

# **Threat Hunting Home-Lab Using Velociraptor**

**By GOKUL KRISHNA K**

## **Objective**

Install and configure Velociraptor on a Linux-based server to create a centralized endpoint monitoring and forensic analysis platform capable of collecting system artifacts, performing live response operations, and enabling proactive threat-hunting activities. This includes setting up the Velociraptor server and client components, managing endpoint check-ins, configuring artifact collections, and analyzing acquired data to identify suspicious behaviors, security anomalies, and indicators of compromise across the environment

## **Tools used**

- .Velociraptor Server & Client
- .Ubuntu server
- .Ubuntu Desktop
- .Virtual Box

# Create a Directory for Velociraptor

```
gokul@gokul:~$ sudo mkdir -p /opt/velociraptor
gokul@gokul:~$ cd /opt/velociraptor
```

Command: sudo mkdir -p /opt/velociraptor  
cd /opt/velociraptor

# Download Velociraptor

I downloaded the velociraptor binary from github

Command: sudo wget  
<https://github.com/Velocidex/velociraptor/releases/download/v0.73/velociraptor-v0.73.2-linux-amd64>

**I rename and make the binary executable:**

```
gokul@gokul:/opt/velociraptor$ sudo chmod +x velociraptor-v0.73.2-linux-amd64
gokul@gokul:/opt/velociraptor$ ls -la
total 59164
drwxr-xr-x 2 root root      4096 Dec  1 21:37 .
drwxr-xr-x 4 root root      4096 Dec  1 21:36 ..
-rwxr-xr-x 1 root root 60571808 Oct 21 2024 velociraptor-v0.73.2-linux-amd64
```

This is for give the executable permission to the file for execute

Command: sudo chmod +x velociraptor-v0.73.2-linux-amd64

## I configure Velociraptor Using Interactive Mode :

I use Velociraptor's interactive configuration mode because it automatically guides us through all the required setup steps, ensures correct server-client settings, and prevents configuration mistakes.

# Update Server Config file

```

dtsk_size: 1073741824
filename_linux: /var/tmp/Velociraptor_Buffer.bin
filename_windows: STEMP/Velociraptor_Buffer.bin
filename_darwin: /var/tmp/Velociraptor_Buffer.bin

API:
  hostname: localhost
  bind_address: 127.0.0.1
  bind_port: 8001
  bind_scheme: tcp
GUI:
  bind_address: 10.0.2.15
  bind_port: 8889
  gw_certificate: |

-----BEGIN CERTIFICATE-----
MIIDQTCAtmgAwIBAgIQFu93fYAf1qzntJDu0vrTANBgkhkIg9w0BAQsFADAA
MRgwFgYDVQKxEw9hZkxvY2lyYXB03IgQ6EwhCNjUxhjAxTcyMD3vhCNnjYx
MjAxMTcyMDM3WApMRUwEwDyVQKCEwxZkxvY2lyYXBB03IxEDAOBgNVBAMb0dS
UENFR1cwgGE1MA0cCSqSISb3D0EBAAUA4AIB0wAwggEKAoIBAQcgUeJWx2Mb46M1
q5aa9wERY6qJUtbvitsghghAaIosseKUGDtzLex/wALx+E1Lece309q+s5R9Y
zgVx9+c26ck2Nbvb04ev5fCN4gor0nXjDRouvg3jExUBgQuIRB-kzof5Va
d3/rphMvxAsF9v-40ifyu1WL5MCurP1ku+Hz75olupx1bEnghiou9xHmzL2z
PlmXmkDgQ83VQfLByqdFt91lf1i+0cLztLT5qgoFOulehkwQS1HECB07nAkz
Tsvs5G01GsdwvnnepmghdClnkKtXwunVZ7/TR01wtwJh/Ovestw-a8NN3z4T2e8
rELFcveAgMBAAQJdByMA4GA1UdDwEB/wQEAWIfodAdbgHSUfjAUUbggrgbEF
9Ecduougtt851ffASbgNVHREECzAjjgdHULBX0xdMAcG0gqS1B30QfBCwJA
A1IBAQCKLd/d0f0h4d0h4d0N1+v4Lp06GCFMLj/gy7kdhmeeqnyL07kj
9EKWt32uLJhuc2u1GnMDT01y2+q907RXa0Wzlh85vuW1fuwJffrsdmFnDp0A
ugGLC/FCNf6j0cAzWFp2VHectqBwUNKLKy/hbN78VTF5Ksc2yD1PxHcSeFF8
FDX035FvoumTS190J-93ptlv/m/okLC6AmAyKq4ggSdL3JseuY/qw4DEeIDjhz
DB0/obsdca1dpUpJQ-0dppdqPM
-----END CERTIFICATE-----

gw_private_key: |
-----BEGIN PRIVATE KEY-----
MIIEogIBAAKCAQ0EAoPHVsdfG0jNaumvbxEM01VF279bbPTYTUT0G1KLHjLB
g7cyxFmf8AC8RP1953nHtzavrkfwn6lcfnnTnuctjAhBzzzuHr0nwjd+BqK9J
4w0crAlYN4xMVAkfokQfp60+Gnd/66YTFCzALBfb/u0n8o7tVL+TA+kadSr
vh8++aJbqc1GxJ4ISKPcR45t19h51spY4Ad1UB54wcqnRXJSIn9sfDnItv
-----END PRIVATE KEY-----
```

