TecMint
The Ideal Linux Blog for Sysadmins & Geeks

LINUX COMMANDS 35

I ❤ TecMint :

29 Practical Examples of Nmap Commands for Linux System/Network Administrators

18 Tar Command Examples in Linux

by Tarunika Shrivastava | Published: December 11, 2013 | Last Updated: January 3, 2015

The **Nmap** aka **Network Mapper** is an open source and a very versatile tool for Linux system/network administrators. **Nmap** is used for **exploring networks**, **perform security scans**, **network audit** and **finding open ports** on remote machine. It scans for Live hosts, Operating systems, packet filters and open ports running on remote hosts.

Nmap Commands and Examples

I'll be covering most of **NMAP** usage in two different parts and this is the first part of nmap serious. Here in this setup, I have used two servers without firewall to test the working of the Nmap command.

- 192.168.0.100 – server1.tecmint.com
- 192.168.0.101 – server2.tecmint.com

How to Add Linux Host to Nagios Monitoring Server Using NRPE Plugin

How to Install Nagios 4.4.5 on RHEL/CentOS 8/7 and Fedora 30

Install Cacti (Network Monitoring) on RHEL/CentOS 8/7 and Fedora 30

How to Install Google Chrome 75 On RHEL/CentOS 7 and Fedora 30

How to Install Ubuntu Alongside With Windows 10 or 8 in Dual-Boot

18 Tar Command Examples in Linux

Nmap command usage

```
# nmap [Scan Type(s)] [Optio
```

How to Install NMAP in Linux

Most of the today’s Linux distributions like **Red Hat**, **CentOS**, **Fedoro**, **Debian** and **Ubuntu** have included **Nmap** in their default package management repositories called Yum and APT. The both tools are used to install and manage software packages and updates. To install **Nmap** on distribution specific use the following command.

```
# yum install nmap

$ sudo apt-get install nmap
```

Once you’ve install latest nmap application, you can follow the example instructions provided in this article.

1. Scan a System with Hostname and IP Address

The **Nmap** tool offers various methods to scan a system. In this example, I am

18 Tar Command Examples in Linux

performing a scan using hostname as **server2.tecmint.com** to find out all open ports, services and MAC address on the system.

Scan using Hostname

```
[root@server1 ~]# nmap serve

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address 
You have new mail in /var/sp
```

Scan using IP Address

```
[root@server1 ~]# nmap 192.1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
```

```
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
958/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
You have new mail in /var/sp
```

2. Scan using “-v” option

You can see that the below command with “-v” option is giving more detailed information about the remote machine.

```
[root@server1 ~]# nmap -v se

Starting Nmap 4.11 ( http://
Initiating ARP Ping Scan aga
The ARP Ping Scan took 0.01s
Initiating SYN Stealth Scan
Discovered open port 22/tcp
Discovered open port 80/tcp
Discovered open port 8888/tc
Discovered open port 111/tcp
Discovered open port 3306/tc
Discovered open port 957/tcp
The SYN Stealth Scan took 0.
Host server2.tecmint.com (19
Interesting ports on server2
```

18 Tar Command Examples in Linux

```
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
               Raw packets s
```

Scan Multiple Hosts

You can scan multiple hosts by simply writing their IP addresses or hostnames with Nmap.

```
[root@server1 ~]# nmap 192.1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
```

```
MAC Address: 08:00:27:D9:8E:
Nmap finished: 3 IP addresse
```

4. Scan a whole Subnet

You can scan a whole subnet or IP range with Nmap by providing * **wildcard** with it.

```
[root@server1 ~]# nmap 192.1

Starting Nmap 4.11 ( http://
Interesting ports on server1
Not shown: 1677 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
851/tcp open  unknown

Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 256 IP addres
You have new mail in /var/sp
```

18 Tar Command Examples in Linux

On above output you can see that nmap scanned a whole subnet and gave the information about those hosts which are **Up** in the **Network**.

5. Scan Multiple Servers using last octet of IP address

You can perform scans on multiple IP address by simple specifying last octet of IP address. For example, here I performing a scan on IP addresses 192.168.0.101, 192.168.0.102 and 192.168.0.103.

```
[root@server1 ~]# nmap 192.1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 3 IP addresse
You have new mail in /var/sp
```

18 Tar Command Examples in Linux

6. Scan list of Hosts from a File

If you have more hosts to scan and all host details are written in a file , you can directly ask nmap to read that file and perform scans. Let's see how to do that.

