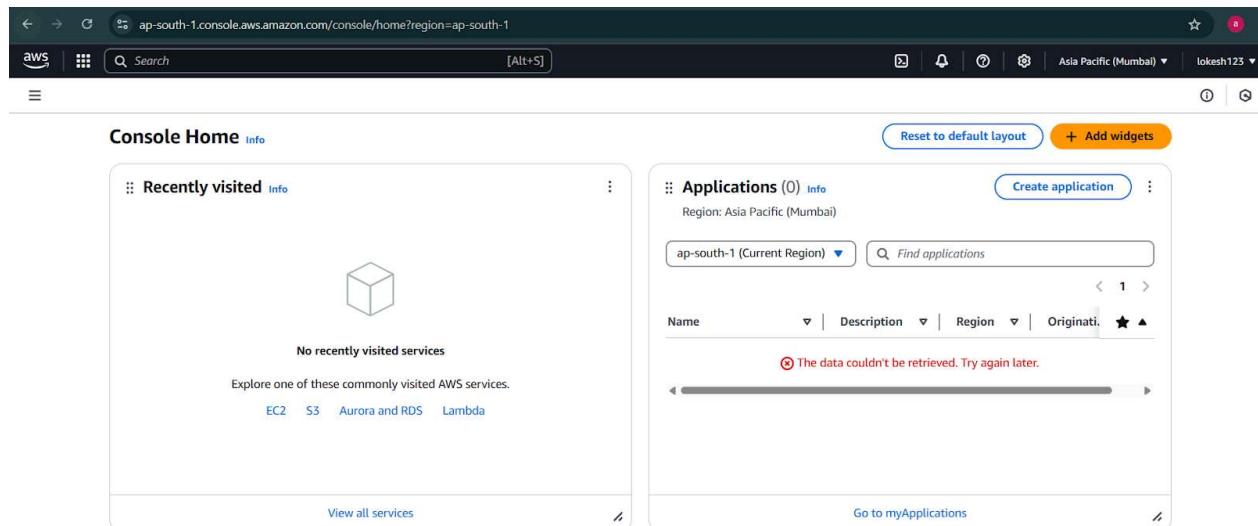


PART1

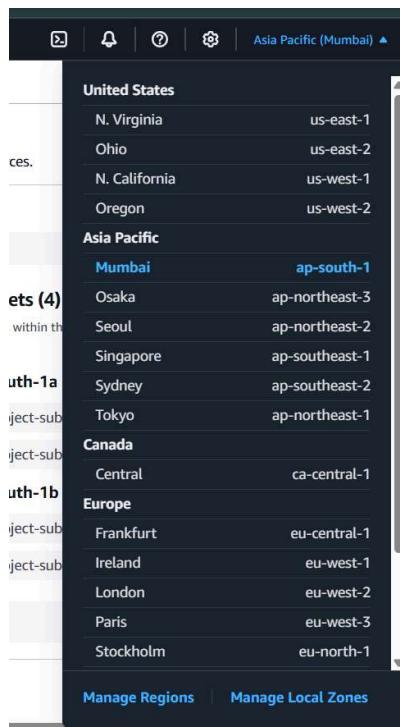
1. Set up AWS/GCP/Azure VPC with subnets, NAT gateways, and security groups.

AWS Console



The screenshot shows the AWS Console Home page. On the left, there's a "Recently visited" section with a large cube icon and a message "No recently visited services". Below it, there are links to EC2, S3, Aurora and RDS, and Lambda. On the right, there's an "Applications" section with a message "The data couldn't be retrieved. Try again later." and a "Create application" button. The top navigation bar shows the region as "ap-south-1" and the user as "lokesh123".

Make sure region should be same for entire project you do



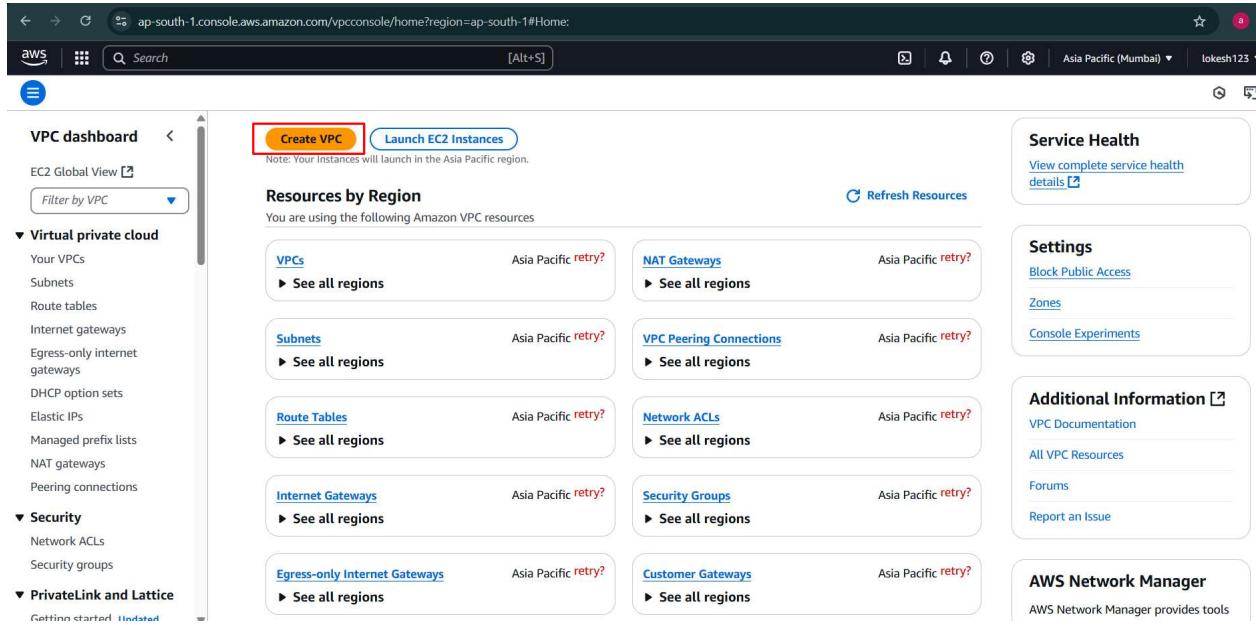
The screenshot shows a dropdown menu for selecting a region. The "Asia Pacific (Mumbai)" region is selected and highlighted in blue. Other regions listed include N. Virginia, us-east-1; Ohio, us-east-2; N. California, us-west-1; Oregon, us-west-2; Mumbai, ap-south-1; Osaka, ap-northeast-3; Seoul, ap-northeast-2; Singapore, ap-southeast-1; Sydney, ap-southeast-2; Tokyo, ap-northeast-1; Central, ca-central-1; Frankfurt, eu-central-1; Ireland, eu-west-1; London, eu-west-2; Paris, eu-west-3; and Stockholm, eu-north-1. At the bottom of the menu are "Manage Regions" and "Manage Local Zones" buttons.

VPC

Service that lets you launch your AWS resources in a logically isolated virtual network. By default, you can have a maximum of 5 VPC per region (soft limit) and 5 CIDR per VPC.

Default vpc is created when you create an account in aws for every region , default vpc comes with Subnets , route table , internet gateway.

Creating Custom VPC



The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with navigation links for VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, and Peering connections. Below that is a section for Security (Network ACLs, Security groups) and PrivateLink and Lattice. The main content area has a heading 'Resources by Region' and a note: 'Note: Your Instances will launch in the Asia Pacific region.' It features several cards: 'VPCs' (Asia Pacific), 'Subnets' (Asia Pacific), 'Route Tables' (Asia Pacific), 'Internet Gateways' (Asia Pacific), 'Egress-only Internet Gateways' (Asia Pacific), 'NAT Gateways' (Asia Pacific), 'VPC Peering Connections' (Asia Pacific), 'Network ACLs' (Asia Pacific), 'Security Groups' (Asia Pacific), and 'Customer Gateways' (Asia Pacific). There are also 'See all regions' links for each category. On the right, there are three boxes: 'Service Health' (with a link to 'View complete service health details'), 'Settings' (with links to 'Block Public Access', 'Zones', and 'Console Experiments'), and 'Additional Information' (with links to 'VPC Documentation', 'All VPC Resources', 'Forums', and 'Report an Issue'). At the bottom right is a box for 'AWS Network Manager'.

Give custom name for VPC

/16 is maximum CIDR notation for VPC

← → ⌂ ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateVpc:createMode=vpcOnly

warn Search [Alt+S] Asia Pacific (Mumbai) | lokes

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
my-vpc-01

IPv4 CIDR block Info
 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block
10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
 No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block IPv6 CIDR owned by me

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="my-vpc-01"/> X Remove tag

Add tag
You can add 49 more tags

Cancel Preview code Create VPC

Created custom vpc with no other component (like subnets , Internet GateWay, route table)

Make sure you to enable DNS hostname & DNS resolution so that any instance that running in VPC can connect to public internet

You successfully created **vpc-0fada53abedf1fe48 / my-vpc-01**

vpc-0fada53abedf1fe48 / my-vpc-01

Details Info

VPC ID vpc-0fada53abedf1fe48	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-00ed73b11bd723ef8	Main route table rtb-0b9e690c3a6001fe1
Main network ACL acl-02ab85a65a234cd25	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 396608771079

Resource map Info

VPC Show details Your AWS virtual network

Subnets (0) Subnets within this VPC

Route tables (1) Route network traffic to resources

Network connections Connections to

Edit VPC Settings -> Enable DNS hostnames

You successfully created **vpc-0fada53abedf1fe48 / my-vpc-01**

vpc-0fada53abedf1fe48 / my-vpc-01

Details Info

VPC ID vpc-0fada53abedf1fe48	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-00ed73b11bd723ef8	Main route table rtb-0b9e690c3a6001fe1
Main network ACL acl-02ab85a65a234cd25	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 396608771079

Actions ▾

- Create flow log
- Edit VPC settings**
- Edit CIDRs
- Manage middlebox routes
- Manage tags
- Delete VPC

Click on save

The screenshot shows the 'Edit VPC settings' page for a VPC with ID `vpc-0fada53abedf1fe48`. In the 'DNS settings' section, two checkboxes are present: 'Enable DNS resolution' (unchecked) and 'Enable DNS hostnames' (checked). The 'Enable DNS hostnames' checkbox is highlighted with a red border. At the bottom right, there are 'Cancel' and 'Save' buttons.

Now you can see

The screenshot shows the 'VPC dashboard' page. A green success message at the top states: 'You have successfully modified the settings for vpc-0fada53abedf1fe48 / my-vpc-01'. Below it, the 'Details' section for the VPC is displayed. Key information includes:

- VPC ID:** `vpc-0fada53abedf1fe48`
- State:** Available
- Tenancy:** default
- Main network ACL:** `acl-02ab85a65a234cd25`
- IPv6 CIDR (Network border group):** -
- Block Public Access:** Off
- DNS resolution:** Enabled
- Default VPC:** No
- IPv4 CIDR:** `10.0.0.0/16`
- Network Address Usage metrics:** Disabled
- Block Public Access:** Off
- DNS hostnames:** Enabled
- Main route table:** `rtb-0b9e690c3a6001fe1`
- IPv6 pool:** -
- Route 53 Resolver DNS Firewall rule groups:** -
- Owner ID:** `396608771079`

The screenshot shows the 'Your VPCs' section of the VPC dashboard. It lists one VPC entry:

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
<code>my-vpc-01</code>	<code>vpc-0fada53abedf1fe48</code>	Available	Off	<code>10.0.0.0/16</code>	-

Subnets

In console these all subnet are default subnet of that particular region

Click on Create Subnet

The screenshot shows the AWS VPC dashboard with the URL ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#subnets. On the left, there's a sidebar with 'VPC dashboard' and 'Virtual private cloud' sections. The main area is titled 'Subnets (3) Info' with a search bar. A table lists three subnets:

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-033647cbe46b74495	Available	vpc-04a1fb36c899c76be	Off	172.31.32.0/24
-	subnet-006b6c8ea965f9fca	Available	vpc-04a1fb36c899c76be	Off	172.31.0.0/24
-	subnet-0514d50004e9c6f79	Available	vpc-04a1fb36c899c76be	Off	172.31.16.0/24

A red box highlights the 'Create subnet' button at the top right.

Creating 2 public subnets for zone A and zone B

The screenshot shows the 'Create subnet' wizard with the URL ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateSubnet. It's on the first step, 'Create subnet'. The 'VPC' section shows a dropdown for 'VPC ID' containing 'my-vpc-01'. The 'Associated VPC CIDRs' section shows 'IPv4 CIDRs' set to '10.0.0.0/16'.

The screenshot shows the 'Subnet settings' step with the URL ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateSubnet. It's on 'Subnet 1 of 2'. The 'Subnet name' field is 'public-subnet-A'. The 'Availability Zone' dropdown is set to 'Asia Pacific (Mumbai) / ap-south-1a'. The 'IPv4 VPC CIDR block' dropdown is set to '10.0.0.0/16'. The 'IPv4 subnet CIDR block' dropdown is set to '10.0.0.0/20'. The 'Tags - optional' section has a tag 'Name' with value 'public-subnet-A'.

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateSubnet

VPC > Subnets > Create subnet

Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 4,096 IPs
< > ^ v

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="public-subnet-B"/> Remove

[Add new tag](#)
You can add 49 more tags.
[Remove](#)

Creating 2 private subnets for zone A and zone B

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateSubnet

VPC > Subnets > Create subnet

Subnet 3 of 4

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 4,096 IPs
< > ^ v

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="private-subnet-A"/> Remove

[Add new tag](#)
You can add 49 more tags.
[Remove](#)

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 4,096 IPs
[Edit](#)

Tags - optional
Key Value - optional [Remove](#)
[Add new tag](#)
You can add 49 more tags.
[Remove](#)

Click on create subnets



Newly created Subnets

You have successfully created 4 subnets: subnet-012b871ec3a0c5341, subnet-0744e6215266c2022, subnet-09fe98352e83b73db, subnet-08e76e011f48dbbef

Last updated less than a minute ago [Actions](#) [Create subnet](#)

Subnets (4) Info

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
<input type="checkbox"/>	private-subnet-B	subnet-08e76e011f48dbbef	Available	vpc-0fada53abedf1fe48 my-v...	<input type="radio"/> Off	10.0.48.0/20
<input type="checkbox"/>	public-subnet-A	subnet-012b871ec3a0c5341	Available	vpc-0fada53abedf1fe48 my-v...	<input type="radio"/> Off	10.0.0.0/20
<input type="checkbox"/>	private-subnet-A	subnet-09fe98352e83b73db	Available	vpc-0fada53abedf1fe48 my-v...	<input type="radio"/> Off	10.0.32.0/20
<input type="checkbox"/>	public-subnet-B	subnet-0744e6215266c2022	Available	vpc-0fada53abedf1fe48 my-v...	<input type="radio"/> Off	10.0.16.0/20

Select a subnet

Internet Gateway

Create Internet Gateway

Internet Gate way -> create internet gateway

The screenshot shows the 'Create internet gateway' wizard. In the 'Internet gateway settings' section, a 'Name tag' is specified as 'my-custom-igw'. Under 'Tags - optional', a single tag 'Name: my-custom-igw' is added. At the bottom right are 'Cancel' and 'Create internet gateway' buttons.

The screenshot shows the details page for the created internet gateway. It displays the Internet gateway ID (igw-09b1b1fe32b3aea7f), State (Detached), VPC ID (-), and Owner (396608771079). The 'Tags' section shows the tag 'Name: my-custom-igw'. There is a 'Manage tags' button and a navigation bar with icons for back, forward, and search.

2 internet gateways listed

One is default internet gateway

Other is which is custom gateway which I created

The screenshot shows a list of two internet gateways. The first is 'my-custom-igw' (ID: igw-09b1b1fe32b3aea7f, State: Detached, VPC ID: -, Owner: 396608771079). The second is a default gateway (ID: igw-07f1d91678de29938, State: Attached, VPC ID: vpc-04a1fb36c899c76be, Owner: 396608771079). The table includes columns for Name, Internet gateway ID, State, VPC ID, and Owner. There are 'Actions' and 'Create internet gateway' buttons at the top right.