^A Help      ^O Write Out      ^W Where Is      ^K Cut      ^T Execute      ^C Location      M-U Undo      M-E Redo      M-S Set Mark      M-B To Bracket      M-Q Where Was      M-W Next

I open Server Config file with the help of nano command and changed the bind address to my velo server ip

## I Created debian file for Velociraptor server and Install

```

container [<flags>] <directory> <files>...
golden [<flags>] <directory>
acl
  show [<flags>] <principal>
  grant [<flags>] <principal> [<policy>]
  gnt [<flags>]
  hunts
    reconstruct
  collector [<flags>] [<spec_file>]
  pool_client [<flags>]
  query [<flags>] <queries>...
  rpm [<flags>]
    client [<flags>]
    server [<flags>]
  tools
    show [<file>]
    rm <name>
    upload --name=NAME [<flags>] [<path>]
  unzip [<flags>] <file> [<members>]
  user
    add --role=ROLE <username> [<password>]
    show [<flags>] <username>
  version
  vql
    list
    export [<old_file>]

Command 'debian' not found, did you mean:
  command 'debian' from deb debian-goodies (0.87ubuntu1.1)
Try: apt install <deb name>
root@ubuntu:/opt/velociraptor# ./velociraptor-v0.73.2-linux-amd64 --config server.config.yaml debian server --binary velociraptor-v0.73.2-linux-amd64
Creating amd64 server package at velociraptor_server_0.73.2_amd64.deb
root@ubuntu:/opt/velociraptor# ls
client.config.yaml  velociraptor_server_0.73.2_amd64.deb
server.config.yaml  velociraptor-v0.73.2-linux-amd64
```

I create and install a Velociraptor .deb file to properly install the server as a system-managed service on Linux, ensuring easier deployment, updates, and long-term stability.

Command: ./velociraptor-v0.73.2-linux-amd64 --config server.config.yaml  
debian server --binary velociraptor-v0.73.2-linux-amd64

## I Extract and Install

```
root@ubuntu:/opt/velociraptor# dpkg -i velociraptor_server_0.73.2_amd64.deb
Selecting previously unselected package velociraptor-server.
(Reading database ... 202631 files and directories currently installed.)
Preparing to unpack velociraptor_server_0.73.2_amd64.deb ...
Unpacking velociraptor-server (0.73.2) ...
Setting up velociraptor-server (0.73.2) ...
Adding group 'velociraptor' (GID 137) ...
Done.
Adding system user 'velociraptor' (UID 129) ...
Adding new user 'velociraptor' (UID 129) with group 'velociraptor' ...
Not creating home directory '/etc/velociraptor/'.
Created symlink /etc/systemd/system/multi-user.target.wants/velociraptor_server.service → /etc/systemd/system/velociraptor_server.service.
root@ubuntu:/opt/velociraptor#
```

Extracting and installing Velociraptor unpacks the program files, places them into correct system directories, applies proper permissions, and enables Velociraptor to run reliably as a managed Linux service

Command: dpkg -i velociraptor-v0.73.2-linux-amd64.deb

## Checking the Validity

```
root@ubuntu:/opt/velociraptor# systemctl status velociraptor_server.service
● velociraptor_server.service - Velociraptor server
   Loaded: loaded (/etc/systemd/system/velociraptor_server.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2025-12-03 19:59:06 IST; 2min 41s ago
       Main PID: 3838 (velociraptor.bin)
          Tasks: 14 (limit: 2262)
         Memory: 48.3M
            CPU: 13.163s
          CGroup: /system.slice/velociraptor_server.service
                  └─3838 /usr/local/bin/velociraptor.bin --config /etc/velociraptor/server.config.yaml frontend
                      ├─3844 /usr/local/bin/velociraptor.bin --config /etc/velociraptor/server.config.yaml frontend

Dec 03 19:59:06 ubuntu systemd[1]: Started Velociraptor server.
root@ubuntu:/opt/velociraptor#
```

I run this command to check whether the Velociraptor server service is running correctly, to view its current status, and to identify any errors or issues during startup.

