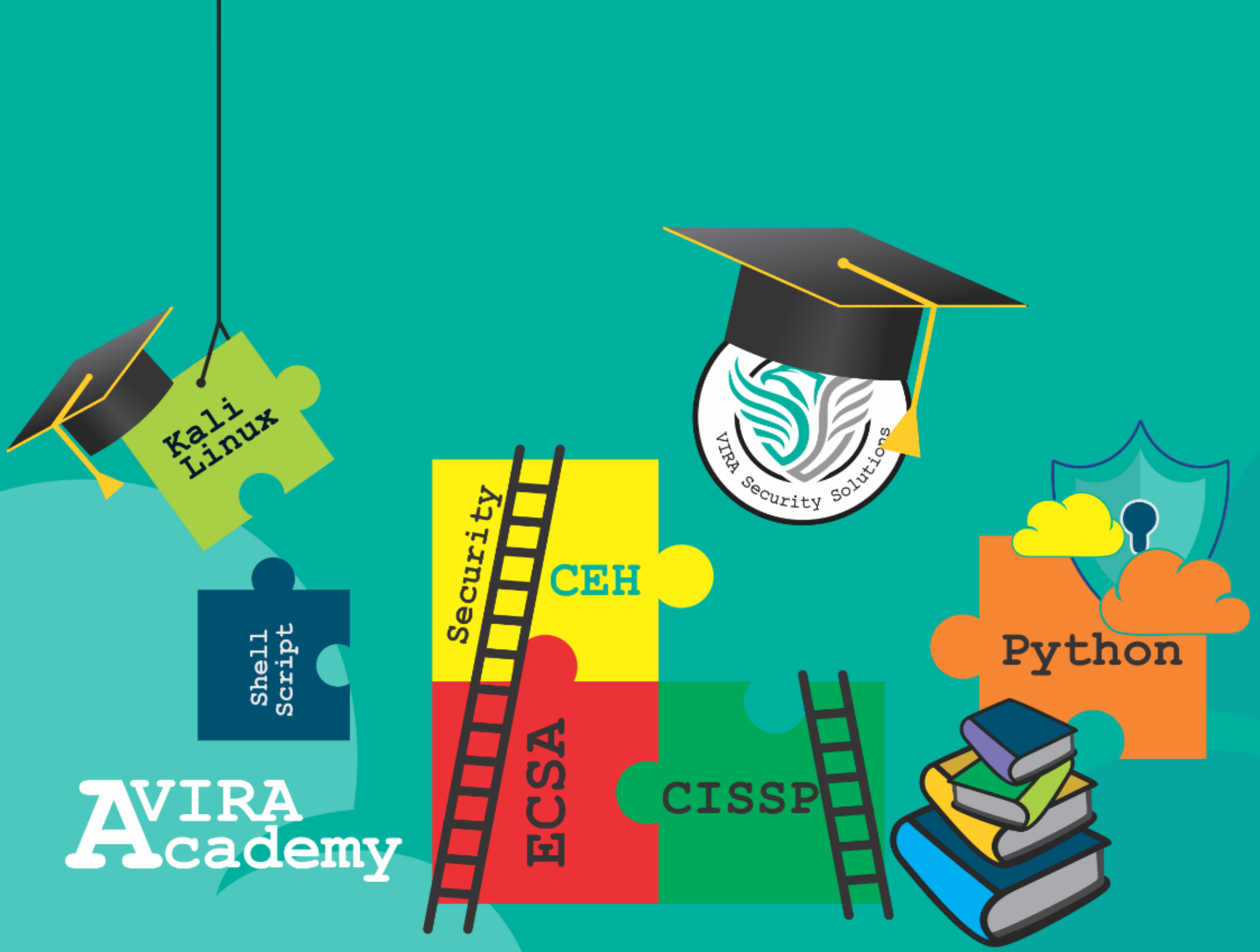
VIRA Security Solutions

راهکارهای امن ویرا
شماره ثبت: ۵۴۰۱۳۹
VIRA Security Solutions


Kali Linux
VIRA Security Solutions
Security
CEH
Shell Script
Python
ECSA
CISSP
AVIRA Academy

