Network Services: Supplement

# Notes & References

Linux systems use runlevels to determine what services should be started after the system is booted. These levels have different meanings, depending on the distribution (Table 13-2).

Table 13-2. Default Runlevels, by Linux Distribution

|  |  |  |  |
| --- | --- | --- | --- |
| Runlevel | CentOS | OpenSuSE | Ubuntu/Mint |
| 0 | Halt | Halt | Halt |
| 1 | Single User | Single User | Single User |
| 2 |  | Multi-user, no networking | Multi-user, graphics  (default) |
| 3 | Multi-user, text only | Multi-user, text only |  |
| 4 |  |  |  |
| 5 | Multi-user, graphics (default) | Multi-user, graphics  (default) |  |
| 6 | Restart | Restart | Restart |

On CentOS and OpenSuSE systems, the default runlevel is 5, while on Ubuntu and Mint systems the default runlevel is 2. The runlevel is a parameter set during system boot; some boot managers (e.g. GRUB) allow the runlevel to be manually modified before the system boots. The init command can be used on a system to change the current runlevel; for example, to reboot the system issue the command

[root@Spica ~]# init 6

Table 13-3 Default included version of OpenSSH, by Linux distribution

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CentOS |  |  | Mint |  |  | 13.1 | 6.2p2 |
| 7.4 | 7.4p1-11 |  | 18.3 | 7.2p2 |  | 12.3 | 6.1p1 |
| 7.3 | 6.6.1p1-31 |  | 18.2 | 7.2p2 |  | 12.2 | 6.0p1 |
| 7.2 | 6.6.1p1-22 |  | 18.1 | 7.2p2 |  | 12.1 | 5.8p2 |
| 7.1 | 6.6.1p1-11 |  | 18 | 7.2p2 |  | 11.4 | 5.8p1 |
| 7.0 | 6.4p1-8 |  | 17.3 | 6.6p1 |  | Ubuntu |  |
| 6.8 | 5.3p1-117 |  | 17.2 | 6.6p1 |  | 17.10 | 7.5p1 |
| 6.7 | 5.3p1-111 |  | 17.1 | 6.6p1 |  | 17.04 | 7.4p1 |
| 6.6 | 5.3p1-104 |  | 17 | 6.6p1 |  | 16.10 | 7.3p1 |
| 6.5 | 5.3p1-94 |  | 16 | 6.2p2 |  | 16.04 | 7.2p2 |
| 6.4 | 5.3p1-84 |  | 15 | 6.1p1 |  | 15.10 | 6.9p1 |
| 6.3 | 5.3p1-81 |  | 14 | 6.0p1 |  | 15.04 | 6.7p1 |
| 6.2 | 5.3p1-70 |  | 13 | 5.9p1 |  | 14.10 | 6.6p1 |
| 6.1 | 5.3p1-52 |  | 12 | 5.8p1 |  | 14.04 | 6.6p1 |
| 6.0 | 5.3p1-20 |  | 11 | 5.8p1 |  | 13.10 | 6.2p2 |
| 5.11 | 4.3p2-82 |  | 10 | 5.5p1 |  | 13.04 | 6.1p1 |
| 5.10 | 4.3p2-82 |  | OpenSuSE |  |  | 12.10 | 6.0p1 |
| 5.9 | 4.3p2-82 |  | 42.3 | 7.2p2 |  | 12.04 | 5.9p1 |
| 5.8 | 4.3p2-82 |  | 42.2 | 7.2p2 |  | 11.10 | 5.8p1 |
| 5.7 | 4.3p2-72 |  | 42.1 | 6.6p1 |  | 11.04 | 5.8p1 |
| 5.6 | 4.3p2-72 |  | 13.2 | 6.6p1 |  |  |  |

Table 13-4. Default included version of vsftpd, by Linux distribution

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CentOS |  |  | Mint |  |  | 13.1 | 3.0.2 |
| 7.4.1708 | 3.0.2-22 |  | 18.3 | 3.0.3 |  | 12.3 | 3.0.2 |
| 7.3.1611 | 3.0.2-21 |  | 18.2 | 3.0.3 |  | 12.2 | 3.0.0 |
| 7.2.1511 | 3.0.2-10 |  | 18.1 | 3.0.3 |  | 12.1 | 2.3.4 |
| 7.1.1503 | 3.0.2-9 |  | 18 | 3.0.3 |  | 11.4 | 2.3.2 |
| 7.0.1406 | 3.0.2-9 |  | 17.3 | 3.0.2 |  | Ubuntu |  |
| 6.8 | 2.2.2-21 |  | 17.2 | 3.0.2 |  | 17.10 | 3.0.3 |
| 6.7 | 2.2.2-14 |  | 17.1 | 3.0.2 |  | 17.04 | 3.0.3 |
| 6.6 | 2.2.2-12 |  | 17 | 3.0.2 |  | 16.10 | 3.0.3 |
| 6.5 | 2.2.2-11 |  | 16 | 3.0.2 |  | 16.04 | 3.0.3 |
| 6.4 | 2.2.2-11 |  | 15 | 3.0.2 |  | 15.10 | 3.0.2 |
| 6.3 | 2.2.2-11 |  | 14 | 2.3.5 |  | 15.04 | 3.0.2 |
| 6.2 | 2.2.2-6 |  | 13 | 2.3.5 |  | 14.10 | 3.0.2 |
| 6.1 | 2.2.2-6 |  | 12 | 2.3.2 |  | 14.04 | 3.0.2 |
| 6.0 | 2.2.2-6 |  | 11 | 2.3.2 |  | 13.10 | 3.0.2 |
| 5.11 | 2.0.5-28 |  | 10 | 2.3.0 |  | 13.04 | 3.0.2 |
| 5.10 | 2.0.5-28 |  | OpenSuSE |  |  | 12.10 | 2.3.5 |
| 5.9 | 2.0.5-28 |  | 42.3 | 3.0.2 |  | 12.04 | 2.3.5 |
| 5.8 | 2.0.4-24 |  | 42.2 | 3.0.2 |  | 11.10 | 2.3.2 |
| 5.7 | 2.0.5-21 |  | 42.1 | 3.0.2 |  | 11.04 | 2.3.2 |
| 5.6 | 2.0.5-16 |  | 13.2 | 3.0.2 |  |  |  |