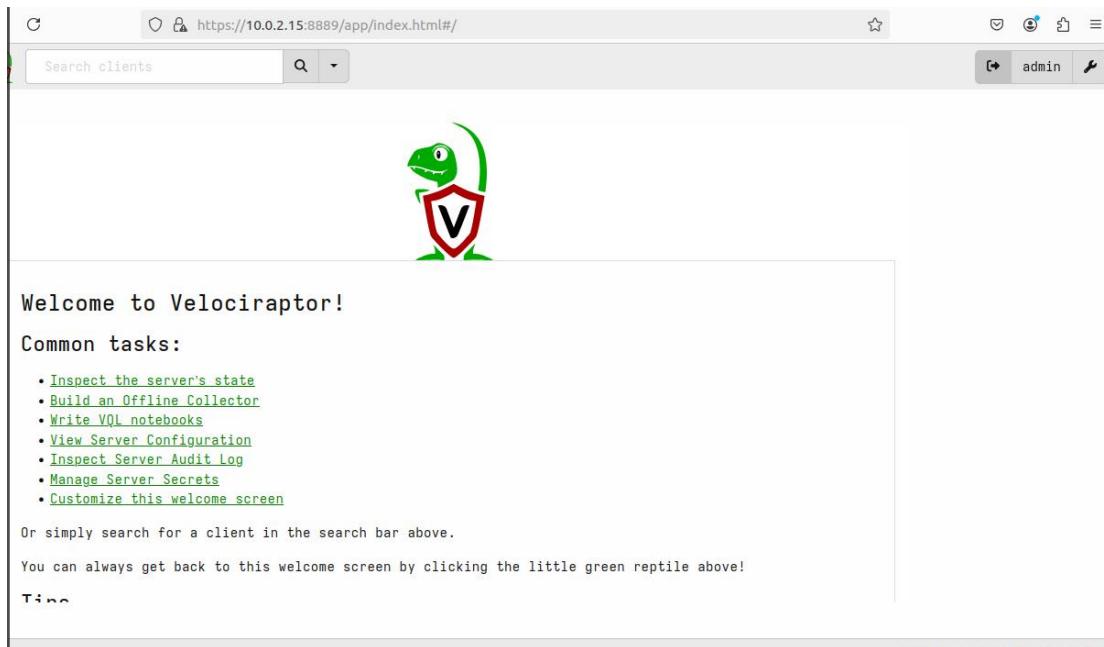
Command: systemctl status velociraptor\_server.service

## Open firewall ports

```
root@ubuntu:/opt/velociraptor# ufw allow 8000/tcp
Rules updated
Rules updated (v6)
root@ubuntu:/opt/velociraptor# ufw allow 8889/tcp
Rules updated
Rules updated (v6)
root@ubuntu:/opt/velociraptor#
```

open firewall ports to allow communication between the Velociraptor server and its endpoint clients, ensuring they can connect, send telemetry, and receive instructions.

Command: ufw allow port number



So I had set the server of velociraptor.next I am going to configure client

## Velociraptor Ubuntu Client Set up

In this stage i created client debian file on Velociraptor server. The same binary file will be used for both client and server.

```
root@ubuntu:/opt/velociraptor# ./velociraptor-v0.73.2-linux-amd64 --config client.config.yaml debian client
Creating amd64 client package at velociraptor_client_0.73.2_amd64.deb
```

Command: ./velociraptor-v0.73.2-linux-amd64 --config client.config.yaml debian client

```
gokul@ubuntu:/opt/velociraptor$ scp velociraptor_client_0.73.2_amd64.deb 10.0.2.15:/tmp/
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:XACeMRmrcn9XciUHZ1e6E50CiFGjgWeqEVdRt500SEK.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
gokul@10.0.2.15's password:
velociraptor_client_0.73.2_amd64.deb                                         100%   22MB   8.9MB/s   00:02
gokul@ubuntu:/opt/velociraptor$
```

Next I transferred this file to Client system using SCP command.