Name	Internet gateway ID	State	VPC ID	Owner
my-custom-igw	igw-09b1b1fe32b3aea7f	Detached	-	396608771079
-	igw-07f1d91678de29938	Attached	vpc-04a1fb36c899c76be	396608771079

VPC dashboard

Internet gateways (1/2)

Name	Internet gateway ID	State	VPC ID
my-custom-igw	igw-09b1b1fe32b3aea7f	Detached	-
-	igw-07fd91678de29938	Attached	vpc-04a1fb36c899c

igw-09b1b1fe32b3aea7f / my-custom-igw

Details

Internet gateway ID igw-09b1b1fe32b3aea7f	State Detached	VPC ID -	Owner 396608771079
--	-------------------	-------------	-----------------------

Only 1 internet gateway is attached to 1 VPC

VPC > Internet gateways > Attach to VPC (igw-09b1b1fe32b3aea7f)

Attach to VPC (igw-09b1b1fe32b3aea7f)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

Q vpc-0fada53abedf1fe48

AWS Command Line Interface command

You can perform the same actions on this page by using the AWS Command Line Interface (CLI) tools. [Learn more](#)

Platform

Choose the platform from which you'll be running this command. The command parameters may be specified differently depending on the platform. Learn more about [specifying parameter values](#).

Linux/Unix/OS X

CLI command

If you're using the AWS CLI tools, you can copy and paste this command - which includes the parameters you specified on this page - into your command line prompt or terminal. Learn more about the available [AWS CLI commands](#).

```
aws ec2 attach-internet-gateway --vpc-id "vpc-0fada53abedf1fe48" --internet-gateway-id "igw-09b1b1fe32b3aea7f" --region ap-south-1
```

Copy

Cancel

Attach internet gateway

Route Table

VPC dashboard < EC2 Global View Filter by VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs

Route tables (2) Info Find resources by attribute or tag

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-0b9e690c3a6001fe1	-	-	Yes	vpc-0fada53abedf1fe48 my-v...
-	rtb-0135143a502c82967	-	-	Yes	vpc-04a1fb36c899c76be

Select a route table

Routable created with vpc, it has all the subnets which we created in vpc

VPC dashboard < EC2 Global View Filter by VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections Security Network ACLs Security groups PrivateLink and Lattice Getting started Updated

VPC vpc-0fada53abedf1fe48 | my-vpc-01 Owner ID 396608771079

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (0) Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnet associations You do not have any subnet associations.			

Subnets without explicit associations (4) Edit subnet associations

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
private-subnet-B	subnet-08e76e011f48dbbf	10.0.48.0/20	-
public-subnet-A	subnet-012b871ec3a0c5341	10.0.0.0/20	-
private-subnet-A	subnet-09fe98352e83b73db	10.0.32.0/20	-
public-subnet-B	subnet-0744e6215266c2022	10.0.16.0/20	-

The route table with the custom internet gateway does not have access to internet

VPC dashboard < VPC > Route tables > rtb-0b9e690c3a6001fe1

rtb-0b9e690c3a6001fe1

Details **Info**

Route table ID: rtb-0b9e690c3a6001fe1
Main: Yes
Owner ID: vpc-0fada53abedf1fe48 | my-vpc-01

Explicit subnet associations: -
Edge associations: -

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Click on create route table

VPC dashboard < VPC > Route tables

Route tables (2) Info

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-0b9e690c3a6001fe1	-	-	Yes	vpc-0fada53abedf1fe48 my-vpc-01
-	rtb-0135143a502c82967	-	-	Yes	vpc-04a1fb36c899c76be

Last updated about 3 hours ago

Give name and select VPC that I have created then click on create route table

Create route table **Info**

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.

VPC
The VPC to use for this route table.

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key **Value** - *optional*
You can add 49 more tags.

Now its created New Route Table named as RouteTableA

The screenshot shows the AWS VPC Route Tables page. A success message at the top states: "Route table rtb-0951dcb45885efdcc | RouteTableA was created successfully." Below this, the title "rtb-0951dcb45885efdcc / RouteTableA" is displayed. The left sidebar shows navigation options like VPC dashboard, EC2 Global View, and Virtual private cloud (Route tables selected). The main content area has tabs for Details, Routes, Subnet associations, Edge associations, Route propagation, and Tags. Under the Details tab, it shows the Route table ID (rtb-0951dcb45885efdcc), Main (No), Owner ID (vpc-0fada53abedf1fe48 | my-vpc-01), and Explicit subnet associations and Edge associations (both listed as "-"). The Routes tab displays one route: Destination 10.0.0.0/16, Target local, Status Active, and Propagated No. There are buttons for Both, Edit routes, and a search bar.

Create another routetable for private subnet

The screenshot shows the "Create route table" wizard. It starts with the "Route table settings" step, where the name "RouteTableB" is entered. In the "VPC" section, the VPC "my-vpc-01" is selected. The next step is the "Tags" section, which allows adding tags. A tag "Name" with value "RouteTableB" is added. The "Create route table" button is highlighted with a red box. A success message at the bottom right says: "Route table RouteTableB was created successfully." The URL in the address bar is "ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateRouteTable".

Now its created New Route Tab named as RouteTableB

The screenshot shows the AWS VPC console with the URL ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0f72c8397e324fd23. A success message at the top states "Route table rtb-0f72c8397e324fd23 | RouteTableB was created successfully." The main page displays the details of the newly created route table "rtb-0f72c8397e324fd23 / RouteTableB". The "Routes" tab is selected, showing one route entry: Destination 10.0.0.16, Target local, Status Active, and Propagated No. The left sidebar shows the VPC dashboard and various cloud services like EC2 Global View, Subnets, Route tables, Internet gateways, etc.

Click on RouteTable1

The screenshot shows the AWS VPC console with the URL ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTables. The "Route tables (1/4)" section lists four route tables: RouteTableA (selected), RouteTableB, rtb-0b9e690c3a6001fe1, and rtb-0135143a502c82967. RouteTableA has a Main status of No and is associated with VPC vpc-0fada53abedf1fe48 | my-vpc-01. Below this, the details for RouteTableA are shown, including its ID, Main status (No), and VPC association.

There are no Subnets in RouteTableA as of newly created

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0951dcba5885efdcc

VPC > Route tables > rtb-0951dcba5885efdcc

rtb-0951dcba5885efdcc / RouteTableA

Details

Route table ID	rtb-0951dcba5885efdcc	Main	No	Explicit subnet associations	-	Edge associations	-
VPC	vpc-0fada53abed1fe48 my-vpc-01	Owner ID	396608771079				

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (0)

No subnet associations
You do not have any subnet associations.

Edit subnet associations

Subnets without explicit associations (4)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Edit subnet associations

Add public subnet A and public subnet B to the RouteTableA

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-0951dcba5885efdcc

VPC > Route tables > rtb-0951dcba5885efdcc > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
private-subnet-B	subnet-08e76e011f48dbbf	10.0.48.0/20	-	Main (rtb-0b9e690c3a6001fe1)
<input checked="" type="checkbox"/> public-subnet-A	subnet-012b871ec3a0c5341	10.0.0.0/20	-	Main (rtb-0b9e690c3a6001fe1)
private-subnet-A	subnet-09fe98352e83b73db	10.0.32.0/20	-	Main (rtb-0b9e690c3a6001fe1)
<input checked="" type="checkbox"/> public-subnet-B	subnet-0744e6215266c2022	10.0.16.0/20	-	Main (rtb-0b9e690c3a6001fe1)

Selected subnets

subnet-012b871ec3a0c5341 / public-subnet-A X subnet-0744e6215266c2022 / public-subnet-B X

Save associations

Now public-subnet-A and public-subnet-B will detach with main route and attach with RouteTableA

You have successfully updated subnet associations for rtb-0951dcba5885efcc / RouteTableA.

rtb-0951dcba5885efcc / RouteTableA

Details **info**

Route table ID rtb-0951dcba5885efcc	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-0fada53abedf1fe48 my-vpc-01	Owner ID 396608771079		

Routes **Subnet associations** **Edge associations** **Route propagation** **Tags**

Explicit subnet associations (2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
public-subnet-A	subnet-012b871ec3a0c5341	10.0.0.0/20	-
public-subnet-B	subnet-0744e6215266c2022	10.0.16.0/20	-

Similarly RouteTableB

Now private-subnet-A and private-subnet-B will detach with main route and attach with RouteTableB

Route tables (1/4) Info

Name	Route table ID	Explicit subnet associa...	Main	VPC
-	rtb-0b9e690c3a6001fe1	-	Yes	vpc-0fada53abedf1fe48 my-vpc-01
-	rtb-0135143a502c82967	-	Yes	vpc-04a1fb36c899c76be
RouteTableA	rtb-0951dcba5885efcc	2 subnets	No	vpc-0fada53abedf1fe48 my-vpc-01
RouteTableB	rtb-0f72c8397e324fd23	-	No	vpc-0fada53abedf1fe48 my-vpc-01

rtb-0f72c8397e324fd23 / RouteTableB

Details **info**

Route table ID rtb-0f72c8397e324fd23	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0fada53abedf1fe48 my-vpc-01	Owner ID 396608771079		

Routes **Subnet associations** **Edge associations** **Route propagation** **Tags**

Explicit subnet associations (0)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
------	-----------	-----------	-----------

No subnet associations
You do not have any subnet associations.

Now add private-subnet-B, private-subnet-A to the RouteTableB

[ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-0f72c8397e324fd23](#)

VPC > Route tables > rtb-0f72c8397e324fd23 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)				
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
private-subnet-B	subnet-08e76e011f48dbbef	10.0.48.0/20	-	Main (rtb-0b9e690c3a6001fe1)
public-subnet-A	subnet-012b871ec3a0c5341	10.0.0.0/20	-	rtb-0951dcb45885efdcc / RouteTableA
private-subnet-A	subnet-09fe98352e83b73db	10.0.32.0/20	-	Main (rtb-0b9e690c3a6001fe1)
public-subnet-B	subnet-0744e6215266c2022	10.0.16.0/20	-	rtb-0951dcb45885efdcc / RouteTableA

Selected subnets

- subnet-09fe98352e83b73db / private-subnet-A
- subnet-08e76e011f48dbbef / private-subnet-B

[Cancel](#) [Save associations](#)

[ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0f72c8397e324fd23](#)

VPC dashboard < VPC > Route tables > rtb-0f72c8397e324fd23

rtb-0f72c8397e324fd23 / RouteTableB

Details [Info](#)

Route table ID rtb-0f72c8397e324fd23	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-0fada53abedf1fe48 my-vpc-01	Owner ID 396608771079		

[Actions](#)

Subnet associations

Explicit subnet associations (2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
private-subnet-B	subnet-08e76e011f48dbbef	10.0.48.0/20	-
private-subnet-A	subnet-09fe98352e83b73db	10.0.32.0/20	-

[Edit subnet associations](#)

When we create route table and associate with the custom vpc bu default it doesn't have access to the internet unless we add route to the internet gateway

Go to RouteTableA

[ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0951dcb45885efdcc](#)

VPC dashboard < VPC > Route tables > rtb-0951dcb45885efdcc

rtb-0951dcb45885efdcc / RouteTableA

Details [Info](#)

Route table ID rtb-0951dcb45885efdcc	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-0fada53abedf1fe48 my-vpc-01	Owner ID 396608771079		

[Actions](#)

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Choose 0.0.0.0/0 means all the ips applicable at destination and choose target as Internet Gateway and then click on save changes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	-	No

Edit routes

Save changes

Now RouteTableA has internet gateway has route to internet via internet gateway

Destination	Target	Status	Propagated
0.0.0.0/0	igw-09b1b1fe32b3aea7f	Active	No
10.0.0.0/16	local	Active	No

Actions

Security Groups

- A security group acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic.
- Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance.
- If you don't specify a security group, Amazon EC2 uses the default security group.
- By default, security groups allow all outbound traffic.
- Security groups are stateful-if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules.
- You can associate more than one security group with an instance.

Security group - Rules

Amazon EC2 blocks traffic on port 25 by default.

Security group rules are always permissive; you can't create rules that deny access.

You can add and remove rules at any time. Your changes are automatically applied to the instances that are associated with the security group.

Specify below at the time of rule creation:

Name

Protocol

Port Range

Type

Source: Custom/AnyWhere/MyIP

Source Value: CIDR Block, Security Group

EC2 one for public subnet -> for webserver

EC2 one for private subnet -> for database server

Go to EC2 instance

Launch Instance

The screenshot shows the AWS EC2 Instances page. The left sidebar is titled 'EC2' and includes 'Dashboard', 'EC2 Global View', 'Events', 'Instances' (which is expanded), 'Instance Types', 'Launch Templates', and 'Spot Requests'. The main content area is titled 'Instances Info' and shows a search bar with 'Find Instance by attribute or tag (case-sensitive)'. Below the search bar are filters for 'Name' and 'Instance ID', and dropdowns for 'Instance state', 'Instance type', 'Status check', 'Alarm status', 'Availability Zone', and 'Public IP'. A message 'No instances' and 'You do not have any instances in this region' is displayed. A blue 'Launch instances' button is located at the bottom right of the main area.

The screenshot shows the 'Launch an instance' wizard. The top navigation bar includes 'Instances' and 'Launch an instance'. The main steps are: 'Name and tags' (with a 'Name' field containing 'ec2-public' and a 'Add additional tags' link), 'Application and OS Images (Amazon Machine Image)' (with a search bar and a list of AMIs including Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian), 'Quick Start' (with a grid of AMI icons), and 'Summary' (which lists 'Number of instances' (1), 'Software Image (AMI)' (Canonical, Ubuntu, 24.04, amd64), 'Virtual server type (instance type)' (t2.micro), 'Firewall (security group)' (New security group), 'Storage (volumes)' (1 volume(s) - 8 GiB), and a note about the 'Free tier'). At the bottom are 'Cancel', 'Launch instance' (in a large orange button), and a 'Preview code' link.

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture
64-bit (x86)

AMI ID
ami-00bb6a80f01f03502

Publish Date
2025-01-15

Username
ubuntu

Verified provider

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

Free tier eligible

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

Create key pair



Key pair name

Key pairs allow you to connect to your instance securely.

ec2-public

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA

RSA encrypted private and public key pair

ED25519

ED25519 encrypted private and public key pair

Private key file format

.pem

For use with OpenSSH

.ppk

For use with PuTTY

⚠️ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

[Cancel](#)

[Create key pair](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

ec2-public

[Create new key pair](#)

▼ Network settings [Info](#)

VPC - required | [Info](#)

vpc-0fada53abedf1fe48 (my-vpc-01)
10.0.0.0/16



Subnet | [Info](#)

subnet-012b871ec3a0c5341 public-subnet-A
VPC: vpc-0fada53abedf1fe48 Owner: 396608771079 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 4091 CIDR: 10.0.0.0/20



[Create new subnet](#)

Auto-assign public IP | [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - required

pub-ssh-http

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#@[]+=&;!\$^

Description - required | [Info](#)

launch-wizard-1 created 2025-03-14T13:28:55.152Z

Inbound Security Group Rules

- ▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type Info ssh	Protocol Info TCP	Port range Info 22	Remove
Source type Info Custom	Source Info Add CIDR, prefix list or security group 0.0.0.0/0 X	Description - optional Info e.g. SSH for admin desktop	

- ▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)

Type Info HTTP	Protocol Info TCP	Port range Info 80	Remove
Source type Info Custom	Source Info Add CIDR, prefix list or security group 0.0.0.0/0 X	Description - optional Info e.g. SSH for admin desktop	

The screenshot shows the AWS EC2 'Launch instance' wizard. In the 'Advanced network configuration' section, there is a note for free-tier eligible customers about EBS General Purpose (SSD) or Magnetic storage. In the 'Configure storage' section, a 1x 8 GiB gp3 volume is selected as the root volume. The 'Software Image (AMI)' is set to Canonical, Ubuntu, 24.04, amd64. The 'Virtual server type (instance type)' is t2.micro. The 'Firewall (security group)' is set to 'New security group'. Under 'Storage (volumes)', it shows 1 volume(s) - 8 GiB. A note about free tier instance store volumes is displayed. At the bottom right, there are 'Cancel', 'Launch instance', and 'Preview code' buttons.

Launch 2nd ec2 instance as database server

The screenshot shows the AWS EC2 Instances page. The left sidebar shows 'EC2' selected under 'Instances'. The main area displays 'Instances (1)' with a table showing one instance: 'ec2-public' (Instance ID: i-07426f92f7c3f38dc, Status: Running, Type: t2.micro). A search bar at the top allows filtering by instance ID, name, and tags. A 'Launch instances' button is visible at the top right. The URL in the browser is ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:instanceId=i-07426f92f7c3f38dc.