Create a text file called "**nmaptest.txt**" and define all the IP addresses or hostname of the server that you want to do a scan.

```
[root@server1 ~]# cat > nmap

localhost
server2.tecmint.com
192.168.0.101
```

Next, run the following command with "**iL**" option with nmap command to scan all listed IP address in the file.

```
[root@server1 ~]# nmap -iL n

Starting Nmap 4.11 ( http://
Interesting ports on localho
Not shown: 1675 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
111/tcp  open  rpcbind
631/tcp  open  ipp
```

```
857/tcp open  unknown

Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
958/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
958/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 3 IP addresse
```

7. Scan an IP Address Range

You can specify an IP range while performing scan with Nmap.

```
[root@server1 ~]# nmap 192.1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 10 IP address
```

8. Scan Network Excluding Remote Hosts

You can exclude some hosts while performing a full network scan or when you are scanning with wildcards with "**–exclude**" option.

```
[root@server1 ~]# nmap 192.1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
```

18 Tar Command Examples in Linux

```
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 255 IP addres
You have new mail in /var/sp
```

9. Scan OS information and Traceroute

With Nmap, you can detect which OS and version is running on the remote host. To enable OS & version detection, script scanning and traceroute, we can use "-A" option with NMAP.

```
[root@server1 ~]# nmap -A 19

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE VERSI
22/tcp   open  ssh     OpenS
80/tcp   open  http    Apach
111/tcp  open  rpcbind  2 (r
957/tcp  open  status   1 (r
3306/tcp open  mysql   MySQL
8888/tcp open  http    light
MAC Address: 08:00:27:D9:8E:
```

18 Tar Command Examples in Linux

```
No exact OS matches for host
TCP/IP fingerprint:
SInfo(V=4.11%P=i686-redhat-l
TSeq(Class=TR%IPID=Z%TS=1000
T1(Resp=Y%DF=Y%W=16A0%ACK=S+
T2(Resp=N)
T3(Resp=Y%DF=Y%W=16A0%ACK=S+
T4(Resp=Y%DF=Y%W=0%ACK=O%Fla
T5(Resp=Y%DF=Y%W=0%ACK=S++%F
T6(Resp=Y%DF=Y%W=0%ACK=O%Fla
T7(Resp=Y%DF=Y%W=0%ACK=S++%F
PU(Resp=Y%DF=N%TOS=C0%IPLEN=

Uptime 0.169 days (since Mon

Nmap finished: 1 IP address
You have new mail in /var/sp
```

In above Output, you can see that nmap is came up with **TCP/IP** fingerprint of the **OS** running on remote hosts and being more specific about the port and services running on the remote hosts.

10. Enable OS Detection with Nmap

Use the option "**-O**" and "**-osscan-guess**" also helps to discover OS information.

```
[root@server1 ~]# nmap -O se
```

18 Tar Command Examples in Linux

```
Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:
No exact OS matches for host
TCP/IP fingerprint:
SInfo(V=4.11%P=i686-redhat-l
TSeq(Class=TR%IPID=Z%TS=1000
T1(Resp=Y%DF=Y%W=16A0%ACK=S+
T2(Resp=N)
T3(Resp=Y%DF=Y%W=16A0%ACK=S+
T4(Resp=Y%DF=Y%W=0%ACK=O%Fla
R%Ops=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%F
T6(Resp=Y%DF=Y%W=0%ACK=O%Fla
T7(Resp=Y%DF=Y%W=0%ACK=S++%F
PU(Resp=Y%DF=N%TOS=C0%IPLEN=

Uptime 0.221 days (since Mon

Nmap finished: 1 IP address
You have new mail in /var/sp
```

11. Scan a Host to Detect Firewall

The below command will perform a scan on a remote host to detect if any packet filters or Firewall is used by host.

```
[root@server1 ~]# nmap -sA 1

Starting Nmap 4.11 ( http://
All 1680 scanned ports on se
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address 
You have new mail in /var/sp
```

12. Scan a Host to check its protected by Firewall

To scan a host if it is protected by any packet filtering software or Firewalls.

```
[root@server1 ~]# nmap -PN 1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
```

```
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
```

13. Find out Live hosts in a Network

With the help of "**-sP**" option we can simply check which hosts are live and up in Network, with this option nmap skips port detection and other things.

```
[root@server1 ~]# nmap -sP 1

Starting Nmap 4.11 ( http://
Host server1.tecmint.com (19
Host server2.tecmint.com (19
MAC Address: 08:00:27:D9:8E:
Nmap finished: 256 IP addres
```

14. Perform a Fast Scan

You can perform a fast scan with "**-F**" option to scans for the ports listed in the nmap-services files and leaves all other ports.

```
[root@server1 ~]# nmap -F 19

Starting Nmap 4.11 ( http://
Interesting ports o
```

18 Tar Command Examples in Linux

```
Not shown: 1234 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
```

15. Find Nmap version

You can find out Nmap version you are running on your machine with "**-V**" option.

```
[root@server1 ~]# nmap -V

Nmap version 4.11 ( http://w
You have new mail in /var/sp
```