Linux

Part8

Mohammad Reza Gerami
Mrgerami@aut.ac.ir
gerami@virasec.ir

Linux Syslog

Tips

How To Setup SysLog Server on CentOS 7 / RHEL 7

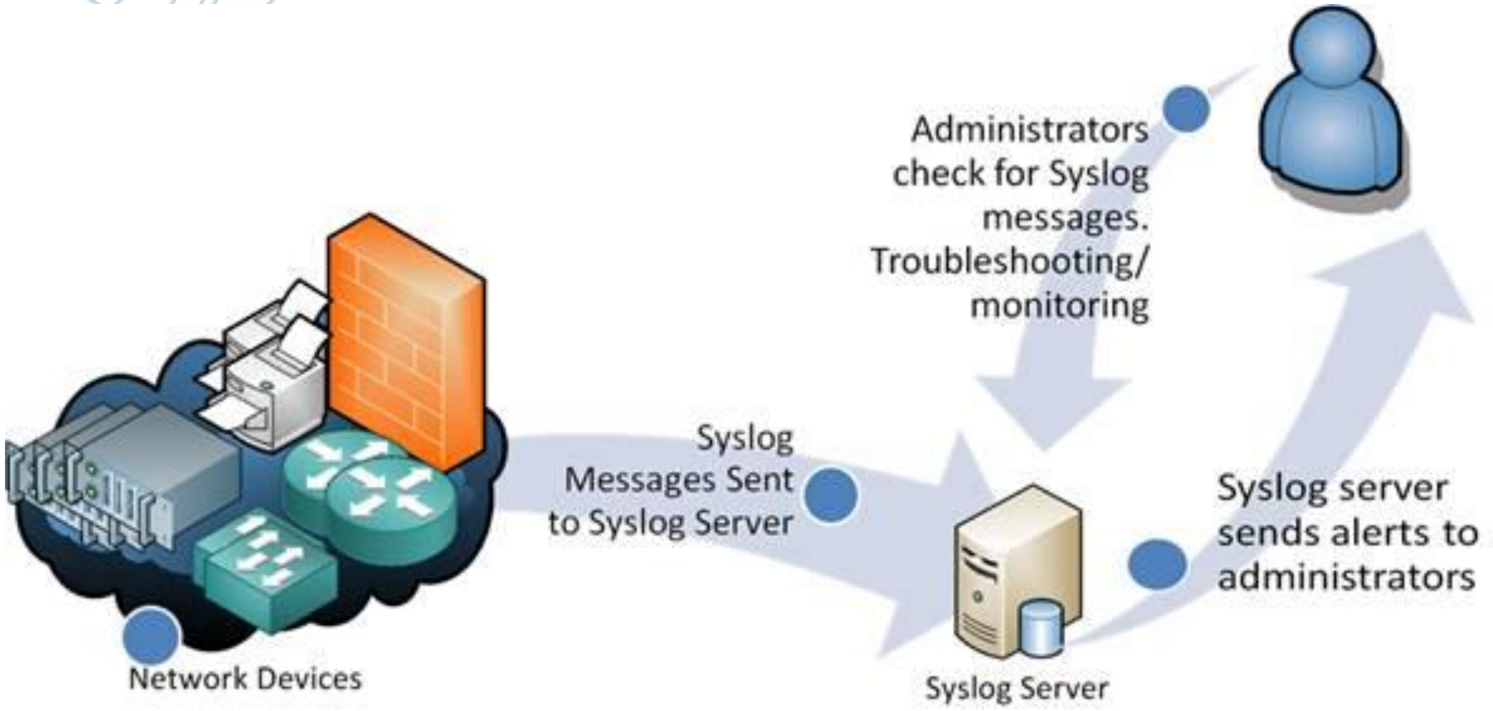
Syslog is a way for network devices to send event messages to a logging server – usually known as a Syslog server.

The Syslog protocol is supported by a wide range of devices and can be used to log different types of events. For example, a router might send messages about users logging on to console sessions, while a web-server might log access-denied events.