← → ⌂ ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

aws | Search [Alt+S]

≡ EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

ec2-private

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents

Quick Start



Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

← → ⌂ ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

aws | Search [Alt+S]

≡ EC2 > Instances > Launch an instance

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-00bb6a80f01f03502 (64-bit (x86)) / ami-09773b29dffbe1f2 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture

AMI ID

Publish Date

Username



ubuntu

Verified provider

▼ Instance type Info | Get advice

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.0171 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

Free tier eligible

All generations

Compare instance types

Create key pair

X

Key pair name

Key pairs allow you to connect to your instance securely.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

 RSA

RSA encrypted private and public key pair

 ED25519

ED25519 encrypted private and public key pair

Private key file format

 .pem

For use with OpenSSH

 .ppk

For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more ↗](#)

Cancel

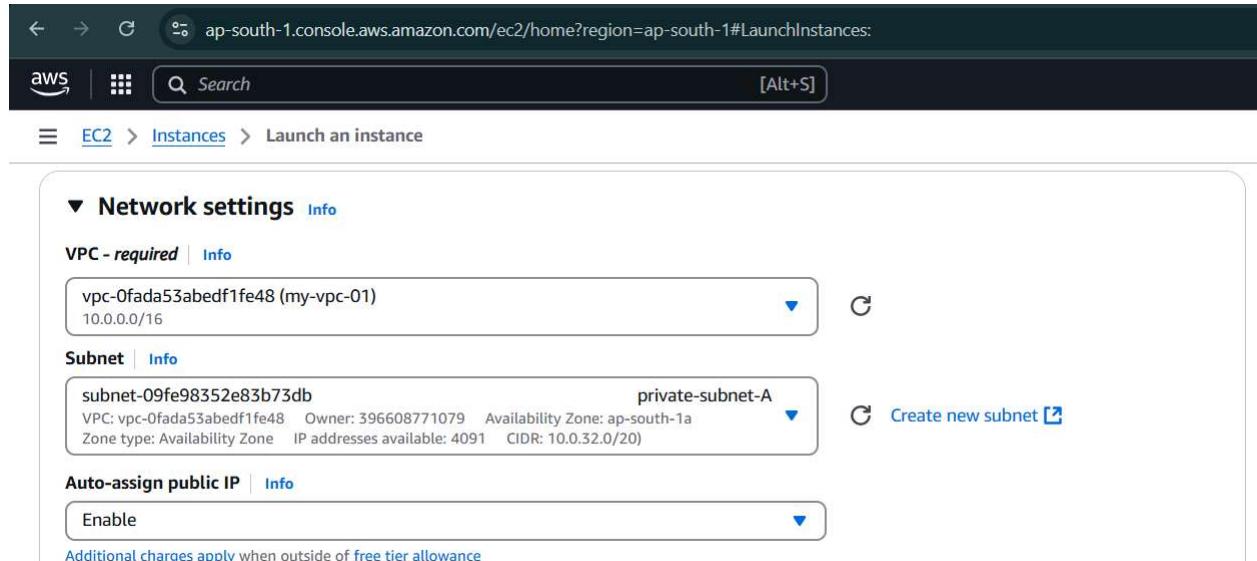
Create key pair

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

 [Create new key pair](#)



← → ⌂ ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

aws | Search [Alt+S]

☰ EC2 > Instances > Launch an instance

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0fada53abedf1fe48 (my-vpc-01)
10.0.0.0/16

Subnet [Info](#)

subnet-09fe98352e83b73db private-subnet-A
VPC: vpc-0fada53abedf1fe48 Owner: 396608771079 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 4091 CIDR: 10.0.32.0/20

 [Create new subnet ↗](#)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - required

private-sg-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#@[]+=&;{}!\$*

Description - required | Info

launch-wizard-1 created 2025-03-14T13:36:55.877Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, sg-0757e55565b9f6ca4)

Remove

Type | Info

ssh

Protocol | Info

TCP

Port range | Info

22

Source type | Info

Custom

Source | Info

Add CIDR, prefix list or security group

Description - optional | Info

e.g. SSH for admin desktop

sg-0757e55565b9f6ca4 X

▼ Security group rule 2 (TCP, 3306, sg-0757e55565b9f6ca4)

Remove

Type | Info

MYSQL/Aurora

Protocol | Info

TCP

Port range | Info

3306

Source type | Info

Custom

Source | Info

Add CIDR, prefix list or security group

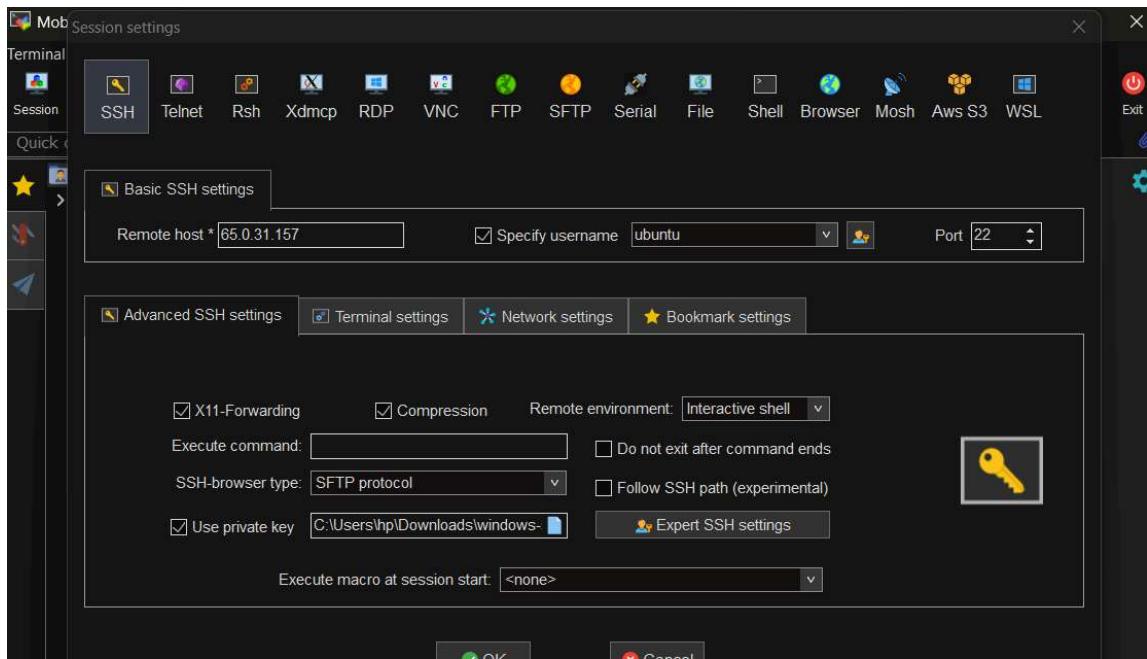
Description - optional | Info

e.g. SSH for admin desktop

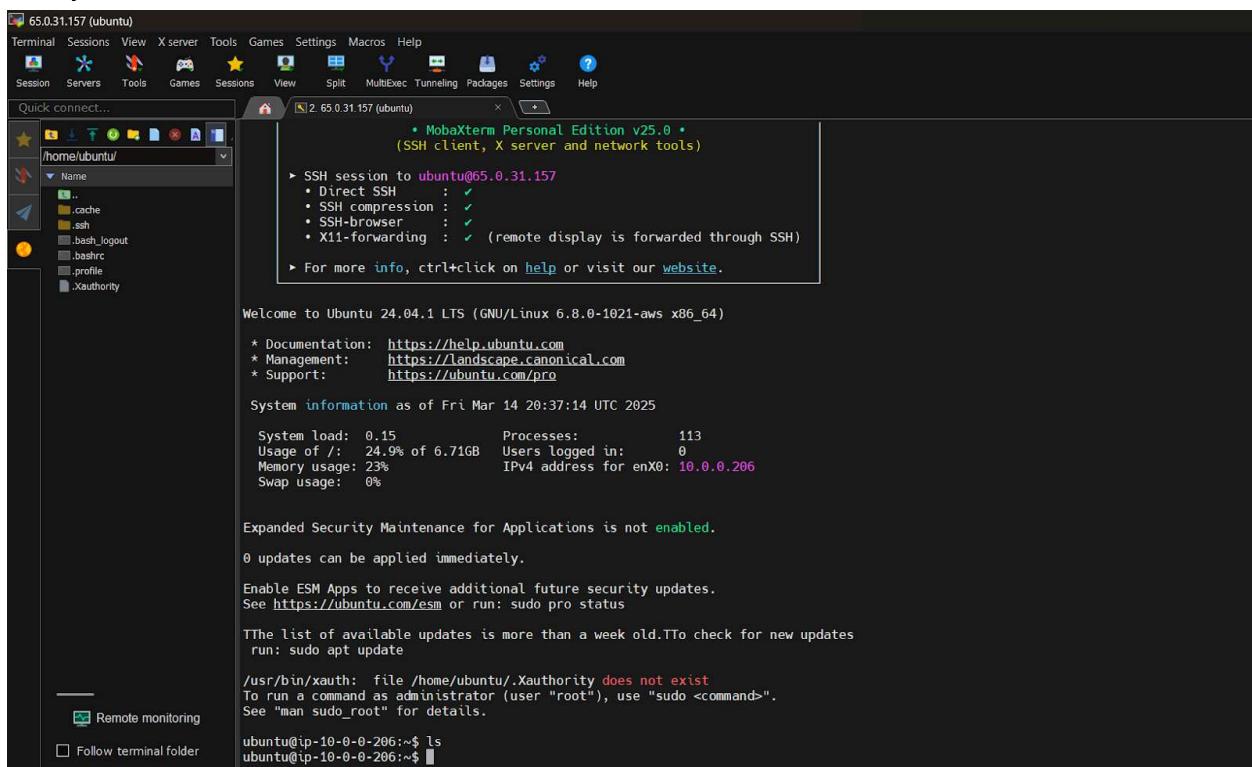
sg-0757e55565b9f6ca4 X

The screenshot shows the AWS EC2 Launch Instances wizard. On the left, under 'Configure storage', a 1x 8 GiB gp3 volume is selected as the root volume. A note indicates that free-tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Below this, there's a note about instance store volumes and a link to refresh backup information. On the right, the 'Summary' section shows 1 instance being launched, using a Canonical, Ubuntu, 24.04 AMI, and a t2.micro instance type. It also lists a new security group named 'New security group' and a single 8 GiB volume. A note about the free tier is present, along with 'Launch instance' and 'Preview code' buttons.

Go to ec2-public and copy Public IPv4 take it as host , give user name as ubuntu and also take key pair past in path give it inthe MobaXtrem



Now you can access the ec2 instance of webserver in MobaXtrem



Go to ec2-private and copy Public IPv4 take it as host , give user name as ubuntu and also take key pair past in path give it in MobaXtrem

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with options like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, and Elastic Block Store. The main area displays 'Instances (1/3) Info' with a search bar and filters. A table lists three instances:

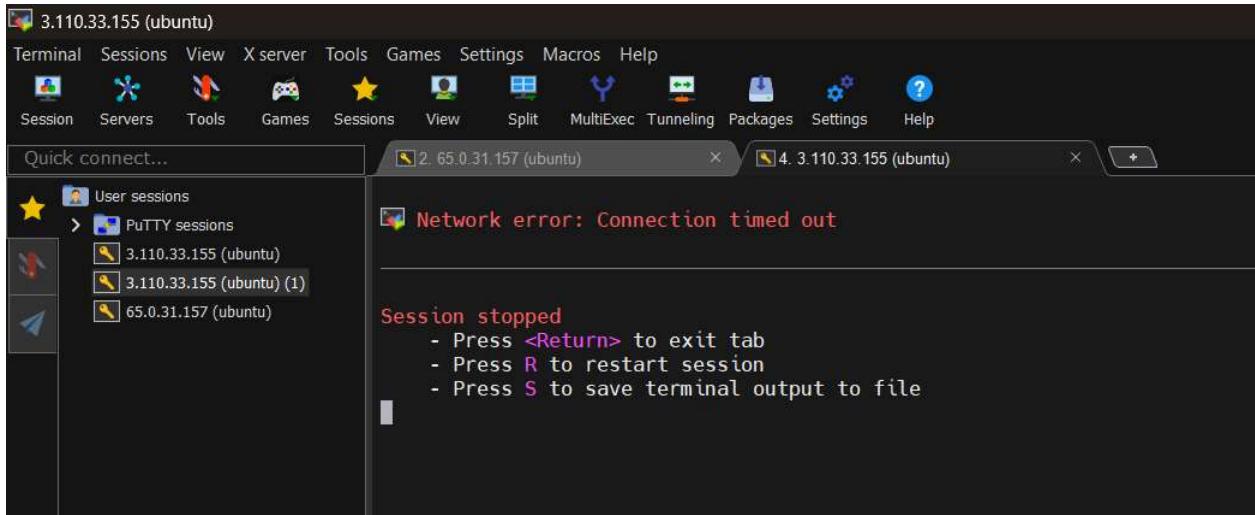
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/>	ec2-private	i-07443f494dcf14487	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	ec2-3-110-33-155.ap-south-1.compute.amazonaws.com
<input type="checkbox"/>	ec2-public	i-06ecf8ebe9b7c73b1	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	ec2-65-0-10.40.189
<input type="checkbox"/>	instance3	i-0addc2ef2a9326c3a	Terminated	t2.micro	-	View alarms +	ap-south-1a	-

Below the table, a detailed view for the ec2-private instance is shown. It includes tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. Under the Details tab, the Public IPv4 address (3.110.33.155) is highlighted with a red box.

The screenshot shows the MobaXterm Session settings window. At the top, there are icons for various connection types: SSH, Telnet, Rsh, Xdmcp, RDP, VNC, FTP, SFTP, Serial, File, Shell, Browser, Mosh, Aws S3, and WSL. The SSH icon is selected.

The main configuration area has tabs for Basic SSH settings and Advanced SSH settings. In the Basic SSH settings tab, the 'Remote host' field is set to '3.110.33.155', 'Specify username' is set to 'ubuntu', and the 'Port' is set to '22'. In the Advanced SSH settings tab, there are checkboxes for 'X11-Forwarding', 'Compression', 'Execute command' (empty field), 'SSH-browser type' (set to 'SFTP protocol'), 'Use private key' (checkbox checked with path 'C:\Users\hp\Downloads\privateKey'), and 'Expert SSH settings' (button). There are also checkboxes for 'Do not exit after command ends' and 'Follow SSH path (experimental)'.

It cant connect as its private network and didnt initiate ssh access to this server



Note :

In Security Groups we can have inbound and outbound rules for the allowed traffic and we don't have any inbound and outbound rule that denies traffic ,whereas NACL have inbound and outbound rules for the allowed and denies traffic

NAT GATEWAY

Gateway is a better alternative of Nat instance

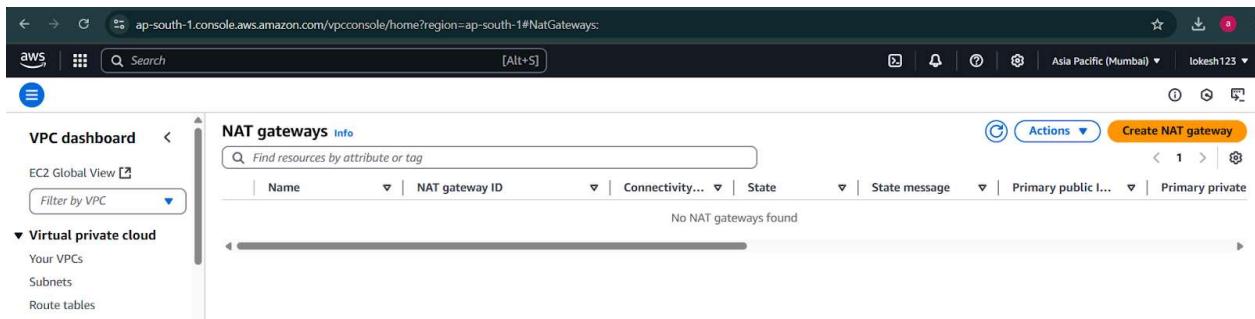
Managed service by AWS, high availability, higher bandwidth, auto-scaling

No security groups to manage

No infra management/server patching is required

1 NAT Gateway can span over 1 AZ for auto-failover

Click on create Nat Gatway



Give name, choose public subnet, Allocate Elastic IP and then click on create NAT gateway

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateNatGateway:

VPC > NAT gateways > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

Connectivity type
Select a connectivity type for the NAT gateway.
 Public
 Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
 Allocate Elastic IP

Additional settings Info

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - <small>optional</small>
<input type="text" value="Name"/>	<input type="text" value="nat-gateway-01"/> <button>Remove</button>

Add new tag
You can add 49 more tags.