16. Scan Ports Consecutively

Use the "**-r**" flag to don't randomize.

```
[root@server1 ~]# nmap -r 19

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
```

18 Tar Command Examples in Linux

```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
```

17. Print Host interfaces and Routes

You can find out host interface and route information with nmap by using “**–iflist**” option.

```
[root@server1 ~]# nmap --ifl

Starting Nmap 4.11 ( http://
************************INTE
DEV  (SHORT) IP/MASK
lo   (lo)    127.0.0.1/8
eth0 (eth0)  192.168.0.100/2

**************************RO
DST/MASK       DEV  GATEWAY
192.168.0.0/0 eth0
169.254.0.0/0 eth0
```

18 Tar Command Examples in Linux

In above output, you can see that map is listing interfaces attached to your system and their respective routes.

18. Scan for specific Port

There are various options to discover ports on remote machine with Nmap. You can specify the port you want nmap to scan with “**-p**” option, by default nmap scans only **TCP** ports.

```
[root@server1 ~]# nmap -p 80

Starting Nmap 4.11 ( http://
Interesting ports on server2
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
```

19. Scan a TCP Port

You can also specify specific port types and numbers with nmap to scan.

```
[root@server1 ~]# nmap -p T:

Starting Nmap 4.11 ( http://
Interesting ports on server2
PORT     STATE SERVICE
```

```
80/tcp   open  http
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
```

20. Scan a UDP Port

```
[root@server1 ~]# nmap -sU 5

Starting Nmap 4.11 ( http://
Interesting ports on server2
PORT     STATE SERVICE
53/udp   open  http
8888/udp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
```

21. Scan Multiple Ports

You can also scan multiple ports using option "**-p**".

```
[root@server1 ~]# nmap -p 80

Starting Nmap 4.11 ( http://
Interesting ports on server2
PORT    STATE  SERVICE
80/tcp  open   http
```

18 Tar Command Examples in Linux

```
443/tcp closed https
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
```

22. Scan Ports by Network Range

You can scan ports with ranges using expressions.

```
[root@server1 ~]#  nmap -p 8
```

23. Find Host Services version Numbers

We can find out service's versions which are running on remote hosts with "**-sV**" option.

```
[root@server1 ~]# nmap -sV 1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE VERSI
22/tcp   open  ssh     OpenS
80/tcp   open  http    Apach
111/tcp  open  rpcbind  2 (r
957/tcp  open  status   1 (r
3306/tcp open  mysql   MySQL
8888/tcp open  http    light
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
```

24. Scan remote hosts using TCP ACK (PA) and TCP Syn (PS)

Sometimes packet filtering firewalls blocks standard **ICMP** ping requests, in that case, we can use **TCP ACK** and **TCP Syn** methods to scan remote hosts.

```
[root@server1 ~]# nmap -PS 1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
You have new mail in /var/sp
```

18 Tar Command Examples in Linux

25. Scan Remote host for specific ports with TCP ACK

```
[root@server1 ~]# nmap -PA -

Starting Nmap 4.11 ( http://
Interesting ports on server2
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address 
You have new mail in /var/sp
```

26. Scan Remote host for specific ports with TCP Syn

```
[root@server1 ~]# nmap -PS -

Starting Nmap 4.11 ( http://
Interesting ports on server2
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:D9:8E:
```

18 Tar Command Examples in Linux

```
Nmap finished: 1 IP address
You have new mail in /var/sp
```

27. Perform a stealthy Scan

```
[root@server1 ~]# nmap -sS 1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address
You have new mail in /var/sp
```

28. Check most commonly used Ports with TCP Syn

```
[root@server1 ~]# nmap -sT 1
```

```
Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerboo
MAC Address: 08:00:27:D9:8E:

Nmap finished: 1 IP address 
You have new mail in /var/sp
```

29. Perform a tcp null scan to fool a firewall

```
[root@server1 ~]# nmap -sN 1

Starting Nmap 4.11 ( http://
Interesting ports on server2
Not shown: 1674 closed ports
PORT     STATE         SERVI
22/tcp   open|filtered ssh
80/tcp   open|filtered http
111/tcp  open|filtered rpcbi
957/tcp  open|filtered unkno
3306/tcp open|filtered mysql
8888/tcp open|filtered sun-a
MAC Address: 08:00:27:D9:8E:
```

```
Nmap finished: 1 IP address
You have new mail in /var/sp
```

That's it with **NMAP** for now, I'll be coming up more creative options of **NMAP** in our second part of this serious. Till then, stay tuned with us and don't forget to share your valuable comments.

Sharing is Caring...