Most network equipment, like routers and switches, can send Syslog messages.

Tips

How To Setup SysLog Server on CentOS 7 / RHEL 7


Administrators check for Syslog messages. Troubleshooting/ monitoring
Syslog Messages Sent to Syslog Server
Syslog server sends alerts to administrators
Network Devices
Syslog Server

Tips

How To Setup SysLog Server on CentOS 7 / RHEL 7

Syslog Servers
Syslog is a great way to consolidate logs from multiple sources into a single location. Typically, most Syslog servers have a couple of components that make this possible.

A Syslog Listener:
A Syslog server needs to receive messages sent over the network. A listener process gathers syslog data sent over UDP port 514. UDP messages aren't acknowledged or guaranteed to arrive, so be aware that some network devices will send Syslog data via TCP 1468 to ensure message delivery.

A Database:
Large networks can generate a huge amount of Syslog data. Good Syslog servers will use a database to store syslog data for quick retrieval.

Management and Filtering Software:
Because of the potential for large amounts of data, it can be cumbersome to find specific log entries when needed. The solution is to use a syslog server that both automates part of the work, and makes it easy to filter and view important log messages. Syslog servers should be able to generate alerts, notifications, and alarms in response to select messages – so that administrators know as soon as a problem occurs and can take swift action!

Tips

How To Setup SysLog Server on CentOS 7 / RHEL 7

Syslog Server Setup

Install the Rsyslog package, if you do not have it installed.

```
yum -y install rsyslog
```

Edit the /etc/rsyslog.conf file.

```
vi /etc/rsyslog.conf
```

How To Setup SysLog Server on CentOS 7 / RHEL 7

TCP or UDP

Rsyslog supports both UDP and TCP protocol for receiving logs. TCP protocol provides reliable transmission of logs.

UDP

Uncomment the following to enable the syslog server to listen on the UDP protocol.

FROM:

```
# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514
```

TO:

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

Tips

How To Setup SysLog Server on CentOS 7 / RHEL 7

TCP

Uncomment the following to enable the syslog server to listen on the TCP protocol.

FROM:

```
# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
```

TO:

```
# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

Restart the syslog service

```
systemctl restart rsyslog
```

Verify the syslog server listening on the port 514.

```
netstat -antup | grep 514
```

Output:

```
udp     0    0 0.0.0.0:514       0.0.0.0:*                1467/rsyslogd
udp6     0    0 :::514          :::*                1467/rsyslogd
```

How To Setup SysLog Server on CentOS 7 / RHEL 7

Syslog Client Setup

Install the Rsyslog package, if you do not have it installed.

```
yum -y install rsyslog
```

Edit the /etc/rsyslog.conf file.

```
vi /etc/rsyslog.conf
```

At the end of the file place the following line to point the client message log to the server.

UDP

```
*.info;mail.none;authpriv.none;cron.none @192.168.0.10:514
```

TCP

```
*.info;mail.none;authpriv.none;cron.none @@192.168.0.10:514
```

You can use either the hostname or the ip address.

Restart the syslog service

```
systemctl restart rsyslog
```

Tips

How To Setup SysLog Server on CentOS 7 / RHEL 7

Now all the message logs are sent to the central server and also it keeps the copy locally.

Firewall

Mostly all the production environments are protected by a hardware firewall, ask them to open the TCP & UDP 514.

If you have FirewallD enabled, run the following command on a server in order to accept incoming traffic on UDP / TCP port 514.

TCP

```
firewall-cmd --permanent --add-port=514/tcp
firewall-cmd –reload
```

UDP

```
firewall-cmd --permanent --add-port=514/udp
firewall-cmd --reload
```

How To Setup SysLog Server on CentOS 7 / RHEL 7 Validate

Goto the syslog server and view the messages log file.

```
tail -f /var/log/messages
```

You should see the client’s logs are being recorded in a syslog server.