Cancel **Create NAT gateway**

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#NatGatewayDetails:natGatewayId=nat-08a9449733236bb30

VPC > NAT gateways > nat-08a9449733236bb30

NAT gateway nat-08a9449733236bb30 | nat-gateway-01 was created successfully.

nat-08a9449733236bb30 / nat-gateway-01

Actions

Details

NAT gateway ID <input type="text" value="nat-08a9449733236bb30"/>	Connectivity type Public	State <small>Pending</small>	State message <small>Info</small> -
NAT gateway ARN <input type="text" value="arn:aws:ec2:ap-south-1:396608771079:natgateway/nat-08a9449733236bb30"/>	Primary public IPv4 address -	Primary private IPv4 address -	Primary network interface ID -
VPC <input type="text" value="vpc-0fada53abedf1fe48 / my-vpc-01"/>	Subnet <input type="text" value="subnet-012b871ec3a0c5341 / public-subnet-A"/>	Created <small>Saturday, March 15, 2025 at 02:54:23 GMT+5:30</small>	Deleted -

Secondary IPv4 addresses Monitoring Tags

Secondary IPv4 addresses

Private IPv4 address	Network interface ID	Status	Failure message
Secondary IPv4 addresses are not available for this nat gateway.			

PART 3

Automated Intrusion Detection & Response (IDR):

1. Deploy **Suricata or Snort for network traffic anomaly detection.**

Snort Installation and setup

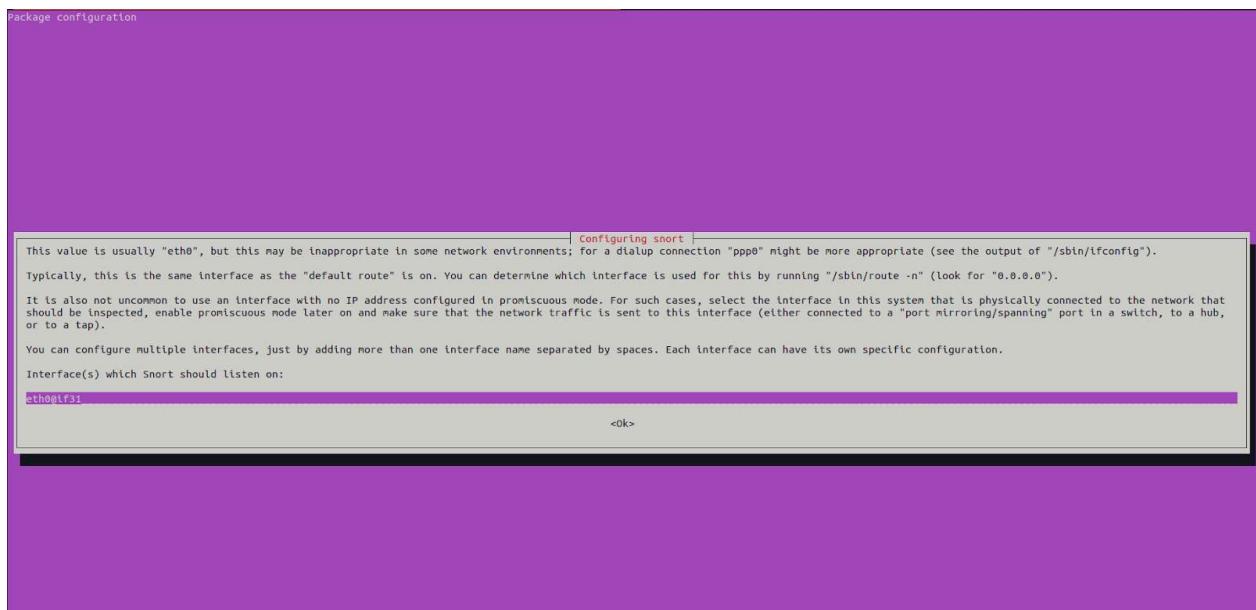
Update all the apt packages

```
lokesh@agent1:~$ sudo apt-get update
[sudo] password for lokesh:
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
```

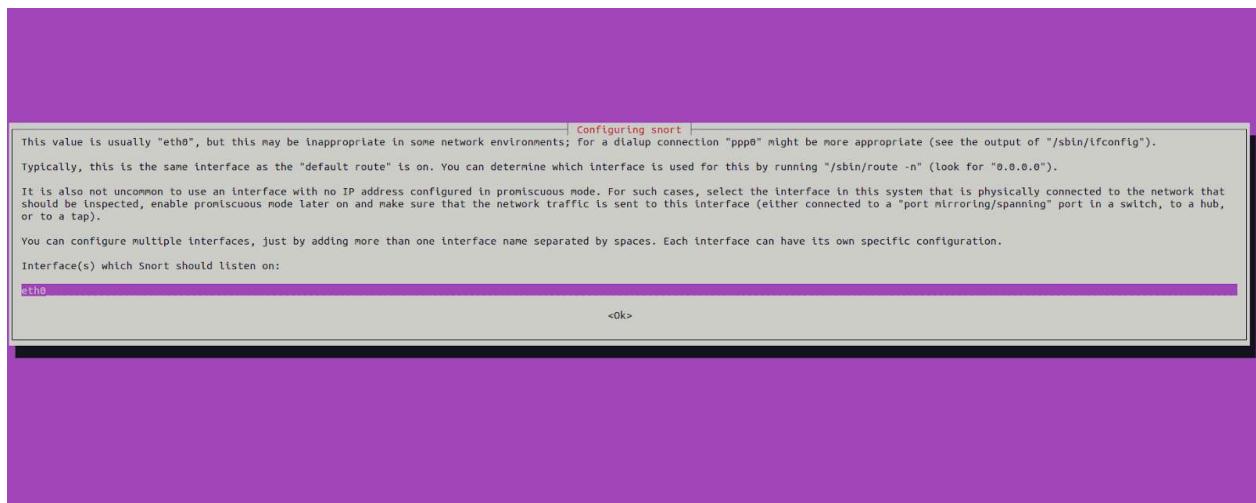
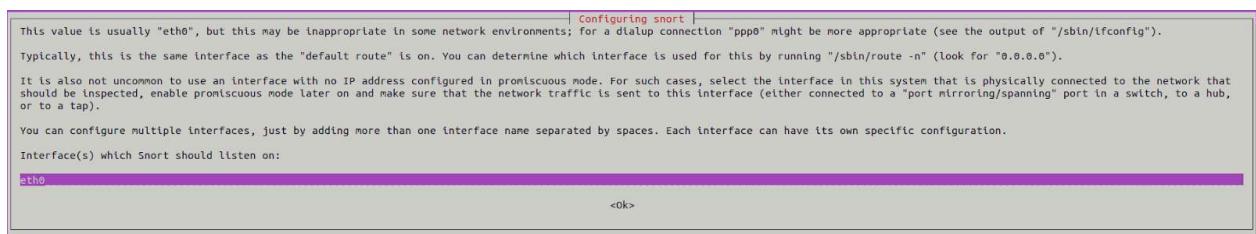
Install Snort

```
lokesh@agent1:~$ sudo apt-get install snort -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libauthen-sasl-perl libclone-perl libdaq2 libdata-dump-perl libdumbnet1
libencode-locale-perl libfile-listing-perl libfont-afm-perl
.
.
.
```

Choose Interface as eth0 for LXD



Give eth0 as interface



```

lokesh@cybercub: $ lxc exec agent1 /bin/bash
root@agent1:~# ip a
1: lo: <LOOPBACK,NOQUEUE,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 state UNKNOWN group default qlen 1000
        link/ether 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
            valid_lft forever preferred_lft forever
            inetnet ::1/128 scope host
                valid_lft forever preferred_lft forever
                valid_lft forever preferred_lft forever
30: eth0@if31: <BRIDGE,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:e0:7b:2 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.18.151.53/24 brd 10.18.151.255 metric 100
        linklayer brd ff:ff:ff:ff:ff:ff
        valid_lft forever preferred_lft forever
        inet net fe80::216:3eff:feee:7b2/64 scope link
            valid_lft forever preferred_lft forever
            inet net fe80::216:3eff:feee:7b2/64 scope link
                valid_lft forever preferred_lft forever

```

To determine which version of the Snort is installed, type the following command:

```
lokesh@agent1:~$ snort -V
```

```

,,_ -*> Snort! <*-
o" )~ Version 2.9.15.1 GRE (Build 15125)
"" By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.10.1 (with TPACKET_V3)
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11

```

List /etc/snort

```
lokesh@agent1:~$ ls -la /etc/snort/
total 368
drwxr-xr-x 3 root root 4096 Nov 15 19:36 .
drwxr-xr-x 90 root root 4096 Nov 15 06:48 ..
-rw-r--r-- 1 root root 1281 Dec 3 2019 attribute_table.dtd
-rw-r--r-- 1 root root 3757 Dec 3 2019 classification.config
-rw-r--r-- 1 root root 82469 Dec 3 2021 community-sid-msg.map
-rw-r--r-- 1 root root 23657 Dec 3 2019 file_magic.conf
-rw-r--r-- 1 root root 32789 Dec 3 2019 gen-msg.map
-rw-r--r-- 1 root root 687 Dec 3 2019 reference.config
drwxr-xr-x 2 root root 4096 Nov 15 06:46 rules
-rw-r----- 1 root snort 29775 Dec 3 2021 snort.conf
-rw----- 1 root root 806 Nov 15 19:36 snort.debian.conf
-rw-r--r-- 1 root root 2335 Dec 3 2019 threshold.conf
-rw-r--r-- 1 root root 160606 Dec 3 2019 unicode.map
```

Edit /etc/snort/snort.conf

```
lokesh@agent1:~$ sudo nano /etc/snort/snort.conf
ipvar HOME_NET 192.168.122.141/32
//ipvar HOME_NET [10.189.151.13,10.189.151.97,10.189.151.161]
var RULE_PATH /etc/snort/rules
include $RULE_PATH/local.rules
#pcap
output log_tcpdump: /var/log/snort/tcpdump.log
#csv
output alert_csv: /var/log/snort/alert.csv default
# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
#include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
#include $RULE_PATH/ddos.rules
#include $RULE_PATH/dns.rules
#include $RULE_PATH/dos.rules
#include $RULE_PATH/experimental.rules
```

Test all the configuration changes right or wrong

```
lokesh@agent1:~$ sudo snort -T -i eth0 -c /etc/snort/snort.conf
Running in Test mode
```

==== Initializing Snort ===-

```
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
```

```
.
.
.
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
```

Snort successfully validated the configuration!

Snort exiting

Create custome rules for snort

```
lokesh@agent1:~$ sudo nano /etc/snort/rules/local.rules
alert icmp any any -> $HOME_NET any (msg:"ICMP Detection Rule"; sid:100001;)
alert tcp any any -> $HOME_NET 22 (msg: "SSH Connection Attempts"; sid:100002; )
alert tcp any any -> $HOME_NET 80 (msg:"Command Execution Attempt"; content:"GET";
content:"/etc/passwd"; sid:100003; )
```

Testing Snort Rules

Firstly; we will send ICMP Ping packets from the Attacker Machine which has IP address 192.168.189.128 to the Ubuntu Machine.

Secondly; we will make an SSH connection attempt from the Attacker Machine to the Ubuntu Machine.

Thirdly; we will send a command execution request with the curl from the Attacker Machine to the Ubuntu Machine.

Snort will also write alerts to the CSV file and PCAP file because we configured We can use these files to investigate attacks later. We can reach this file in the /var/log/snort directory.

```
lokesh@cybercub:~$ ping 10.189.151.53
PING 10.189.151.53 (10.189.151.53) 56(84) bytes of data.
64 bytes from 10.189.151.53: icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from 10.189.151.53: icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from 10.189.151.53: icmp_seq=3 ttl=64 time=0.050 ms
64 bytes from 10.189.151.53: icmp_seq=4 ttl=64 time=0.072 ms
```

Check logs in Agent1

```
root@agent1:~# sudo snort -q -l /var/log/snort -i eth0 -A console -c /etc/snort/snort.conf
11/18-19:10:58.251654 [**] [1:100001:0] "ICMP Detection Rule" [**] [Priority: 0] {ICMP}
10.189.151.1 -> 10.189.151.53
11/18-19:10:59.276037 [**] [1:100001:0] "ICMP Detection Rule" [**] [Priority: 0] {ICMP}
10.189.151.1 -> 10.189.151.53
11/18-19:11:00.300047 [**] [1:100001:0] "ICMP Detection Rule" [**] [Priority: 0] {ICMP}
```

2. Configure fail2ban to block repeated SSH & web attacks automatically.

WHAT IS FAIL2BAN?

- 01 Helps prevent brute-force attacks
- 02 Watches logs for authentication failure
- 03 Creates firewall rules to block IP addresses
- 04 Able to protect multiple services
- 05 Completely customizable

```
root@fail2ban:~# apt update
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [3433 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
.
.
.
```

```
root@fail2ban:~# apt install fail2ban -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify whois
0 upgraded, 3 newly installed, 0 to remove and 52 not upgraded.
Need to get 444 kB of archives.
After this operation, 2400 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 fail2ban all 0.11.1-1 [375 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-pyinotify all 0.9.6-1.2ubuntu1
[24.8 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/main amd64 whois amd64 5.5.6 [44.7 kB]
```

```
root@fail2ban:~# systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
```

```
root@fail2ban:~# ls -al /etc/fail2ban/
total 72
drwxr-xr-x  6 root root  4096 Mar 14 22:53 .
drwxr-xr-x  96 root root  4096 Mar 14 22:53 ..
drwxr-xr-x  2 root root  4096 Mar 14 22:53 action.d
-rw-r--r--  1 root root  2817 Jan 11  2020 fail2ban.conf
drwxr-xr-x  2 root root  4096 Mar  2  2020 fail2ban.d
drwxr-xr-x  3 root root  4096 Mar 14 22:53 filter.d
-rw-r--r--  1 root root 25740 Jan 11  2020 jail.conf
drwxr-xr-x  2 root root  4096 Mar 14 22:53 jail.d
-rw-r--r--  1 root root   645 Jan 11  2020 paths-arch.conf
-rw-r--r--  1 root root 2827 Jan 11  2020 paths-common.conf
-rw-r--r--  1 root root   573 Jan 11  2020 paths-debian.conf
-rw-r--r--  1 root root   738 Jan 11  2020 paths-opensuse.conf
```

Jail is a configuration file that contains filters and arguments that protect system or a particular service

```
root@fail2ban:~# less /etc/fail2ban/jail.conf
```

```
.
```

```
root@fail2ban:~# nano /etc/fail2ban/jail.local
```

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 3600
ignoreip = 127.0.0.1 //this is for whitelisting ip
```

```
root@fail2ban:~# systemctl restart fail2ban
```

```
root@fail2ban:~# systemctl status fail2ban
```

- fail2ban.service - Fail2Ban Service

```
    Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor pres>
```

```
    Active: active (running) since Sat 2025-03-15 00:10:01 UTC; 8s ago
```

```
      Docs: man:fail2ban(1)
```

```
    Process: 1455 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status>
```

```
    Main PID: 1456 (f2b/server)
```

```
      Tasks: 5 (limit: 18795)
```

```
      Memory: 11.0M
```

```
      CPU: 97ms
```

```
    CGroup: /system.slice/fail2ban.service
```

```
        └─1456 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```

```
Mar 15 00:10:01 fail2ban systemd[1]: Starting Fail2Ban Service...
```

```
Mar 15 00:10:01 fail2ban systemd[1]: Started Fail2Ban Service.
```

```
Mar 15 00:10:01 fail2ban fail2ban-server[1456]: Server ready
```

```
SSH jail got activated
root@fail2ban:~# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:          sshd
```

```
From another machine trying brute ssh
root@sensor1:~# hydra -l root -P /wordlists/rockyou.txt ssh://10.189.151.97 -l -v
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-15 02:48:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
reduce the tasks: use -t 4
[ERROR] File for passwords not found: /wordlists/rockyou.txt
```

```
On the machine where fail2ban hosted it worked as ssh login failed over brute force
root@fail2ban:~# cat /var/log/auth.log
Mar 14 22:47:38 sensor4 sshd[219]: Server listening on 0.0.0.0 port 22.
Mar 14 22:47:38 sensor4 sshd[219]: Server listening on :: port 22.
Mar 14 22:47:38 sensor4 systemd-logind[173]: New seat seat0.
Mar 14 22:49:53 fail2ban sshd[218]: Server listening on 0.0.0.0 port 22.
Mar 14 22:49:53 fail2ban sshd[218]: Server listening on :: port 22.
Mar 14 22:49:53 fail2ban systemd-logind[201]: New seat seat0.
Mar 14 22:50:26 fail2ban sshd[221]: Server listening on 0.0.0.0 port 22.
Mar 14 22:50:26 fail2ban sshd[221]: Server listening on :: port 22.
Mar 14 22:50:26 fail2ban systemd-logind[202]: New seat seat0.
Mar 14 23:06:01 fail2ban CRON[1315]: pam_unix(cron:session): session opened for user root
by (uid=0)
Mar 14 23:06:01 fail2ban CRON[1315]: pam_unix(cron:session): session closed for user root
Mar 14 23:17:01 fail2ban CRON[1320]: pam_unix(cron:session): session opened for user root
by (uid=0)
Mar 14 23:17:01 fail2ban CRON[1320]: pam_unix(cron:session): session closed for user root
Mar 15 00:12:33 fail2ban sshd[1468]: Connection closed by authenticating user root
10.189.151.79 port 54714 [preauth]
Mar 15 00:12:59 fail2ban sshd[1470]: Connection closed by authenticating user root
10.189.151.79 port 36770 [preauth]
Mar 15 00:13:29 fail2ban sshd[1472]: Connection closed by authenticating user root
10.189.151.79 port 50430 [preauth]
Mar 15 00:16:42 fail2ban sshd[1478]: Connection closed by authenticating user root
10.189.151.1 port 55416 [preauth]
Mar 15 00:17:01 fail2ban CRON[1480]: pam_unix(cron:session): session opened for user root
by (uid=0)
Mar 15 00:17:01 fail2ban CRON[1480]: pam_unix(cron:session): session closed for user root
```