Share on Facebook | Share on Twitter | Share on Linkedin | Share on Reddit

If You Appreciate What We Do Here On TecMint, You Should Consider:

1. Stay Connected to: Twitter | Facebook | Google Plus
2. Subscribe to our email updates: Sign Up Now

18 Tar Command Examples in Linux

Tags: linux nmap command nmap commands nmap example commads

Tarunika Shrivastava View all Posts

I am a linux server admin and love to play with Linux and all other distributions of it. I am working as System Engineer with a Web Hosting Company.

Your name can also be listed here. Got a tip? Submit it here to become an TecMint author.

18 Tar Command Examples in Linux

Tecmint
Linux Foundation LFCS / LFCE Certification Preparation Guide
LINUX FOUNDATION CERTIFIED SYSADMIN
LINUX FOUNDATION CERTIFIED ENGINEER
CentOS

PREVIOUS STORY
Trouble Maker – Breaks Your Linux Machine and Ask You to Fix Broken Linux

NEXT STORY
BleachBit – A Free Disk Space Cleaner and Privacy Guard for Linux Systems

YOU MAY ALSO LIKE...

27

How to Set Static IP Address and Configure Network in Linux

13 APR, 2016

2

Exa – A Modern Replacement for “ls Command” Written in Rust

7 AUG, 2017

5

Manage Files Effectively using head, tail and cat Commands in Linux

1 APR, 2014

35 RESPONSES

Comments 7 Pingbacks

18 Tar Command Examples in Linux

ruchi May 22, 2019 at 11:00 am

Hello,

I was doing **udp** port scanning on **nmap** .I have some udp ports open but in nmap it is showing open | filtered only. Please give me solution for this. Is there any other tool for this?

Reply

jared February 19, 2019 at 4:58 am

This article was very helpful! Thanks for taking the time to write this.

Reply

Muhammad Karam Shehzad

November 4, 2016 at 5:09 pm

What is the best way to go about finding all ports being used by MySQL for clustering purposes?

I am on Linux platform with MySQL NDB 5.7. I am trying to monitor all traffic related to MySQL clustering – between data nodes, management node and sql nodes. To that end, I used netstat to list all open ports listening on my machine before starting MySQL cluster. Then, I started MySQL cluster and ran netstat again. I assumed that the ports that were listening the second time around, but not the first time, were related to MySQL clustering.

But there are two problems with this. First, there could be ports opened by other processes between the two netstat runs. Second, MySQL might open other ports after I ran the netstat command the second time.

What is the best way to go about finding all ports being used by MySQL for clustering purposes? I believe ephemeral ports are picked dynamically, so perhaps if I knew all the MySQL clustering related processes that would

18 Tar Command Examples in Linux

be running, I can figure out every port that they are using. Pointers will be very welcome.

Reply

joy November 3, 2016 at 2:53 pm

nice post

Reply

borris July 9, 2016 at 12:21 am

very nice article thanks although i did already learned all this just by reading the man page supplied by nmap :)

Reply

bustdathing January 3, 2016 at 9:15 pm

Good article, but using a version of Nmap many versions behind. Also should review the NSE (NMAP SCRIPTING ENGINE) , very powerful. Version 7 of nmap brings a lot of interesting features to the table.

Reply

Ravi Saive January 4, 2016 at 10:41 am

@Bustdathing,

Thanks for updating about NSE (NMAP SCRIPTING ENGINE).. never heard about it…Let me check and see what kind of other features its provides than standard Nmap..

Reply

« Older Comments

GOT SOMETHING TO SAY? JOIN THE DISCUSSION.

Comment

18 Tar Command Examples in Linux

Name *

Email *

Website

□

Save my name, email, and website in this browser for the next time I comment.

□ **Notify me of followup comments via e-mail. You can also subscribe without commenting.**

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

LINUX MONITORING TOOLS

- CBM – Shows Network Bandwidth in Ubuntu
- whowatch – Monitor Linux Users and Processes in Real Time
- Sysstat – All-in-One System Performance and Usage Activity Monitoring Tool For Linux

LINUX INTERVIEW QUESTIONS

- 10 MySQL Database Interview Questions for Beginners and Intermediates
- 10 Useful "Squid Proxy Server" Interview Questions and Answers in Linux
- 10 Core Linux Interview Questions and Answers

OPEN SOURCE TOOLS

- 6 Online Tools for Generating and Testing Cron Jobs for Linux
- 11 Best Tools to Access Remote Linux Desktop
- 9 Tools to Monitor Linux Disk Partitions and Usage in Linux

18 Tar Command Examples in Linux

How to Install Zabbix Agent and Add Windows Host to Zabbix Monitoring – Part 4

Use Glances to Monitor Remote Linux in Web Server Mode

10 VsFTP (Very Secure File Transfer Protocol) Interview Questions and Answers

10 Useful Interview Questions and Answers on Linux Commands

5 Most Frequently Used Open Source Shells for Linux

21 Best Open Source Text Editors (GUI + CLI) in 2019

18 Tar Command Examples in Linux