Command: scp velociraptor\_client\_0.73.2\_amd64.deb Client IP Address:/tmp/

```
gokul@gokul:/tmp$ ls
snap-private-tmp
systemd-private-c8078b66fe5f4ef68af9837a43550164-ModemManager.service-Xb5KXd
systemd-private-c8078b66fe5f4ef68af9837a43550164-power-profiles-daemon.service-pa0ze5
systemd-private-c8078b66fe5f4ef68af9837a43550164-switcheroo-control.service-Ubd6YL
systemd-private-c8078b66fe5f4ef68af9837a43550164-systemd-logind.service-fh8Udu
systemd-private-c8078b66fe5f4ef68af9837a43550164-systemd-oamd.service-ONZJeH
systemd-private-c8078b66fe5f4ef68af9837a43550164-systemd-resolved.service-WNeunV
systemd-private-c8078b66fe5f4ef68af9837a43550164-systemd-timesyncd.service-H2GvZh
velociraptor_client_0.73.2_amd64.deb
gokul@gokul:/tmp$
```

I got the debian file inside the tmp directory of my ubuntu desktop client machine

## Extract the debian file

```
root@gokul:/tmp# dpkg -i velociraptor_client_0.73.2_amd64.deb
Selecting previously unselected package velociraptor-client.
(Reading database ... 163803 files and directories currently installed.)
Preparing to unpack velociraptor_client_0.73.2_amd64.deb ...
Unpacking velociraptor-client (0.73.2) ...
Setting up velociraptor-client (0.73.2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/velociraptor_client.service → /etc/systemd/system/velociraptor_client.service.
root@gokul:/tmp#
```

Command: dpkg -i /tmp/velociraptor\_client\_0.73.2\_amd64.deb

## Check the status

```
root@gokul:/tmp# systemctl status velociraptor_client.service
● velociraptor_client.service - Velociraptor client
   Loaded: loaded (/etc/systemd/system/velociraptor_client.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2025-12-03 16:28:53 UTC; 5min ago
       Main PID: 23286 (velociraptor_cl)
          Tasks: 8 (limit: 11291)
        Memory: 27.3M
           CPU: 1min 27.391s
          CGroup: /system.slice/velociraptor_client.service
                   └─23286 /usr/local/bin/velociraptor_client --config /etc/velociraptor/client.config.yaml

Dec 03 16:28:53 gokul systemd[1]: Started Velociraptor client.
lines 1-11/11 (END)
```

My client velo also successfully running

Command: systemctl status velociraptor\_client.service

	Client ID	Hostname	FQDN	OS Version	Labels
	C.fd64c495c236d15e	gokul	gokul	ubuntu22.04	

My velo server successfully added my client ubuntu device

The screenshot shows the Velo web interface with the following details:

**Client Overview:**

- Client ID:** C.fd64c495c236d15e
- Agent Version:** 0.73.2
- Agent Build Time:** 2024-10-21T00:14:07Z
- First Seen At:** 2025-12-03T18:14:30Z
- Last Seen At:** 2025-12-03T18:28:16.265Z
- Last Seen IP:** 10.0.2.15:50014
- Labels:** None

**Operating System:**

- Hostname:** gokul
- FQDN:** gokul
- Release:** ubuntu22.04
- Architecture:** amd64
- MAC Addresses:** 08:00:27:ca:6b:64

**Client Metadata:**

None

Bottom right corner: 2025-12-03T18:20:18.794Z

This is the overview of my client ubuntu machine

The screenshot shows the VFS interface for the client 'gokul' with the following details:

**File System Overview:**

- auto:** Contains boot, cdrom, dev, etc, home, lost+found, media, mnt, opt, proc, root, run, snap, srv, sys, tmp, usr, var.
- ntfs:** Contains registry.

**/bin:**

Download	Name	Size	Mode	mtime	atime
	bin	7	lrwxrwxrwx	2024-09-11T14:18:27Z	2025-12-03T07:30:16Z
	boot	4Kb	drwxr-xr-x	2025-12-03T15:32:14Z	2025-12-03T15:32:18Z
	cdrom	4Kb	dr-xr-xr-x	2024-09-11T18:46:29Z	2025-12-03T07:28:19Z
	dev	4Kb	drwxr-xr-x	2025-12-03T15:05:03Z	2025-12-03T15:24:47Z
	etc	12Kb	drwxr-xr-x	2025-12-03T18:14:28Z	2025-12-03T15:56:12Z

**/bin Properties:**

Size	7
Mode	lrwxrwxrwx
Mtime	2024-09-11T14:18:27Z
Atime	2025-12-03T07:30:16Z
Ctime	2025-12-03T07:28:19Z
Btime	0001-01-01T00:00:00Z

Bottom right corner: 2025-12-04T07:57:52.442Z

I can see my full directories and the files inside those directories of my client ubuntu system

## Conclusion

By setting up Velociraptor Server,i create a dedicated endpoint forensics and threat-hunting platform. This environment allows SOC analysts and incident responders to collect forensic artifacts, run VQL queries, and investigate suspicious activity across multiple endpoints in real time.