Mar 15 02:30:41 fail2ban sshd[221]: Received signal 15; terminating.
Mar 15 02:30:41 fail2ban sshd[1535]: Server listening on 0.0.0.0 port 22.
Mar 15 02:30:41 fail2ban sshd[1535]: Server listening on :: port 22.
Mar 15 02:30:48 fail2ban sshd[1535]: Received signal 15; terminating.
Mar 15 02:30:48 fail2ban sshd[1539]: Server listening on 0.0.0.0 port 22.
Mar 15 02:30:48 fail2ban sshd[1539]: Server listening on :: port 22.
Mar 15 02:31:06 fail2ban sshd[1540]: Connection closed by authenticating user root
10.189.151.79 port 44738 [preauth]
Mar 15 02:31:14 fail2ban sshd[1542]: Connection closed by authenticating user root
10.189.151.79 port 32808 [preauth]
Mar 15 02:32:13 fail2ban sshd[1546]: Connection closed by authenticating user root
10.189.151.79 port 46542 [preauth]
Mar 15 02:56:51 fail2ban sshd[1568]: Connection closed by authenticating user root
10.189.151.1 port 38304 [preauth]
Mar 15 02:56:55 fail2ban sshd[1570]: Connection closed by authenticating user root
10.189.151.1 port 38308 [preauth]

SIEM & Log Aggregation

1. Centralize logs with **ELK Stack (Elasticsearch, Logstash, Kibana)**

Before installation of ELK do set up for dependencies required :

Check ubuntu version you are using

```
root@elk:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.6 LTS
Release:        20.04
Codename:       focal
```

Install java dependencies

Check java version

```
root@elk:~# javac -version  
javac 11.0.26
```

Make sure that curl installed if not then install curl

```
root@elk:~# sudo apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
curl is already the newest version (7.68.0-1ubuntu2.25).
curl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 29 not upgraded.
```

Add the elasticsearch APT repository key by using the below command (run these commands Root

```
root@elk:~# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -  
OK
```

Add the Elastic Search to the APT source List by using the below command

```
root@elk:~# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" >  
/etc/apt/sources.list.d/elastic-7.x.list
```

Installation of Elastic search:

```
root@elk:~# apt update  
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]  
Get:2 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [143 kB]  
Get:3 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]  
Hit:4 http://archive.ubuntu.com/ubuntu focal InRelease  
Get:5 http://archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]  
Get:6 http://archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]  
Fetched 540 kB in 2s (320 kB/s)  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
29 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Install elastic search

```
root@elk:~# apt install elasticsearch -y
```

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following NEW packages will be installed:

 elasticsearch

0 upgraded, 1 newly installed, 0 to remove and 29 not upgraded.

Need to get 325 MB of archives.

After this operation, 542 MB of additional disk space will be used.

```
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elasticsearch amd64 7.17
```

Configuration of elasticsearch

```
root@elk:~# nano /etc/elasticsearch/elasticsearch.yml
network.host: '10.189.151.79'
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
discovery.type: single-node
```

```
root@elk:~# nano /etc/elasticsearch/jvm.options
-Xms512m
-Xmx512m
```

Enable Elasticsearch

```
root@elk:~# systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service →
/lib/systemd/system/elasticsearch.service.
```

Start Elasticsearch

```
root@elk:~# systemctl start elasticsearch
```

```
root@elk:~# curl -X GET "10.189.151.79:9200"
{
  "name" : "elk",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "y34ksPnVTziER2z1cq-ycw",
  "version" : {
    "number" : "7.17.28",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "139cb5a961d8de68b8e02c45cc47f5289a3623af",
    "build_date" : "2025-02-20T09:05:31.349013687Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.3",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

```
← → C ⚠ Not secure 10.189.151.79:9200
Pretty print □

{
  "name" : "elk",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "y34ksPnVTziER2z1cq-ycw",
  "version" : {
    "number" : "7.17.28",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "139cb5a961d8de68b8e02c45cc47f5289a3623af",
    "build_date" : "2025-02-20T09:05:31.349013687Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.3",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Logstash setup

Install logstash

```
root@elk:~# apt install logstash -y
```

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following NEW packages will be installed:

 logstash

0 upgraded, 1 newly installed, 0 to remove and 29 not upgraded.

Need to get 375 MB of archives.

After this operation, 632 MB of additional disk space will be used.

```
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash amd64 1:7.17.28-1 [375 MB]
```

Fetched 375 MB in 1min 40s (3738 kB/s)

Selecting previously unselected package logstash.

.

.

OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.

```
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaserun/pl
```

atform/base.rb:112: warning: constant ::Fixnum is deprecated

Successfully created system startup script for Logstash

```
root@elk:~# systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service →
/etc/systemd/system/logstash.service.
root@elk:~# systemctl start logstash
root@elk:~# systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2025-03-15 04:44:44 UTC; 7s ago
     Main PID: 5130 (java)
        Tasks: 25 (limit: 18795)
       Memory: 535.3M
          CPU: 31.473s
         CGroup: /system.slice/logstash.service
             └─5130 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSIn
```

Kibana Set up

```
root@elk:~# apt update
Hit:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
29 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
root@elk:~# apt install kibana -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
```

```
  kibana
0 upgraded, 1 newly installed, 0 to remove and 29 not upgraded.
Need to get 293 MB of archives.
After this operation, 744 MB of additional disk space will be used.
```

```
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.17.28 [293 MB]
```

```
Creating kibana group... OK
root@elk:~# systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service →
/etc/systemd/system/kibana.service.
```

```
root@elk:~# systemctl start kibana
root@elk:~# systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2025-03-15 04:53:07 UTC; 8s ago
     Docs: https://www.elastic.co
 Main PID: 7519 (node)
    Tasks: 11 (limit: 18795)
   Memory: 246.8M
      CPU: 8.224s
     CGroup: /system.slice/kibana.service

```

Before Configuration set up make sure that you stop all services
Stop Kibana service

```
root@elk:~# sudo systemctl stop kibana
Stop Elasticsearch service
root@elk:~# sudo systemctl stop elasticsearch
root@elk:~# sudo nano /etc/elasticsearch/elasticsearch.yml
```

xpack.security.enabled: true
xpack.security.authc.api_key.enabled:true

```
root@elk:~# sudo systemctl restart elasticsearch
```

Generate Passwords
Go to /usr/share/elasticsearch/bin/
root@elk:~# cd /usr/share/elasticsearch/bin/
root@elk:/usr/share/elasticsearch/bin# sudo ./elasticsearch-setup-passwords auto
Initiating the setup of passwords for reserved users elastic_system,beats_system,remote_monitoring_user.
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y
Changed password for user apm_system

PASSWORD apm_system = 5JYIfFJZ7LE71X6sLMTh

Changed password for user kibana_system

PASSWORD kibana_system = sMIBnZ4xK9Od1yLbvyRH

Changed password for user kibana

PASSWORD kibana = sMIBnZ4xK9Od1yLbvyRH

Changed password for user logstash_system

PASSWORD logstash_system = 5XRU2T99usCKWFs0VQO3

Changed password for user beats_system

PASSWORD beats_system = uSUOq3YDzKYkVvYuiTmh

Changed password for user remote_monitoring_user

PASSWORD remote_monitoring_user = wK8wB4NsTmuZFy5PBhRF

Changed password for user elastic

PASSWORD elastic = 50X1xcn80az1w5HrJjK9

Open kibana.yml

root@elk:/usr/share/elasticsearch/bin# nano /etc/kibana/kibana.yml

server.port: 5601

server.host: "10.189.151.79"

elasticsearch.hosts: ["http://10.189.151.79:9200"]

elasticsearch.username: "elastic"

elasticsearch.password: "50X1xcn80az1w5HrJjK9"

Restart kibana

root@elk:~# systemctl restart kibana

The image shows two screenshots of the Elastic Stack interface. The top screenshot is a login page titled 'Welcome to Elastic' with fields for 'Username' (elastic) and 'Password'. The bottom screenshot is the 'Welcome home' dashboard, featuring four main sections: 'Enterprise Search' (yellow), 'Observability' (pink), 'Security' (teal), and 'Analytics' (blue). The left sidebar contains navigation links for 'Analytics', 'Enterprise Search', 'Observability', and 'Management'.

Implement real-time threat detection & alerting for anomalies.

Note : I have already worked on this to save time I am attaching entire procedure of my previous project !

Download filebeat in windows machine

<https://www.elastic.co/downloads/past-releases/filebeat-7-17-12>

Go to filebeat.yml

In filebeat inputs à type enabed ,path ,tags are configured

```

# ===== Filebeat inputs =====

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

# filestream is an input for collecting log messages from files.
- type: log

  # Unique ID among all inputs, an ID is required.
  #id: my-filestream-id

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx
  tags: ["sysmon"]

  #- /var/log/*.log
  #- c:\programdata\elasticsearch\logs\*

```

In logstash output ip and port of .conf file con.d folder of logstash

```

# ----- Logstash Output -----
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.195.148:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificateAuthorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

```

Navigate to filbeat path :

```
PS C:\WINDOWS\system32> cd "C:\Program Files\Filebeat"
```

Apply changes

Check configuration of filebeat
 .\filebeat.exe -e test config

```

PS C:\Program Files\Filebeat> ./filebeat.exe -c test config
2023-09-23T02:54:14.768+0530 INFO instance/beat.go:698 Home path: [C:\Program Files\Filebeat] Config path: [C:\Program Files\Filebeat] Data path: [C:\Program Files\Filebeat\data] Logs path: [C:\Program Files\Filebeat\logs] Hosts Path: [/]
2023-09-23T02:54:14.768+0530 INFO instance/beat.go:706 Beat ID: 38f326b3-3fa1-4a17-96c2-5032a3c22fcf
2023-09-23T02:54:14.768+0530 WARN [add_cloud_metadata] add_cloud_metadata/provider_aws_ec2.go:79 read token request for getting IMDSv2 token returns empty: Put "http://169.254.169.254/latest/api/oken"; dial tcp 169.254.169.254:80; connectx: A socket operation was attempted to an unreachable network.. No token in the metadata request will be used.
2023-09-23T02:54:14.714+0530 INFO [beat] instance/beat.go:1052 Beat info {"system_info": {"beat": {"path": {"config": "C:\Program Files\Filebeat", "data": "C:\Program Files\Filebeat\data", "home": "C:\Program Files\Filebeat", "logs": "C:\Program Files\Filebeat\logs"}, "type": "filebeat", "uuid": "38f326b3-3fa1-4a17-96c2-5032a3c22fcf"}}, "build": {"commit": "50d7b81886765543bd9e9501826670871a046d", "libbeat": "7.17.12", "time": "2023-07-18T20:14:21.000Z", "version": "7.17.12"}}
2023-09-23T02:54:14.714+0530 INFO [beat] instance/beat.go:1064 Go runtime info {"system_info": {"go": {"os": "windows", "arch": "amd64", "max_procs": 8, "version": "go1.19.10"}}, "beat": {"path": {"config": "C:\Program Files\Filebeat", "data": "C:\Program Files\Filebeat\data", "home": "C:\Program Files\Filebeat", "logs": "C:\Program Files\Filebeat\logs"}, "type": "filebeat", "uuid": "38f326b3-3fa1-4a17-96c2-5032a3c22fcf"}}, "build": {"commit": "50d7b81886765543bd9e9501826670871a046d", "libbeat": "7.17.12", "time": "2023-07-18T20:14:21.000Z", "version": "7.17.12"}}
2023-09-23T02:54:14.714+0530 INFO [add_cloud_metadata] add_cloud_metadata/add_cloud_metadata.go:101 add_cloud_metadata: hosting provider type not detected.
2023-09-23T02:54:14.714+0530 INFO [beat] instance/beat.go:1070 Host info {"system_info": {"host": {"architecture": "x86_64", "boot_time": "2023-09-22T10:00:17+05:30", "name": "Loke4884", "ip": {"fe80::be19:c43d:2681:95df", "169.254.209.109", "fe80::ae9:69ff:fe30:77a", "169.254.90.209"}, "fe80::5faa:b6f5:c121:572e", "169.254.117.95", "fe80::6b08:244f:7792:c765", "192.168.128.1", "fe80::de01:2274:75ee:91f8", "192.168.195.1", "2409::4070:4495:1980:861:a7:bd77:1b96", "2409::4070:4495:1980:94b1:edf7:711", "fe80::e7d2:74:9200:1bf3", "192.168.231.18", "fe80::6801:f9ed:5c39:ee0f", "169.254.126.9", ":", "127.0.0.1"}, "kernel_version": "0.0.0", "os": {"name": "Windows", "platform": "Windows", "version": "Windows 11 Home Single Language", "os": "Windows", "family": "Windows", "platform": "Windows", "name": "Windows 11 Home Single Language", "os": "Windows", "version": "10.0", "minor": "10", "patch": "0", "build": "2621.2283"}, "timezone": "IST", "timezone_offset_set": "19880", "id": "701a2e2e-04-4127-a7f2-648770a858b8"}}, "beat": {"path": {"config": "C:\Program Files\Filebeat", "data": "C:\Program Files\Filebeat\data", "home": "C:\Program Files\Filebeat", "logs": "C:\Program Files\Filebeat\logs"}, "type": "filebeat", "uuid": "38f326b3-3fa1-4a17-96c2-5032a3c22fcf"}}, "build": {"commit": "50d7b81886765543bd9e9501826670871a046d", "libbeat": "7.17.12", "time": "2023-07-18T20:14:21.000Z", "version": "7.17.12"}}
2023-09-23T02:54:14.714+0530 INFO [beat] instance/beat.go:1099 Process info {"system_info": {"process": {"cwd": "C:\Program Files\Filebeat", "exe": "C:\Program Files\Filebeat\filebeat.exe", "name": "filebeat.exe", "pid": 7232, "start_time": "2023-09-23T02:54:13.932+0530"}}, "beat": {"path": {"config": "C:\Program Files\Filebeat", "data": "C:\Program Files\Filebeat\data", "home": "C:\Program Files\Filebeat", "logs": "C:\Program Files\Filebeat\logs"}, "type": "filebeat", "uuid": "38f326b3-3fa1-4a17-96c2-5032a3c22fcf"}}, "build": {"commit": "50d7b81886765543bd9e9501826670871a046d", "libbeat": "7.17.12", "time": "2023-07-18T20:14:21.000Z", "version": "7.17.12"}}
2023-09-23T02:54:14.714+0530 INFO instance/beat.go:292 Setup Beat: filebeat; Version: 7.17.12
2023-09-23T02:54:14.714+0530 INFO [publisher] pipeline/module.go:113 Beat name: Loke4884
2023-09-23T02:54:14.714+0530 WARN beater/filebeat.go:202 Filebeat is unable to load the ingest pipelines for the configured modules because the Elasticsearch output is not configured/enabled. If you have already loaded the ingest pipelines or are using Logstash pipelines, you can ignore this warning.
Config OK

```

Install filebeat

PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1

