

# 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

```

jokul@jokul:~/git/velociraptor$ sudo wget https://github.com/Velocidae/velociraptor/releases/download/v0.73/velociraptor-v0.73.2-linux-amd64

--2025-12-01 21:37:34-- https://github.com/Velocidae/velociraptor/releases/download/v0.73/velociraptor-v0.73.2-linux-amd64
Resolving github.com (github.com)... 64:ff9b:b9c7:6d85::208
Connecting to github.com (github.com):[64:ff9b:b9c7:6d85::208]... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://release-assets.githubusercontent.com/github-production-release-asset/126567080/3257690d-bb6b-476b-9eb3-b13dd3493339?rh=-a818-1-0988rs-b9pqt-hptpsse-2025-12-011733407334142Zscd-attchmentb8n3f1lenamex3velociraptor-v0.73.2-linux-amd64rscat-type=application/octet-stream [Following]
33f1lenamex3velociraptor-v0.73.2-linux-amd64rscat-type=application/octet-stream [Following]
HTTP request sent, awaiting response... 200 OK
length: 60571806 (58M) [application/octet-stream]
Saving to: 'velociraptor-v0.73.2-linux-amd64'

velociraptor-v0.73.2-linux-amd64 100%[=====] 57.77M 357KB/s in 11n 41s

2025-12-01 21:49:19 (64.3 KB/s) - 'velociraptor-v0.73.2-linux-amd64' saved [60571806/60571806]

```

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 :

```
gokul@gokul:/opt/velociraptor$ sudo /opt/velociraptor/velociraptor-v0.73.2-linux-and64 config generate
[sudo] password for gokul:
?
Welcome to the Velociraptor configuration generator
-----
I will be creating a new deployment configuration for you. I will
begin by identifying what type of deployment you need.

What OS will the server be deployed on?
linux
? Path to the datastore directory. yes
? Self Signed SSL
? What is the public DNS name of the Master Frontend (e.g. www.example.com): localhost
? Enter the frontend port to listen on. 8000
? Enter the port for the GUI to listen on. 8889
? Would you like to try the new experimental websocket comms?

Websocket is a bidirectional low latency communication protocol supported by
most modern proxies and load balancers. This method is more efficient and
portable than plain HTTP. Be sure to test this in your environment.
Yes
? Would you like to use the registry to store the writeback files? (Experimental) No
? Which DynDns provider do you use? none
? GUI Username or email address to authorize (empty to end): admin
? Password
X Sorry, your reply was invalid: Value is required
? GUI Username or email address to authorize (empty to end): admin
? GUI Username or email address to authorize (empty to end): admin
? GUI Username or email address to authorize (empty to end): admin
? GUI Username or email address to authorize (empty to end): admin
[INFO] 2025-12-01T17:20:36Z
[INFO] 2025-12-01T17:20:36Z
[INFO] 2025-12-01T17:20:36Z
[INFO] 2025-12-01T17:20:36Z
[INFO] 2025-12-01T17:20:36Z
[INFO] 2025-12-01T17:20:36Z
[INFO] 2025-12-01T17:20:36Z Digging deeper! https://www.velocidex.com
[INFO] 2025-12-01T17:20:36Z This is Velociraptor 0.73.2 built on 2024-10-21T00:14:07Z (3f1f268)
[INFO] 2025-12-01T17:20:36Z Generating keys please wait....
? Path to the logs directory. Enter
? Do you want to restrict VQL functionality on the server?

This is useful for a shared server where users are not fully trusted.
It removes potentially dangerous plugins like execve(), filesystem access etc.

NOTE: This is an experimental feature only useful in limited situations. If you
do not know you need it select N here!
No
? Where should I write the server config file? server.config.yaml
? Where should I write the client config file? client.config.yaml
```