```
Feb  9 04:26:09 client systemd: Stopping System Logging Service...
Feb  9 04:26:09 client rsyslogd: [origin software="rsyslogd" swVersion="8.24.0-41.el7_7.2" x-pid="910" x-info="http://www.rsyslog.com"] exiting on signal 15.
Feb  9 04:26:09 client systemd: Stopped System Logging Service.
Feb  9 04:26:09 client systemd: Starting System Logging Service...
Feb  9 04:26:09 client rsyslogd: [origin software="rsyslogd" swVersion="8.24.0-41.el7_7.2" x-pid="1546" x-info="http://www.rsyslog.com"] start
Feb  9 04:26:09 client systemd: Started System Logging Service.
```

In this way, you can monitor the other logs such as secure, mail, cron logs, etc.

Linux Tips

Tips

dmesg

The ‘dmesg‘ command displays the messages from the kernel ring buffer. A system passes multiple runlevel from where we can get lot of information like system architecture, cpu, attached device, RAM etc. When computer boots up, a kernel (core of an operating system) is loaded into memory. During that period number of messages are being displayed where we can see hardware devices detected by kernel.

The messages are very important in terms of diagnosing purpose in case of device failure. When we connect or disconnect hardware device on the system, with the help of dmesg command we come to know detected or disconnected information on the fly.
The dmesg command is available on most Linux and Unix based Operating System.
Let’s throw some light on most famous tool called ‘dmesg’ command with their practical examples as discussed below. The exact syntax of dmesg as follows.

```
dmseg [options...]
```

Tips

List all loaded Drivers in Kernel

We can use text-manipulation tools i.e. ‘more‘, ‘tail‘, ‘less‘ or ‘grep‘ with dmesg command. As output of dmesg log won’t fit on a single page, using dmesg with pipe more or less command will display logs in a single page.

```
dmesg | more
dmesg | less
```

Tips

List all loaded Drivers in Kernel

```
dmesg | more
dmesg | less
```

```
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Initializing cgroup subsys cpuacct
[    0.000000] Linux version 3.11.0-13-generic (buildd@aatxe) (gcc version 4.8.1
(Ubuntu/Linaro 4.8.1-10ubuntu8) ) #20-Ubuntu SMP Wed Oct 23 17:26:33 UTC 2013
(Ubuntu 3.11.0-13.20-generic 3.11.6)
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   NSC Geode by NSC
[    0.000000]   Cyrix CyrixInstead
[    0.000000]   Centaur CentaurHauls
[    0.000000]   Transmeta GenuineTMx86
[    0.000000]   Transmeta TransmetaCPU
[    0.000000]   UMC UMC UMC UMC
```

Tips

List all Detected Devices

```
dmesg | grep sda
```

To discover which hard disks has been detected by kernel, you can search for the keyword “sda” along with “grep” like shown below.

```
[    1.280971] sd 2:0:0:0: [sda] 488281250 512-byte logical blocks: (250 GB/232 GiB)
[    1.281014] sd 2:0:0:0: [sda] Write Protect is off
[    1.281016] sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
[    1.281039] sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[    1.359585]  sda: sda1 sda2 < sda5 sda6 sda7 sda8 >
[    1.360052] sd 2:0:0:0: [sda] Attached SCSI disk
[    2.347887] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts: (null)
[   22.928440] Adding 3905532k swap on /dev/sda6.  Priority:-1 extents:1 across:3905532k FS
[   23.950543] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro
```

NOTE: The ‘sda’ first SATA hard drive, ‘sdb’ is the second SATA hard drive and so on. Search with ‘hda’ or ‘hdb’ in the case of IDE hard drive.

Tips

Print Only First 20 Lines of Output

```
dmesg | head  -20
```

The ‘head’ along with dmesg will show starting lines i.e. ‘dmesg | head -20’ will print only 20 lines from the starting point.