```
PS C:\Program Files\Filebeat> PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1
```

Security warning

Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run C:\Program Files\Filebeat\install-service-filebeat.ps1?

[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R

Status	Name	DisplayName
Stopped	filebeat	filebeat

Start the service of filebeat

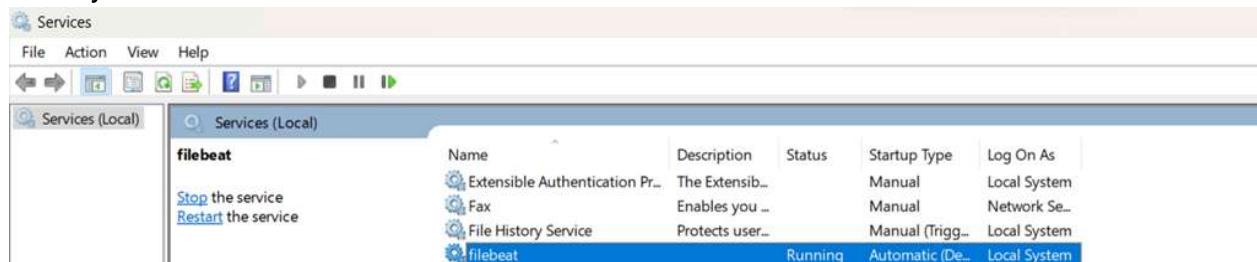
```
PS C:\Program Files\Filebeat> Start-Service filebeat
```

To check configuration of filebeat

```
PS C:\Program Files\Filebeat> .\filebeat.exe test config
Config OK
```

Search services in windows

There you can see status of filebeat



Get-Process -Name "filebeat"

```
PS C:\Program Files\Filebeat> Get-Process -Name "filebeat"
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
213	17	40360	48244	0.80	22700	0	filebeat

To check Filebeat logs

\filebeat.exe -e

Go to conf.d folder

In this folder you write configuration code for logstash to port to elk

```
root@lokesha-manikanta:/# cd /etc/logstash/conf.d/
```

Create a file with extention .conf

```
root@lokesha-manikanta:/etc/logstash/conf.d# touch sysmon.conf
```

To known any other conf file

```
root@lokes...:/etc/logstash/conf.d# ls  
sysmon.conf
```

Write a code inside sysmon.conf

```
root@lokesha-manikanta:/etc/logstash/conf.d# nano sysmon.conf
```

```
root@lokesh-manikanta:/etc/logstash/conf.d
GNU nano 6.2                                     sysmon.conf

input {
  beats {
    port => 5044
  }
}

filter {
  if "sysmon" in [tags] {
    grok {
      match=>["%{DATESTAMP}Date %{LOGLEVEL:LOGLEVEL} %{IP:ip} %{GREEDYDATA:data}","%{DATESTAMP}Date1 %{LOGLEVEL:LOGLEVEL1} %{GREEDYDATA:data1}","%{DATESTAMP}Date2 %{GREEDYDATA:data2}"]
    }
    # Add additional filter plugins for further processing as needed
  }
}

output {
  elasticsearch {
    hosts => ["192.168.195.148:9200"]
    user => "elastic"
    password => "7gln9uo4vSh1c5n4I"
    index => "sysmon-%{+YYYY.MM.dd}"
  }
}
```

Save and close Sysmon.conf

Sysmon.conf code :

```

input {
  beats {
    port => 5044
  }
}

filter {
  if "sysmon" in [tags] {
    grok {

match=>{"message"=>["%{DATESTAMP:Date} %{LOGLEVEL:LOGLEVEL} %{IP:ip}
%{GREEDYDATA:data}","%{DATESTAMP:Date1} %{LOGLEVEL:LOGLEVEL1} %{GREEDYDATA:data1}"
,"%{DATESTAMP:Date2} %{GREEDYDATA:data2}"]
    }
  }
  # Add additional filter plugins for further processing as needed
}

output {
  elasticsearch {
    hosts => ["192.168.195.148:9200"]
    user => "elastic"
    password => "u7gin9UoF4vSh1c5n44I"
    index => "sysmon-%{+YYYY.MM.dd}"
  }
}

```

Restart logstash

```
root@lolesh-manikanta:/etc/logstash/conf.d# systemctl restart logstash
```

Start the services of the logstash

```
root@lolesh-manikanta:/etc/logstash/conf.d# sudo service logstash start
```

To see logs of logstash (logs will be stored in logstash-plain.log)

```
root@lolesh-manikanta:/etc/logstash/conf.d# tail -f /var/log/logstash/logstash-plain.log
[2023-09-23T02:46:37.850][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch version determined (7.17.13) {:es_version=>7}
[2023-09-23T02:46:37.853][WARN ][logstash.outputs.elasticsearch][main] Detected a 6.x and above cluster: the 'type' event field won't be used to determine the document _type {:es_version=>7}
[2023-09-23T02:46:37.993][INFO ][logstash.outputs.elasticsearch][main] config is not compliant with data streams. 'data_stream => auto' resolved to 'false'
[2023-09-23T02:46:38.000][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch output using cluster config at https://192.168.195.148:9200?_xipio=true, es_version=7, :ecs_compatibility=>disabled
[2023-09-23T02:46:38.481][INFO ][logstash.javapipeline ][main] Starting pipeline (pipeline_id=>"main", :pipeline.workers=>2, "pipeline.batch.delay"=>50, "pipeline.max_inflight"=>50, "pipeline.sources"=>["/etc/logstash/conf.d/sysmon.conf"], :thread=>#<Thread:0x5c6d886f run>)
[2023-09-23T02:46:39.520][INFO ][logstash.javapipeline ][main] Pipeline Java execution initialization time ("seconds"=>1.02)
[2023-09-23T02:46:39.552][INFO ][logstash.inputs.beats ][main] Starting input listener (:address=>"0.0.0.0:5044")
[2023-09-23T02:46:39.587][INFO ][logstash.javapipeline ][main] Pipeline started ("pipeline.id"=>"main")
[2023-09-23T02:46:39.777][INFO ][org.logstash.beats.Server][main][e4d3d8525bbc91cf19057eb2d17ade11541ddc09da2a79ef06da0d020ef] Starting server on port: 5044
[2023-09-23T02:46:39.846][INFO ][logstash.agent ] Pipelines running (:{count=>1, :running_pipelines=>["main"], :non_running_pipelines=>[]})
```

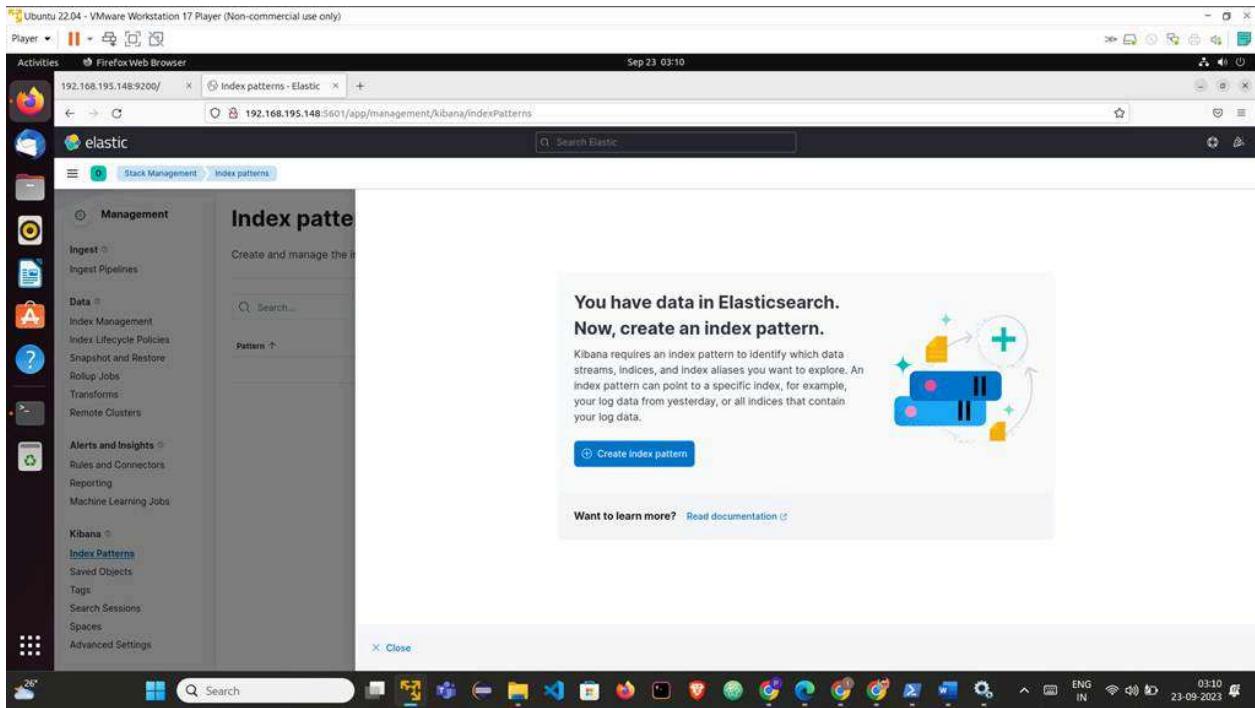
Go to Date à Index Mangement

You will get index you created in logstash configuration file(ex : sysmon.conf)

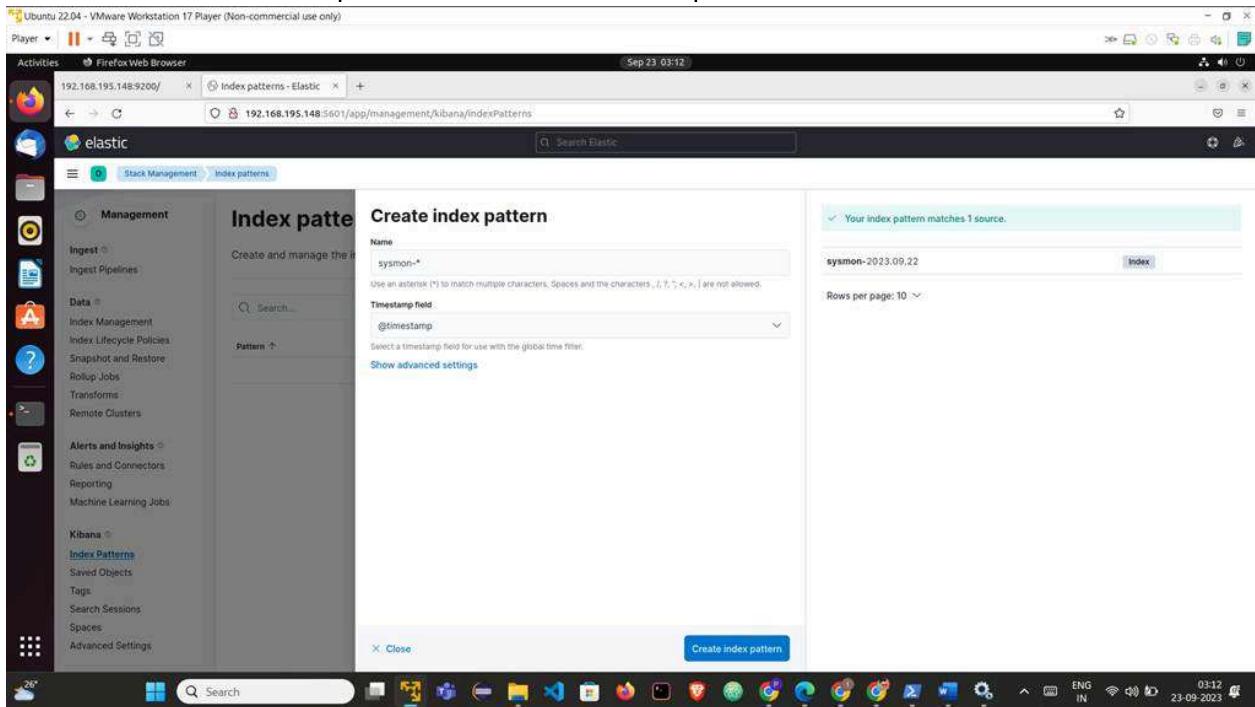
The screenshot shows the Elasticsearch Index Management interface. On the left, a sidebar menu includes sections for Management, Ingest, Data, Alerts and Insights, and Kibana. The 'Index Management' section is selected. The main area displays the 'Index Management' page with tabs for Indices, Data Streams, Index Templates, and Component Templates. The 'Indices' tab is active, showing a table with one row for the index 'sysmon-2023.09.22'. The table columns include Name, Health, Status, Primaries, Replicas, Doc count, Storage size, and Data stream. A search bar and filter options for rollup and hidden indices are at the top of the table. The status of 'sysmon-2023.09.22' is shown as yellow with an open status, 1 primary, 1 replica, 208817 documents, 151.2mb storage, and no specific data stream.

Go to kibana à Index Pattern à Create Index Pattern

The screenshot shows the Elasticsearch Index patterns interface. The sidebar menu is identical to the previous screen. The main area displays the 'Index patterns' page with a heading 'Create and manage the index patterns that help you retrieve your data from Elasticsearch.' Below this is a search bar and a table header with a 'Create index pattern' button. The table has a single column labeled 'Pattern'. A message 'No items found' is displayed below the table. The status bar at the bottom indicates the date and time as Sep 23 03:10.



Give name and time stamp and click on create index pattern



Go to discover choose what Index you created

Ubuntu 22.04 - VMware Workstation 17 Player (Non-commercial use only)

Activities Firefox Web Browser

192.168.195.148:9200/ | sysmon - Elastic | + Sep 23 03:12

elastic

Stack Management Index pattern sysmon-*

sysmon-*

Time field: @timestamp

View and edit fields in sysmon-. Field attributes, such as type and searchability, are based on [field mappings](#) in Elasticsearch.

Fields (57) Scripted fields (0) Field filters (0)

Search

Name ↗	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	
@version	text		●		
@version.keyword	keyword		●	●	
_id	_id		●	●	
_index	_index		●	●	
_score					
_source	_source				
_type	_type		●	●	
agent.ephemeral_id	text				
agent.ephemeral_id.keyword	keyword		●		

Add field

ENG IN WiFi 03:12 23-09-2023

Ubuntu 22.04 - VMware Workstation 17 Player (Non-commercial use only)

Activities Firefox Web Browser

192.168.195.148:9200/ | Discover - Elastic | + Sep 23 03:13

elastic

Discover

Search

+ Add filter

sysmon-* 208,817 hits

Chart options

Time Document

Last 15 minutes Show dates Refresh

Time	Document
Sep 23, 2023 03:03:06.567	@timestamp: Sep 23, 2023 03:03:06.567 @version: 1 agent.ephemeral_id: ab93feef-c92f-470b-a80e-f8c354807e46 agent.hostname: Loke4884 agent.id: b50bbe03-cd44-4506-9b23-6ed32fbba26 agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 ecs.version: 1.12.0 host.architecture: x86_64 host.hostname: Loke4884 host.id: 7d1a2ece-0d45-4127-a72f-648770a85b0b host.ip: fe80::be19:c43d:2b81:95df, 169.254.289.109, fe80::7ae9:409e:f3f0:f72, 169.254.98.202, fe80::5faa:b6f5:c121:572e, 169.254.117.95, fe80::6b58:2447:7252:c7b5, 192.168.128.1, fe80::de01:2274:25ee:91f8, 192.168.195.1, 2409:4070:4495:d109:861a:d07:bd77:1b9e, 2409:4070:4495:d1b9:9d81:94b1:eedf:771, fe80::e7d2:74:9200:1bf3, 192.168.231.18, fe80::6801:f9ed:5c39:ee0f, 169.254.126.9 host.mac: 00:ff:8f:b9:ed:f8, 92:e8:68:1e:9c:23, 2409:4070:4495:d1b9:9d81:94b1:eedf:771, fe80::e7d2:74:9200:1bf3, 192.168.231.18, fe80::6801:f9ed:5c39:ee0f, 169.254.126.9 host.mac: 00:ff:8f:b9:ed:f8, 92:e8:68:1e:9c:23
Sep 23, 2023 03:03:06.567	@timestamp: Sep 23, 2023 03:03:06.567 @version: 1 agent.ephemeral_id: ab93feef-c92f-470b-a80e-f8c354807e46 agent.hostname: Loke4884 agent.id: b50bbe03-cd44-4506-9b23-6ed32fbba26 agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 ecs.version: 1.12.0 host.architecture: x86_64 host.hostname: Loke4884 host.id: 7d1a2ece-0d45-4127-a72f-648770a85b0b host.ip: fe80::be19:c43d:2b81:95df, 169.254.289.109, fe80::7ae9:409e:f3f0:f72, 169.254.98.202, fe80::5faa:b6f5:c121:572e, 169.254.117.95, fe80::6b58:2447:7252:c7b5, 192.168.128.1, fe80::de01:2274:25ee:91f8, 192.168.195.1, 2409:4070:4495:d109:861a:d07:bd77:1b9e, 2409:4070:4495:d1b9:9d81:94b1:eedf:771, fe80::e7d2:74:9200:1bf3, 192.168.231.18, fe80::6801:f9ed:5c39:ee0f, 169.254.126.9 host.mac: 00:ff:8f:b9:ed:f8, 92:e8:68:1e:9c:23, 2409:4070:4495:d1b9:9d81:94b1:eedf:771, fe80::e7d2:74:9200:1bf3, 192.168.231.18, fe80::6801:f9ed:5c39:ee0f, 169.254.126.9 host.mac: 00:ff:8f:b9:ed:f8, 92:e8:68:1e:9c:23
Sep 23, 2023 03:03:06.567	@timestamp: Sep 23, 2023 03:03:06.567 @version: 1 agent.ephemeral_id: ab93feef-c92f-470b-a80e-f8c354807e46 agent.hostname: Loke4884 agent.id: b50bbe03-cd44-4506-9b23-6ed32fbba26 agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 ecs.version: 1.12.0 host.architecture: x86_64 host.hostname: Loke4884 host.id: 7d1a2ece-0d45-4127-a72f-648770a85b0b host.ip: fe80::be19:c43d:2b81:95df, 169.254.289.109, fe80::7ae9:409e:f3f0:f72, 169.254.98.202, fe80::5faa:b6f5:c121:572e, 169.254.117.95, fe80::6b58:2447:7252:c7b5, 192.168.128.1, fe80::de01:2274:25ee:91f8, 192.168.195.1, 2409:4070:4495:d109:861a:d07:bd77:1b9e, 2409:4070:4495:d1b9:9d81:94b1:eedf:771, fe80::e7d2:74:9200:1bf3, 192.168.231.18, fe80::6801:f9ed:5c39:ee0f, 169.254.126.9 host.mac: 00:ff:8f:b9:ed:f8, 92:e8:68:1e:9c:23, 2409:4070:4495:d1b9:9d81:94b1:eedf:771, fe80::e7d2:74:9200:1bf3, 192.168.231.18, fe80::6801:f9ed:5c39:ee0f, 169.254.126.9 host.mac: 00:ff:8f:b9:ed:f8, 92:e8:68:1e:9c:23

ENG IN WiFi 03:13 23-09-2023

PART 4: NETWORK AUTOMATION & CI/CD FOR INFRASTRUCTURE

Continuous Compliance & Auditing:

Implement OpenSCAP or CIS Benchmark scans for security compliance.