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

```

#-----BEGIN CERTIFICATE-----
MIIEQTCCAkgwIBAgIQFgu93XfYAf1qzntJDv0vrrTANBgkqhkiG9w0BAQsFAoAa
MRgwFgYDVQKQEW9H2kxvY2lyYXB0b3Igc09EwHhcNjUxMjAxMTcyMDM3Mjc3YX
MjAxMTcyMDM3MjUxMTUwQKQKQKQKQKQKQKQKQKQKQKQKQKQKQKQKQKQKQKQKQK
UENFR1cwggE1MA0GCSCGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCGUeJWx2Mb46M1
q5Aa9VERY63guTbv1ts8hghQhAaIosseKUGDtZLEK/wALXE+P1Lece309q+sSR9Y
zqVx9+c226cK2MCEHbP04ev5FCN34Gor0nXjDRytouVg3jEXUBQWLRB+kzopSYa
d3/rpHwXKASf9v+401fyJuLW5KCURpIKuH75oLupx1TBengh10u9xHjm2L2F
PlmXKdQ0B3VQLjBykdF9iLi1j+80c12wL15qgorouetHwXZQ5IHECB07aAKz
TsVs5G01GsdRwTnEqhQdCjLnWkFXUnVZ7/TR01wTDjM/ove5Iw+a8NN3z4T2e8
rrrElFcevAgwBAACjd0BYMA4GA1UdDwEB/wQEAwIFoAdBgNVHSUEFjAUBgggrBgEF
BQcDAQYIKwYBBQUHAWIwDAYDVRR0AQH/BAIwADAfBgNVHSMEGDAwBQqbJx60Yqr
9cESAougH2tT85LffjASBgNVHREECzA3ggdHULB0X6dXMA0GCSCGSIb3DQEBCwUA
A4IBAQCkLE0/doAck887PqXtCHmWvJLuiok2q6IKESqTCwbU0Jumy6gI12X66A
9EKvLmUoSpb1nr4T6HJhudaN1+vALnCPbdGCPmJj/0y074ldHhweegnyZL07Kj
s70kt3zulTjhuw2uz1GnMDT0jyz4n907RxaDWZ1h85uW11fukjFfrsbnfdnPorA
UpGlc/fcNFg40cAZwHFD2VNhecqTBwUNK1KCY/hbN78vTF5Kac2YbIPxnHcSeFF8
FDx033Fvgun7sL9qrj+0JPTLV/m/okLC6AAyKq4gqS9dL3jseuY/qw4DEeIJMyhZ
Db56/ubsdcaLdpugDLQJDDpdqPM
-----END CERTIFICATE-----

gw_private_key: |
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAoFHVsdjG+0jNauWmvbXEW0LYFE279bbPIYIUTG1KLLH1B
g7CyxfBAC8BPj9S3nhtzvavrEkfNm6LcfnNtuncTjAh82zzuHr0nwjd+BqK9J1
4w0craLLYN4xMVAakFokFpM6D+WGnd/g6YTFcZALBfb/udon8o7tVl+Tarkad5r
vh8++aJbqcYLGxJ4ISKFPcR45t19Ht5L5pA4EAd1UB54wcqNRX/SIn9SftDnItr

```

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>]
gui [<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 'debman' 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.bi)
        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

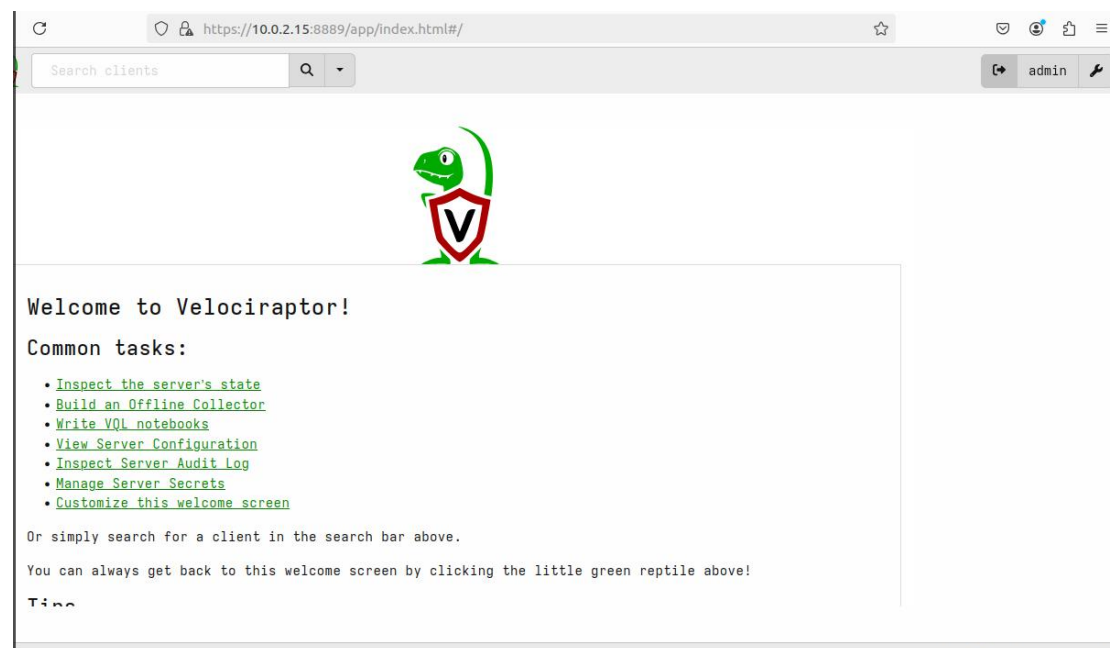
```

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:XACeMRrcn9XciUHZ1e6E50ClFGjgWeqEVdRtS00SEK.
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-ps02e5
systemd-private-c8078b66fe5f4ef68af9837a43550164-switcheroo-control.service-Ub05YL
systemd-private-c8078b66fe5f4ef68af9837a43550164-systemd-logind.service-fh9UdU
systemd-private-c8078b66fe5f4ef68af9837a43550164-systemd-oomd.service-CNZJeH
systemd-private-c8078b66fe5f4ef68af9837a43550164-systemd-resolved.service-WHeunv
systemd-private-c8078b66fe5f4ef68af9837a43550164-systemd-timesyncd.service-W36vZh
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