```
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Initializing cgroup subsys cpuacct
[    0.000000] Linux version 3.11.0-13-generic (buildd@aatxe) (gcc version 4.8.1 (Ubuntu/Linaro 4.8.1-10ubuntu8) )
#20-Ubuntu SMP Wed Oct 23 17:26:33 UTC 2013 (Ubuntu 3.11.0-13.20-generic 3.11.6)
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   NSC Geode by NSC
[    0.000000]   UMC UMC UMC UMC
[    0.000000] e820: BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000007dc08bff] usable
```

Tips

Print Only Last 20 Lines of Output

```
dmesg | tail  -20
```

The ‘tail’ along with dmesg command will print only 20 last lines, this is useful in case we insert removable device.

```
parport0: PC-style at 0x378, irq 7 [PCSPP,TRISTATE]
ppdev: user-space parallel port driver
EXT4-fs (sda1): mounted filesystem with ordered data mode
Adding 2097144k swap on /dev/sda2.  Priority:-1 extents:1 across:2097144k
readahead-disable-service: delaying service auditd
ip_tables: (C) 2000-2006 Netfilter Core Team
nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
NET: Registered protocol family 10
lo: Disabled Privacy Extensions
e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
Slow work thread pool: Starting up
Slow work thread pool: Ready
```

Tips

Search Detected Device or Particular String

It’s difficult to search particular string due to length of dmesg output. So, filter the lines with are having string like ‘usb‘ ‘dma‘ ‘tty‘ and ‘memory‘ etc. The ‘-i’ option instruct to grep command to ignore the case (upper or lower case letters).

```
dmesg | grep -i usb
dmesg | grep -i dma
dmesg | grep -i tty
dmesg | grep -i memory
```

Tips

Clear dmesg Buffer Logs

Yes, we can clear dmesg logs if required with below command. It will clear dmesg ring buffer message logs till you executed the command below. Still you can view logs stored in ‘/var/log/dmesg‘ files. If you connect any device will generate dmesg output.

```
dmesg -c
```

Tips

Monitoring dmesg in Real Time

Some distro allows command ‘tail -f /var/log/dmesg’ as well for real time dmesg monitoring.

```
watch "dmesg | tail -20"
```

Tips

How to View Linux System Information

To know only system name, you can use uname command without any switch will print system information or uname -s command will print the kernel name of your system.

```
uname
```

To view your network hostname, use ‘-n’ switch with uname command as shown.

```
uname -n
```

To get information about kernel-version, use ‘-v’ switch.

```
uname -v
```

Tips

How to View Linux System Information

To get the information about your kernel release, use ‘-r’ switch.

```
uname -r
```

To print your machine hardware name, use ‘-m’ switch:

```
uname -m
```

All this information can be printed at once by running ‘uname -a’ command as shown below.

```
uname -a
```

Tips

How to View Linux System Hardware Information

Here you can use the lshw tool to gather vast information about your hardware components such as cpu, disks, memory, usb controllers etc.
lshw is a relatively small tool and there are few options that you can use with it while extracting information. The information provided by lshw gathered form different /proc files.

Note: Do remember that the lshw command executed by superuser (root) or sudo user.

To print information about your Linux system hardware, run this command.

```
lshw
lshw -short
lshw -html > lshw.html
```

Tips

How to View Linux CPU Information

To view information about your CPU, use the lscpu command as it shows information about your CPU architecture such as number of CPU's, cores, CPU family model, CPU caches, threads, etc from sysfs and /proc/cpuinfo.

lscpu

Tips

How to Collect Linux Block Device Information

Block devices are storage devices such as hard disks, flash drives etc. lsblk command is used to report information about block devices as follows.

```
lsblk
```

If you want to view all block devices on your system then include the -a option.

```
lsblk -a
```

Tips

How to Print USB Controllers Information

The lsusb command is used to report information about USB controllers and all the devices that are connected to them.

```
lsusb
```

You can use the -v option to generate a detailed information about each USB device.

```
lsusb -v
```

Tips

How to Print PCI Devices Information

PCI devices may included usb ports, graphics cards, network adapters etc. The lspci tool is used to generate information concerning all PCI controllers on your system plus the devices that are connected to them.
To print information about PCI devices run the following command

lspci

Use the -t option to produce output in a tree format.

lspci -t

Use the -v option to produce detailed information about each connected device.

lspci -v

Tips

How to Print Information about SATA Devices

You can find some information about sata devices on your system as follows using the hdparm utility. In the example below, I used the block device /dev/sda1 which the harddisk on my system.