Download the compressed XML

```
lokesh@cybercub:~$ wget
https://security-metadata.canonical.com/oval/com.ubuntu.$(lsb_release -cs).usn.oval.xml.bz2
--2025-03-15 15:55:54--
https://security-metadata.canonical.com/oval/com.ubuntu.jammy.usn.oval.xml.bz2
Resolving security-metadata.canonical.com (security-metadata.canonical.com)...
2620:2d:4000:1::28, 2620:2d:4000:1::27, 2620:2d:4000:1::26, ...
Connecting to security-metadata.canonical.com
(security-metadata.canonical.com)|2620:2d:4000:1::28|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 653195 (638K) [application/x-bzip2]
Saving to: 'com.ubuntu.jammy.usn.oval.xml.bz2'

com.ubuntu.jammy.us 100%[=====] 637.89K 435KB/s in 1.5s

2025-03-15 15:56:33 (435 KB/s) - 'com.ubuntu.jammy.usn.oval.xml.bz2' saved [653195/653195]
```

Uncompress the data

```
lokesh@cybercub:~$ bunzip2 com.ubuntu.$(lsb_release -cs).usn.oval.xml.bz2
```

To evaluate the OVAL , Install Dependencies

```
lokesh@cybercub:~$ sudo apt install libopenscap8
[sudo] password for lokesh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  libopenscap8
0 upgraded, 1 newly installed, 0 to remove and 54 not upgraded.
Need to get 2,189 kB of archives.
```

After this operation, 66.0 MB of additional disk space will be used.

```
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libopenscap8 amd64  
1.2.17-0.1ubuntu7.22.04.2 [2,189 kB]  
Fetched 2,189 kB in 6s (379 kB/s)  
Selecting previously unselected package libopenscap8.  
(Reading database ... 245543 files and directories currently installed.)  
Preparing to unpack .../libopenscap8_1.2.17-0.1ubuntu7.22.04.2_amd64.deb ...  
Unpacking libopenscap8 (1.2.17-0.1ubuntu7.22.04.2) ...  
Setting up libopenscap8 (1.2.17-0.1ubuntu7.22.04.2) ...  
Processing triggers for man-db (2.10.2-1) ...  
Processing triggers for libc-bin (2.35-0ubuntu3.9) ...
```

Use OpenSCAP to evaluate the OVAL and generate an html report:

```
lokesh@cybercub:~$ oscap oval eval --report report.html com.ubuntu.$(lsb_release  
-cs).usn.oval.xml  
Definition oval:com.ubuntu.jammy:def:991000000: false  
Definition oval:com.ubuntu.jammy:def:981000000: false  
Definition oval:com.ubuntu.jammy:def:971000000: false  
Definition oval:com.ubuntu.jammy:def:961000000: false  
Definition oval:com.ubuntu.jammy:def:951000000: false  
Definition oval:com.ubuntu.jammy:def:941000000: false  
Definition oval:com.ubuntu.jammy:def:931000000: false  
Definition oval:com.ubuntu.jammy:def:921000000: false  
Definition oval:com.ubuntu.jammy:def:911000000: false  
Definition oval:com.ubuntu.jammy:def:901000000: false  
Definition oval:com.ubuntu.jammy:def:891000000: false  
. . .  
Definition oval:com.ubuntu.jammy:def:100: true  
Evaluation done.
```

```
lokesh@cybercub:~$ ll
total 18856
drwxr-x---+ 23 lokesh lokesh 4096 Mar 15 16:00 .
drwxr-xr-x. 3 root root 4096 Jul 27 2024 ..
-rw----- 1 lokesh lokesh 34550 Mar 15 15:02 .bash_history
-rw-r--r--. 1 lokesh lokesh 220 Jul 27 2024 .bash_logout
-rw-r--r--. 1 lokesh lokesh 3881 Nov 11 00:39 .bashrc
drwx----- 21 lokesh lokesh 4096 Feb 12 01:51 .cache/
.
.
.
-rw-rw-r-- 1 lokesh lokesh 2480339 Mar 15 16:00 report.html
```

OpenScap result of scans for security compliance for my local machine

OVAL Results Generator Information						
Schema Version	Product Name	Product Version	Date	Time	OVAL Definition Generator Information	
5.11.1	cpe:/a:open-scap:oscap	1.2.17	2025-03-15	16:00:25	#Definitions	1
#X	#	#Error	#Unknown	#Other	#Tests	2025-03-15
0	1401	0	0	1	#Objects	07:43:55
					#States	
					#Variables	
					1402 Total	3043
					3043	3043
						2099

System Information						
Host Name	cybercub					
Operating System	Linux					
Operating System Version	#53-22-04-1-Ubuntu SMP PREEMPT_DYNAMIC Wed Jan 15 19:18:46 UTC 2					
Architecture	x86_64					

Interfaces	Interface Name	lo
	IP Address	127.0.0.1
	MAC Address	00:00:00:00:00:00
	Interface Name	virbr0
	IP Address	192.168.127.1
	MAC Address	52:54:00:C7:B2:4F
	Interface Name	bxnet0
	IP Address	10.0.3.1
	MAC Address	00:16:3E:00:00:00
	Interface Name	wlp1s0
	IP Address	192.168.29.7
	MAC Address	90:CB:4C:9C:23:AC
	Interface Name	br-1e0dd4c2c9ac
	IP Address	172.16.0.1
	MAC Address	02:42:CF:D8:05:62
	Interface Name	docker0
	IP Address	172.17.0.1
	MAC Address	02:42:F0:07:3E:2C
	Interface Name	vxdbr0
	IP Address	10.51.9.1
	MAC Address	00:16:3E:51:25:26
	Interface Name	vxbr1
	IP Address	10.189.151.1
	MAC Address	00:16:3E:B7:CA:8E
	Interface Name	lo
	IP Address	-1
	MAC Address	00:00:00:00:00:00
	Interface Name	wlp1s0
	IP Address	2405:201::023:4134:646f:15d3:9b00:11d7
	MAC Address	90:EB:68:1E:9C:23
	Interface Name	vxbr0
	IP Address	2405:201::023:4134:769:9d99:c9a3:3c97
	MAC Address	90:EB:68:1E:9C:23
	Interface Name	wlp1s0
	IP Address	9e90:9ebe:933:fa46:922e
	MAC Address	90:EB:68:1E:9C:23
	Interface Name	br-1e0dd4c2c9ac

OVAL Definition Results				Title
	True	Inventory	[LSN-0099-1], [CVE-2023-42754], [CVE-2023-37771], [CVE-2023-3609], [CVE-2023-42753], [CVE-2023-4623], [CVE-2023-3567], [CVE-2023-40283], [CVE-2023-5191], [CVE-2023-3776], [CVE-2023-4623], [CVE-2023-3609]	Check that Ubuntu 22.04 LTS (jammy) is installed.
ID	Result	Class	Reference ID	
oval:com:ubuntu:jammy:def:100	true	inventory	[LSN-0099-1], [CVE-2023-42754], [CVE-2023-37771], [CVE-2023-3609], [CVE-2023-42753], [CVE-2023-4623], [CVE-2023-3567], [CVE-2023-40283], [CVE-2023-5191], [CVE-2023-3776], [CVE-2023-4623], [CVE-2023-3609]	LSN-0099-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:991000000	false	patch	[LSN-0098-1], [CVE-2023-3776], [CVE-2023-3609], [CVE-2023-21409], [CVE-2023-4004], [CVE-2023-3777], [CVE-2023-40283], [CVE-2023-3090], [CVE-2023-3567]	LSN-0098-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:981000000	false	patch	[LSN-0097-1], [CVE-2023-31248], [CVE-2023-32623], [CVE-2023-3098], [CVE-2023-3398], [CVE-2023-35788], [CVE-2023-35003], [CVE-2023-3389]	LSN-0097-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:961000000	false	patch	[LSN-0096-1], [CVE-2023-31430], [CVE-2023-35001], [CVE-2023-30456], [CVE-2023-31248], [CVE-2023-1380]	LSN-0096-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:951000000	false	patch	[LSN-0095-1], [CVE-2023-32233], [CVE-2023-26121], [CVE-2023-0386], [CVE-2023-1877], [CVE-2023-1380], [CVE-2023-31430]	LSN-0095-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:941000000	false	patch	[LSN-0094-1], [CVE-2023-1281], [CVE-2023-0468]	LSN-0094-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:931000000	false	patch	[LSN-0093-1], [CVE-2023-0461], [CVE-2023-0179]	LSN-0093-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:921000000	false	patch	[LSN-0092-1], [CVE-2022-42898], [CVE-2022-4378], [CVE-2022-43945]	LSN-0092-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:911000000	false	patch	[LSN-0091-1], [CVE-2022-42719], [CVE-2022-41222]	LSN-0091-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:901000000	false	patch	[LSN-0090-1], [CVE-2022-42720], [CVE-2022-1019], [CVE-2022-41674], [CVE-2022-42722], [CVE-2022-2602], [CVE-2022-42721]	LSN-0090-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:891000000	false	patch	[LSN-0089-1], [CVE-2022-2588], [CVE-2022-2588], [CVE-2022-29981], [CVE-2022-2588], [CVE-2022-34918], [CVE-2022-21429]	LSN-0089-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:871000000	false	patch	[LSN-0087-1]	LSN-0087-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:861000000	false	patch	[LSN-0086-1], [CVE-2022-1058], [CVE-2022-0482], [CVE-2022-30594], [CVE-2022-1118], [CVE-2022-21489], [CVE-2021-39713], [CVE-2022-29581]	LSN-0086-1 -- Kernel Live Patch Security Notice
oval:com:ubuntu:jammy:def:751100000	false	patch	[USN-7351-1], [CVE-2020-10688], [CVE-2020-1695], [CVE-2020-25633], [CVE-2021-20289], [CVE-2023-0482], [CVE-2024-9822]	USN-7351-1 -- RESTEasy vulnerabilities
oval:com:ubuntu:jammy:def:7350100000	false	patch	[USN-7350-1], [CVE-2022-30333], [CVE-2022-46578], [CVE-2023-40477], [CVE-2024-33899]	USN-7350-1 -- UnRAR vulnerabilities
oval:com:ubuntu:jammy:def:7349100000	false	patch	[USN-7349-1], [CVE-2022-30333], [CVE-2023-40477]	USN-7349-1 -- RAR vulnerabilities
oval:com:ubuntu:jammy:def:7347100000	false	patch	[USN-7347-1], [CVE-2024-38438], [CVE-2024-38440], [CVE-2024-38441]	USN-7347-1 -- Netatalk vulnerabilities
oval:com:ubuntu:jammy:def:7346100000	false	patch	[USN-7346-1], [CVE-2021-42780], [CVE-2023-2077], [CVE-2023-4060], [CVE-2023-40661], [CVE-2023-3992], [CVE-2024-45615], [CVE-2024-45616], [CVE-2024-45617], [CVE-2024-45618]	USN-7346-1 -- OpenSC vulnerabilities
oval:com:ubuntu:jammy:def:7345100000	false	patch	[USN-7345-1], [CVE-2025-24070]	USN-7345-1 -- .NET vulnerability
oval:com:ubuntu:jammy:def:7343100000	false	patch	[USN-7343-1], [CVE-2024-56201], [CVE-2024-56328], [CVE-2025-27510]	USN-7343-1 -- Jing2 vulnerabilities
oval:com:ubuntu:jammy:def:7337100000	false	patch	[USN-7337-1], [CVE-2025-1089]	USN-7337-1 -- LibreOffice vulnerabilities
oval:com:ubuntu:jammy:def:7336100000	false	patch	[USN-7336-1], [CVE-2021-30184]	USN-7336-1 -- GNU Chess vulnerability
oval:com:ubuntu:jammy:def:7335100000	false	patch	[USN-7335-1], [CVE-2025-26699]	USN-7335-1 -- Django vulnerabilities
oval:com:ubuntu:jammy:def:7329100000	false	patch	[USN-7329-1], [CVE-2024-50274], [CVE-2024-53094], [CVE-2024-56672], [CVE-2025-0927]	USN-7329-1 -- Linux kernel vulnerabilities
oval:com:ubuntu:jammy:def:7323300000	false	patch	[USN-7328-3], [CVE-2024-56673], [CVE-2023-6921]	USN-7328-3 -- Linux kernel vulnerabilities
oval:com:ubuntu:jammy:def:7323200000	false	patch	[USN-7328-2], [CVE-2024-56672], [CVE-2025-0927]	USN-7328-2 -- Linux kernel vulnerabilities

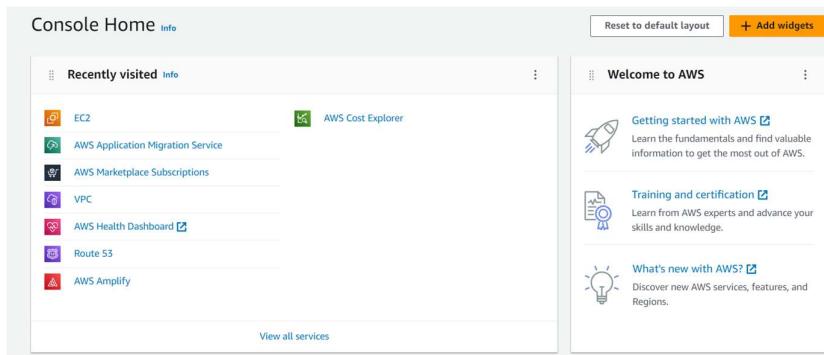
PART 5: ENTERPRISE-GRADE BACKUP & DATA PROTECTION

Data Encryption & Access Control:

Implement **Zero Trust Security Model (ZTNA)** for remote access.

Implemented a **Zero Trust Security Model (ZTNA)** for remote access using **OpenVPN** deployed on an **Amazon EC2 instance**. The setup enforces a "**Never Trust, Always Verify**" policy, ensuring strict authentication and authorization for every access request. Additionally, for enhanced security, **key pairs** are enabled to establish secure and verified remote connections.