Table 13-5. Default included version of Samba, by Linux distribution

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CentOS |  |  | Mint |  |  | 13.1 | 4.1.0 |
| 7.4.1709 | 4.6.2 |  | 18.3 | 4.3.11 |  | 12.3 | 3.6.12 |
| 7.3.1611 | 4.4.4-9 |  | 18.2 | 4.3.8 |  | 12.2 | 3.6.7 |
| 7.2.1511 | 4.2.3-10 |  | 18.1 | 4.3.8 |  | 12.1 | 3.6.1 |
| 7.1.1503 | 4.1.12-21 |  | 18 | 4.3.8 |  | 11.4 | 3.5.7 |
| 7.0.1406 | 4.1.1-31 |  | 17.3 | 4.1.6 |  | Ubuntu |  |
| 6.8 | 3.6.23-33 |  | 17.2 | 4.1.6 |  | 17.10 | 4.6.7 |
| 6.7 | 3.6.23-20 |  | 17.1 | 4.1.6 |  | 17.04 | 4.5.4 |
| 6.6 | 3.6.23-12 |  | 17 | 4.1.6 |  | 16.10 | 4.4.5 |
| 6.5 | 3.6.9-154 |  | 16 | 3.6.18 |  | 16.04 | 4.3.8 |
| 6.4 | 3.6.9-151 |  | 15 | 3.6.9 |  | 15.10 | 4.1.17 |
| 6.3 | 3.5.10-125 |  | 14 | 3.6.6 |  | 15.04 | 4.1.13 |
| 6.2 | 3.5.10-114 |  | 13 | 3.6.3 |  | 14.10 | 4.1.11 |
| 6.1 | 3.5.6-86 |  | 12 | 3.5.11 |  | 14.04 | 4.1.6 |
| 6.0 | 3.5.4-68 |  | 11 | 3.5.8 |  | 13.10 | 3.6.18 |
| 5.11 | 3.0.33-3.40 |  | 10 | 3.5.4 |  | 13.04 | 3.6.9 |
| 5.10 | 3.0.33-3.39 |  | OpenSuSE |  |  | 12.10 | 3.6.6 |
| 5.9 | 3.0.33-3.39 |  | 42.3 | 4.6.5 |  | 12.04 | 3.6.3 |
| 5.8 | 3.0.33-3.37 |  | 42.2 | 4.4.2 |  | 11.10 | 3.5.11 |
| 5.7 | 3.0.33-3.29 |  | 42.1 | 4.2.4 |  | 11.04 | 3.5.8 |
| 5.6 | 3.0.33-3.29 |  | 13.2 | 4.1.12 |  |  |  |
|  |  |  |  |  |  |  |  |

Exercises

1. Use ssh-keygen to regenerate the keys on an OpenSSH server.
2. It is possible to use Cygwin to run OpenSSH server on a Windows system. Download Cygwin from <https://www.cygwin.com/>. Run the setup tool and install the OpenSSH server (Figure 13-20). Once the server is installed, launch the Cygwin terminal (as administrator) and run the script ssh-host-config to setup and configure OpenSSH. Start the server, and verify it works by connecting to it from a remote system. Be sure to open the proper port in the firewall.

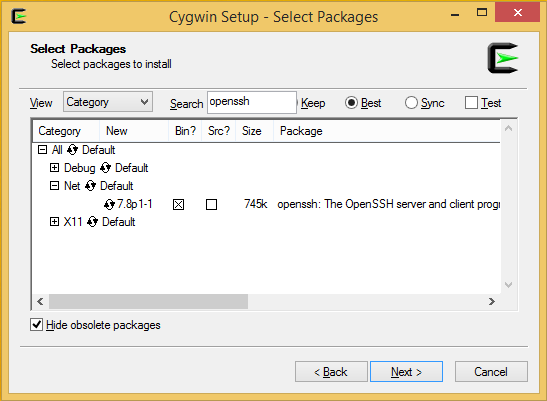


Figure 13-20. Using the Cygwin setup program to install OpenSSH server on Windows 8.1.

1. Construct two Linux systems with system A running an OpenSSH server. On system B, create a key pair, and copy the public key to system A so that a user on B can login to A. Use the techniques of Chapter 2 to exploit system B. If the key is not protected by a passphrase, have the attacker download the key to the attacker's system and use it to log in to A. If the key is protected by a passphrase and the passphrase has been loaded into an agent, show that the attacker can log into A from B using the key provided by the agent.
2. One defense against brute force attacks against an SSH server is to configure the authentication system to temporarily lock out an account after a set number of failed login attempts. Investigate the PAM module pam\_tally2, and configure a Linux target to lock accounts after five failed login attempts. What are the advantages and disadvantages of applying this policy to the root account?
3. Run an NMap scan against a host running SSH. What appears in the logs for SSH? Does the result change if version detection is enabled in the scan? Does the result change is default and safe scripts are included in the scan?
4. Write a Python script that opens the appropriate Linux log file and counts the number of failed login attempts that occur each a day.
5. Run a brute force attack against a Linux Samba server. When the attack concludes, check the status of the account with pdbedit using the -L and -v flags. Note the value of the Account Flags section. Reset the locked-out account with the -c flag.