```
hdparm /dev/sda1
```

To print information about device geometry interms of cylinders, heads, sectors, size and the starting offset of the device, use the -g option.

```
hdparm -g /dev/sda1
```

Tips

How to Print Linux File System Information

To gather information about file system partitions, you can use fdisk command. Although the main functionality of fdisk command is to modify file system partitions, it can also be used to view information about the different partitions on your file system.

You can print partition information as follows. Remember to run the command as a superuser or else you may not see any output.

```
fdisk -l
```

Tips

How to Extract Information about Hardware Components

You can also use the dmidecode utility to extract hardware information by reading data from the DMI tables. To print information about memory, run this command as a superuser.

```
dmidecode -t memory
```

To print information about system, run this command.

```
dmidecode -t system
```

To print information about BIOS, run this command.

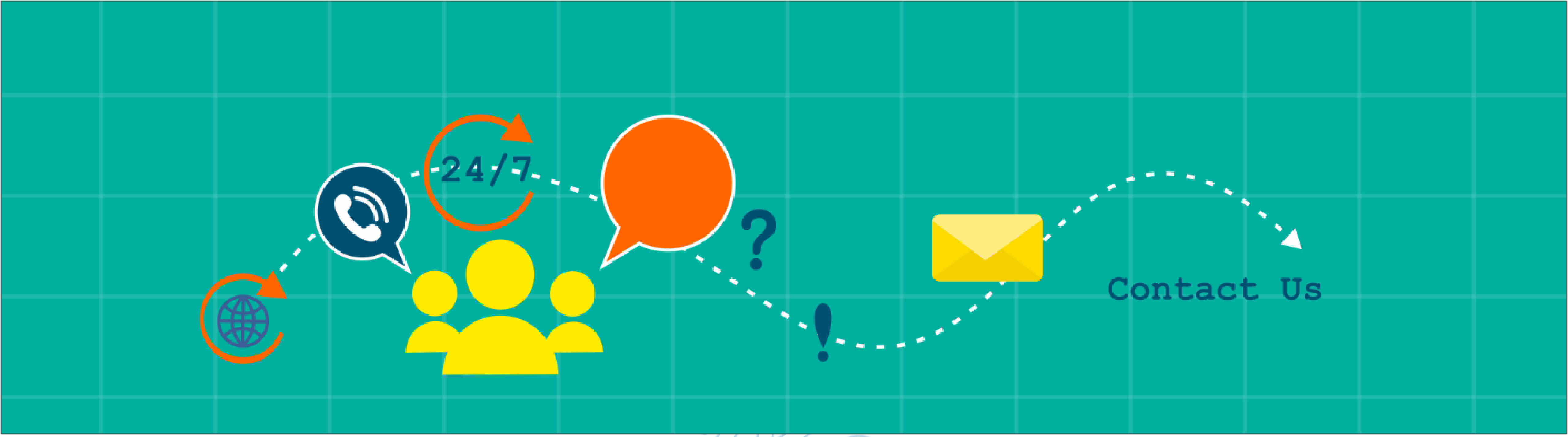
```
dmidecode -t bios
```

Tips

How to Extract Information about Hardware Components

To print information about processor, run this command.

```
dmidecode -t processor
```



Visiting Address: Unit 20, Floor 4, No 53 Vafa Manesh Ave
Heravi, Pasdaran Ave, TEHRAN-IRAN

Post Code:1668838803

Tel No: 0098 21 2298 1027-09125792641

Email: info@ virasecsolutions.com

Website: www.virasecsolutions.com

آدرس: تهران، پاسداران، هروی، خیابان وفامنش، پلاک ۵۳
طبقه چهارم، واحد ۲۰
کد پستی: ۱۶۶۸۸۳۸۸۰۳
شماره تماس: ۰۲۱۲۲۹۸۱۰۲۷-۰۹۱۲۵۷۹۲۶۴۱