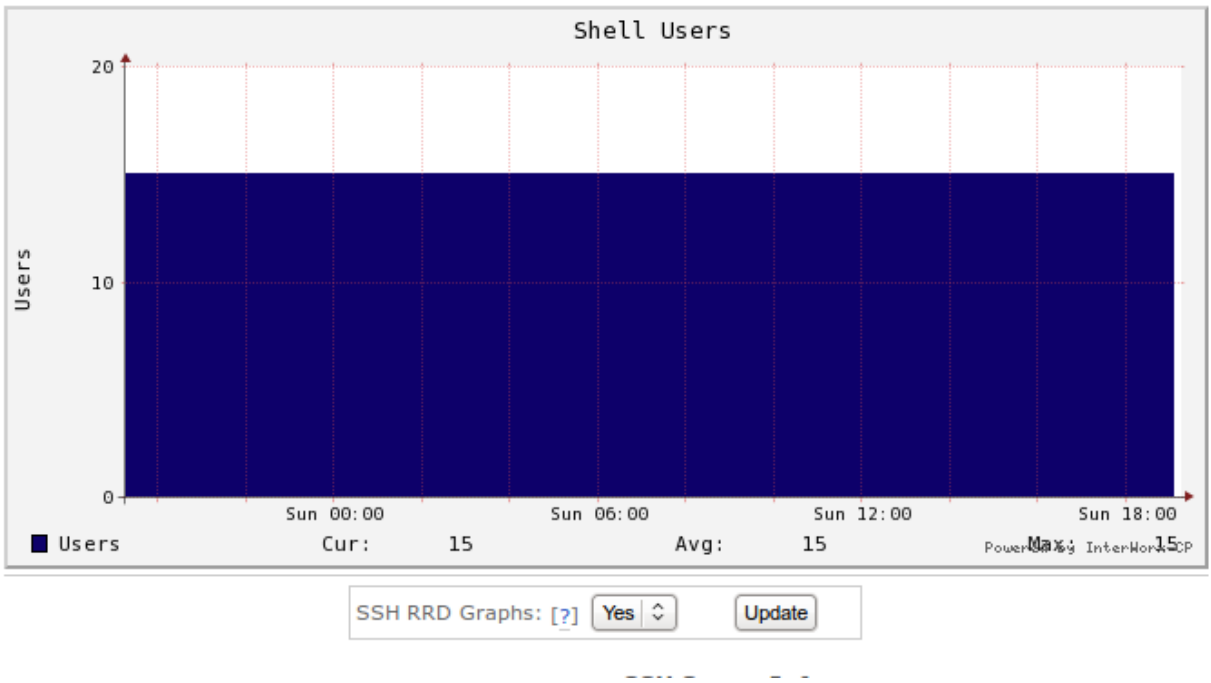

Figure 1.1: ssh rrd graph

Figure 1.2: SSH control

Figure 1.3: ssh info

Figure 1.4: ssh options

1.4.2 SSHD Config File Syntax

This tells you whether there are any syntax errors in your sshd_config file. If there are, you can click on the details link to see where the problem lies. This is recomended for advanced users who need atypical SSH configurations.

1.5 SSH Server Options

1.5.1 Port

This is the port that shell users will connect to, by default this is port 22.
Allow Root Login Sets whether the root user can login via ssh.

1.5.1.1 Yes

Root user is permitted to login

1.5.1.2 Without Password

Disables password authentication for the root user

1.5.1.3 Forced Command Only

Login is allowed but only if a command option was specified. Example: ssh root@test.com uptime

1.5.1.4 No

Root user is not permitted to login

1.5.2 Loglevel

Sets the verbosity that is used when logging sshd messages

1.5.3 Privilege Seperation

Toggles privilege separation. Used to prevent privilege escalation during the authentication process.

1.5.4 Two Potential Configurations

If you plan on giving SiteWorx users shell access, you should make sure to set the port to its default of 22. This is the standard that most end users will be used to. If SSH is set to listen on port 22, then you should set Allow Root Login to either No or Without Pass. http://www.linuxproblem.org/art_9.html Passwordless SSH is more secure and ties your root login to a single computer with the correct keys.

If you don't plan on giving SiteWorx users shell acces, then you may want to Allow Root Login to yes but set the port to something arbitrary but not in use by another service on your system. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_n For example, a potential port to use is 2220.

1.6 Current Shell Sessions

This table shows the shell sessions currently active. Including the following information:

1.6.1 User

Shell user currently logged in.

1.6.2 From

The IP address the shell user is currently logged in from. Time

The time the shell user logged in.

1.6.3 Idle Time

The amount of time the shell user has been idle.

1.6.4 Command

The current command the shell user is running.

This box can also be used to Terminate active SSH sessions.