```

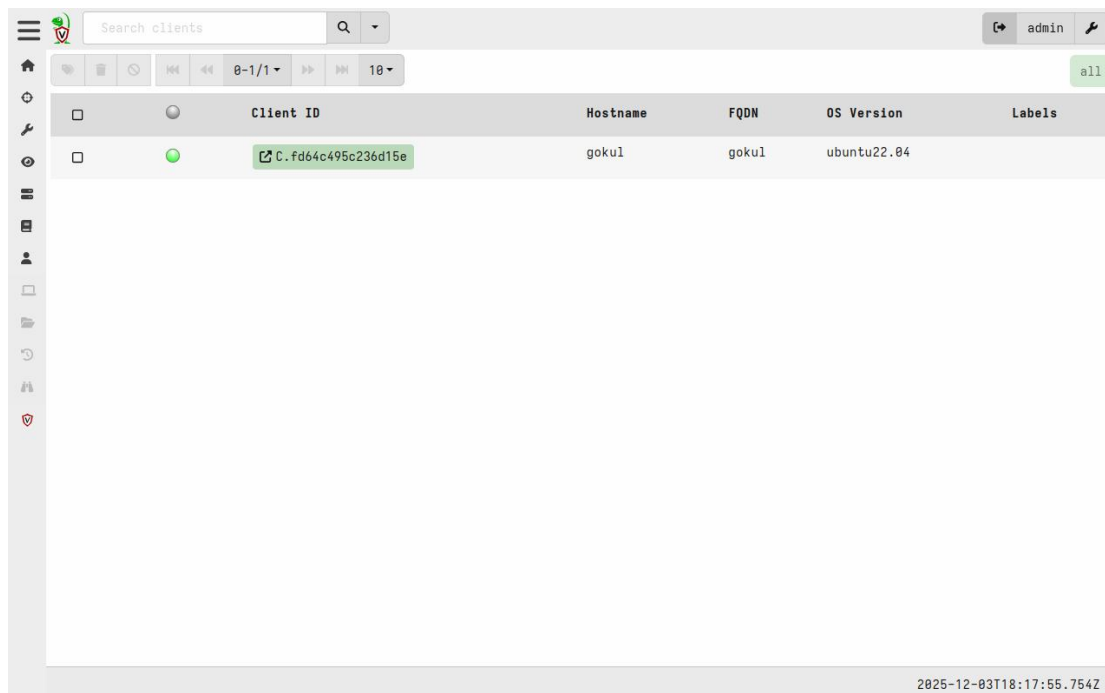
root@gokul:/tmp# systemctl status velociraptor_client.service
● velociraptor_client.service - Velociraptor client
   Loaded: loaded (/etc/systemd/system/velociraptor_client.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-12-03 16:28:53 UTC; 5min ago
     Main PID: 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`



The screenshot shows the Velociraptor web interface. At the top, there is a search bar labeled 'Search clients' and a user profile icon for 'admin'. Below the search bar, there are navigation icons and a table of clients. The table has columns for 'Client ID', 'Hostname', 'FQDN', 'OS Version', and 'Labels'. A single client is listed with the ID 'C.f64c495c236d15e', hostname 'gokul', FQDN 'gokul', and OS version 'ubuntu22.04'. The client's status is indicated by a green circle and the label 'all'. The bottom of the interface shows a timestamp '2025-12-03T18:17:55.754Z'.

Client ID	Hostname	FQDN	OS Version	Labels
C.f64c495c236d15e	gokul	gokul	ubuntu22.04	all



My velo server successfully added my client ubuntu device

Search clients

gokul Connected

admin

InterrogateVFSCollected

OverviewVQL DrilldownShell

gokul

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

2025-12-03T18:20:16.265Z

Last Seen IP

10.0.2.15:50014

Labels

Operating System

linux

Hostname

gokul

FQDN

gokul

Release

ubuntu22.04

Architecture

amd64

MAC Addresses

08:00:27:ca:6b:64

Client Metadata

+

2025-12-03T18:20:18.794Z

This is the overview of my client ubuntu machine

10.0.2.14:8889/app/index.html#/vfs/C.fd64c495c236d15e/auto/

gokul Connected

admin

auto

boot

cdrom

dev

etc

home

lost+found

media

mnt

opt

proc

root

run

snap

srv

sys

tmp

usr

var

ntfs

registry

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

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

Properties

DevMajor

253

DevMinor

0

FSType

ext2

Link

usr/bin

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.