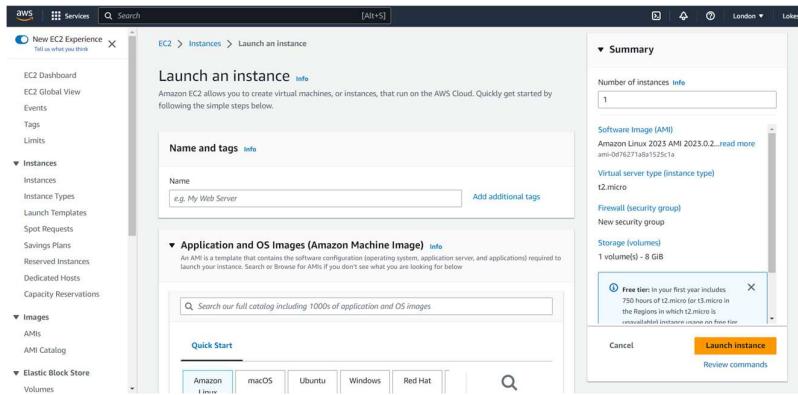
Click on EC2



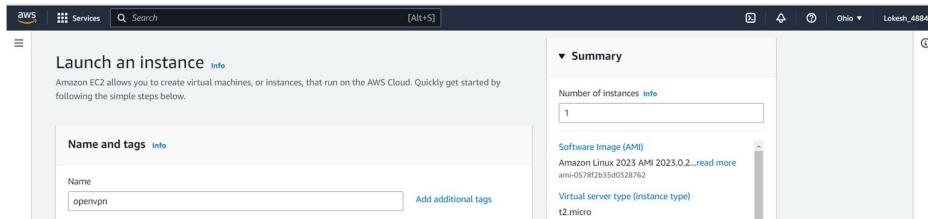
Go to EC2 -> Launch Instance

The image contains two side-by-side screenshots of the AWS EC2 Dashboard. Both screenshots show the same interface with minor differences in the status of the 'Instances' section. In both, the 'Launch instance' button is highlighted. The 'Service health' section indicates that the service is operating normally. The 'Account attributes' section shows supported platforms (VPC), default VPC (vpc-0fcd7f13339802b9), settings, EBS encryption, zones, EC2 Serial Console, default credit specification, and console experiments. The 'Explore AWS' section promotes Amazon GuardDuty Malware Protection and offers to save up to 90% on EC2 with Spot Instances.

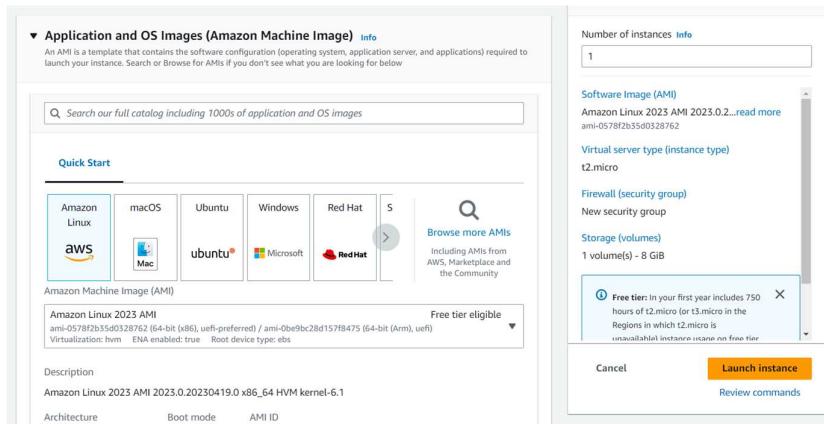
Launch the instance



Set name for launch instance :



Click on Browse more AMIs



After clicking AMIs

Go to AMIS Marketplace and search for openvpn

Click on continue

Select free tier Instance type as t2.micro

The screenshot shows the 'Instance type' section of the AWS instance creation wizard. The 't2.micro' option is selected, highlighted with a blue border. To its right, it says 'Free tier eligible'. Below this, it lists 'Family: t2' with '1 vCPU' and '1 GiB Memory', and 'Current generation: true'. On the far right, there's a 'All generations' button and a 'Compare instance types' link. A note at the bottom states: 'The AMI vendor recommends using a t2.small instance (or larger) for the best experience with this product.'

Create a new Key pair using RSA for OpenSSH then choose .pem file and click on create key pair

This image contains two screenshots from the AWS console. The left screenshot shows the 'Create key pair' dialog with a key pair name 'testopenvpn' entered. It includes fields for 'Key pair type' (RSA selected), 'Private key file format' (.pem selected), and a 'Create key pair' button. The right screenshot shows the 'Key pair (login)' dialog where the same key pair name is selected, along with a 'Create new key pair' button.

Allow SSH traffic , CUSTOMTCP traffic, CUSTOMUDP, HTTPS traffic from the internet

0.0.0.0/0 means "anywhere on the internet."

The screenshot shows the 'Firewall (security groups)' configuration screen. It features a 'Create security group' button (highlighted in blue) and a 'Select existing security group' button. Below these, it says 'We'll create a new security group called 'OpenVPN Access Server-2.11.3-AutogenByAWSMP--1' with the following rules:' followed by five checkboxes for allowing different types of traffic from anywhere (0.0.0.0/0). The rules listed are: Allow SSH traffic from anywhere, Allow CUSTOMTCP traffic from anywhere, Allow CUSTOMTCP traffic from anywhere, Allow CUSTOMUDP traffic from anywhere, and Allow HTTPS traffic from the internet.

Click on Launch Instance :

Allow SSH traffic from
Recommended rule from AMI
Anywhere
0.0.0.0/0

Allow CUSTOMTCP traffic from
Recommended rule from AMI
Anywhere
0.0.0.0/0

Allow CUSTOMTCP traffic from
Recommended rule from AMI
Anywhere
0.0.0.0/0

Allow CUSTOMUDP traffic from
Recommended rule from AMI
Anywhere
0.0.0.0/0

Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server
Allow HTTP traffic from the internet

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours

Cancel Launch instance Review commands

It takes some time

EC2 > Instances > Launch an instance

Launching instance

Please wait while we launch your instance.
Do not close your browser while this is loading.

Subscribing to Marketplace AMI 77%

▶ Details

Go to Instances -> Instances

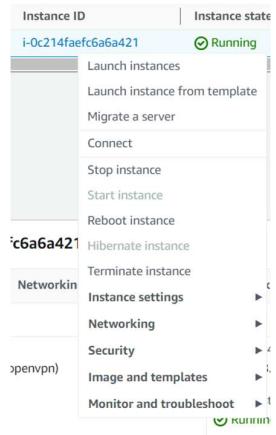
New EC2 Experience Tell us what you think

Instances (1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
openvpn	i-0c214faefc6a6a421	Running	t2.micro	Initializing	No alarms	us-east-2c	ec2-13-58-6-67.us-east-2.compute.amazonaws.com

Select an instance

Right Click on Instance ID



Click on Connect

EC2 > Instances > i-0c214faefc6a6a421 > Connect to instance

Connect to instance Info

Connect to your instance i-0c214faefc6a6a421 (openvpn) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID
i-0c214faefc6a6a421 (openvpn)

Public IP address
13.58.6.67

User name
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, root.
root

Note: In most cases, the default user name, root, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel | **Connect**

Go to SSH client

EC2 Instance Connect | Session Manager | **SSH client** | EC2 serial console

Instance ID
i-0c214faefc6a6a421 (openvpn)

- Open an SSH client.
- Locate your private key file. The key used to launch this instance is testopenvpn.pem
- Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 testopenvpn.pem
- Connect to your instance using its Public DNS:
ec2-13-58-6-67.us-east-2.compute.amazonaws.com

Example:
ssh -i "testopenvpn.pem" root@ec2-13-58-6-67.us-east-2.compute.amazonaws.com

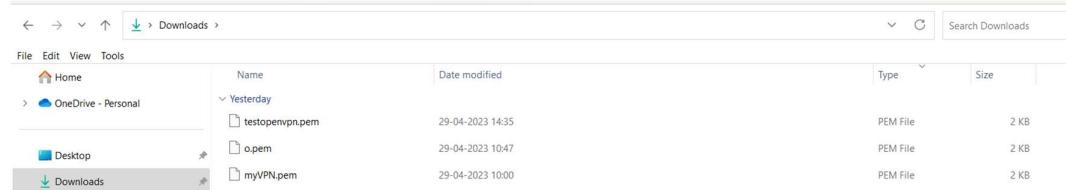
Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Copy example

Example:

```
ssh -i "testopenvpn.pem" root@ec2-13-58-6-67.us-east-2.compute.amazonaws.com
```

Copy that Command and paste it on Command Prompt (only where testopenvpn file is existed) :



Open Command prompt in download location and Execute that command :

```
Microsoft Windows [Version 10.0.22621.1555]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP\Downloads>ssh -i "testopenvpn.pem" root@ec2-13-58-6-67.us-east-2.compute.amazonaws.com
The authenticity of host 'ec2-13-58-6-67.us-east-2.compute.amazonaws.com (13.58.6.67)' can't be established.
ED25519 key fingerprint is SHA256:nJmDm2e3VNsU0AL+r87ITw72U4FIwtNSi12L7YHMA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-58-6-67.us-east-2.compute.amazonaws.com' (ED25519) to the list of known hosts.
Please login as the user "openvpnas" rather than the user "root".
Connection to ec2-13-58-6-67.us-east-2.compute.amazonaws.com closed.
```

It asks to use as openvpnas as User than root so it refuses

Use Same Command replace root as openvpnas :

Example:

```
ssh -i "testopenvpn.pem" openvpnas@ec2-13-58-6-67.us-east-2.compute.amazonaws.com
```

Instead root we use openvpnas(from the command)

```
C:\Users\HP\Downloads>ssh -i "testopenvpn.pem" openvpnas@ec2-13-58-6-67.us-east-2.compute.amazonaws.com
Welcome to OpenVPN Access Server Appliance 2.11.3

System information as of Sun Apr 30 12:34:50 UTC 2023

System load: 0.0      Processes:         98
Usage of /: 38.6% of 7.57GB  Users logged in:   0
Memory usage: 27%          IPv4 address for eth0: 172.31.40.195
Swap usage:  0%

53 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

*** System restart required ***
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

OpenVPN Access Server
Initial Configuration Tool
```

OpenVPN Access Server End User License Agreement (OpenVPN-AS EULA)

1. Copyright Notice: OpenVPN Access Server License;
Copyright (c) 2009-2022 OpenVPN Inc. All rights reserved.
"OpenVPN" is a trademark of OpenVPN Inc.
2. Redistribution of OpenVPN Access Server binary forms and related documents,
are permitted provided that redistributions of OpenVPN Access Server binary
forms and related documents reproduce the above copyright notice as well as
a complete copy of this EULA.
3. You agree not to reverse engineer, decompile, disassemble, modify,
translate, make any attempt to discover the source code of this software,
or create derivative works from this software.
4. The OpenVPN Access Server is bundled with other open source software
components, some of which fall under different licenses. By using OpenVPN
or any of the bundled components, you agree to be bound by the conditions
of the license for each respective component. For more information, you can
find our complete EULA (End-User License Agreement) on our website
(<http://openvpn.net>), and a copy of the EULA is also distributed with the
Access Server in the file /usr/local/openvpn_as/license.txt.

Like that it shows all User License Agreement

Just go with all default option

```
Please enter 'yes' to indicate your agreement [no]: yes

Once you provide a few initial configuration settings,
OpenVPN Access Server can be configured by accessing
its Admin Web UI using your Web browser.

Will this be the primary Access Server node?
(enter 'no' to configure as a backup or standby node)
> Press ENTER for default [yes]: yes

Please specify the network interface and IP address to be
used by the Admin Web UI:
(1) all interfaces: 0.0.0.0
(2) eth0: 172.31.40.195
Please enter the option number from the list above (1- 2).
> Press Enter for default [1]:
```

```
What public/private type/algorithms do you want to use for the OpenVPN CA?
Recommended choices:

rsa      - maximum compatibility
secp384r1 - elliptic curve, higher security than rsa, allows faster connection setup and smaller user profile files
showall  - shows all options including non-recommended algorithms.
> Press ENTER for default [rsa]:
```

```
What key size do you want to use for the certificates?
Key size should be between 2048 and 4096
> Press ENTER for default [ 2048 ]:
```

```
What public/private type/algorithms do you want to use for the self-signed web certificate?
Recommended choices:

rsa      - maximum compatibility
secp384r1 - elliptic curve, higher security than rsa, allows faster connection setup and smaller user profile files
showall  - shows all options including non-recommended algorithms.
> Press ENTER for default [rsa]:
```

```
What key size do you want to use for the certificates?
Key size should be between 2048 and 4096
```

```

> Press ENTER for default [ 2048 ]:
Please specify the port number for the Admin Web UI.
> Press ENTER for default [943]:
Please specify the TCP port number for the OpenVPN Daemon
> Press ENTER for default [443]:
Should client traffic be routed by default through the VPN?
> Press ENTER for default [no]:
Should client DNS traffic be routed by default through the VPN?
> Press ENTER for default [no]:
Admin user authentication will be local
Private subnets detected: ['172.31.0.0/16']
Should private subnets be accessible to clients by default?
> Press ENTER for EC2 default [yes]:

```

You can give password manually or otherwise just give enter it assigns a default password

```

To initially login to the Admin Web UI, you must use a
username and password that successfully authenticates you
with the host UNIX system (you can later modify the settings
so that RADUS or LDAP is used for authentication instead).

You can login to the Admin Web UI as "openvpn" or specify
a different user account to use for this purpose.

Do you wish to login to the Admin UI as "openvpn"?
> Press ENTER for default [yes]:
Type a password for the 'openvpn' account (if left blank, a random password will be generated):
Please, remember this password Scq4qRvFYlgM

> Please specify your Activation key (or leave blank to specify later):

```

```

Initializing OpenVPN ...
Removing Cluster Admin user login...
userdel "admin_c"
Writing configuration file...
Perform sa init...
Modifying previous userdb...
Creating default profile...
Modifying default profile...
Adding new user to userdb...
Modifying new user as superuser in userdb...
Auto-generated pass = "Scq4qRvFYlgM". Setting in db...
Getting hostname
Hostname: 13.58.6.67
Preparing web certificates...
Getting web user account...
Adding web group account...
Adding web group...
Adjusting license directory ownership...
Initializing confdb...
Initial version is not set. Setting it to 2.11.3...
Generated config for openvpnas ...
Enabling service
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service → /lib/systemd/system/openvpnas.service.
Starting openvpnas ...

NOTE: Your system clock must be correct for OpenVPN Access Server
to perform correctly. Please ensure that your time and date
are correct on this system.

```

```

Initial Configuration Complete!

You can now continue configuring OpenVPN Access Server by
directing your Web browser to this URL:

https://13.58.6.67:943/admin

During normal operation, OpenVPN AS can be accessed via these URLs:
Admin UI: https://13.58.6.67:943/admin
Client UI: https://13.58.6.67:943/
To login please use the "openvpn" account with "Scq4qRvFYlgM" password.

See the Release Notes for this release at:
https://openvpn.net/vpn-server-resources/release-notes/

```

Go to EC2 Instance Connect Copy Public IP address :

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID
i-0c214faefc6a6a421 (openvpn)

Public IP address
13.58.6.67

User name
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, root.
root

Note: In most cases, the default user name, root, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Search : <https://13.58.6.67:943/admin/>

Just proceed for action and you will get a login page :

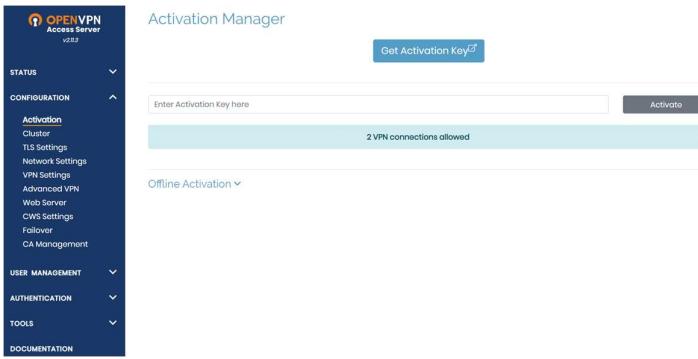
Enter user name as openvpn which you have given in making a instance in AWS and next give password which was created in command prompt



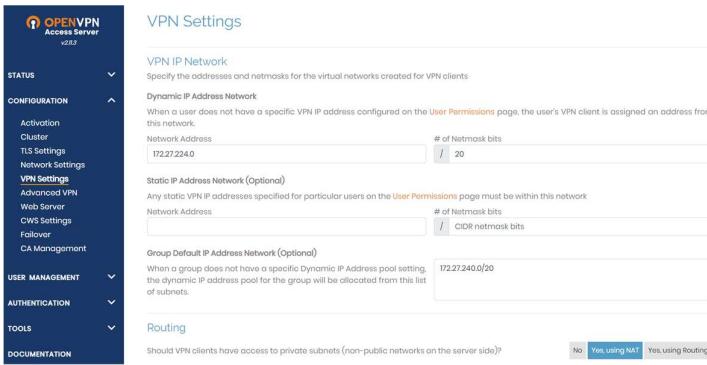
Next you will get this page press on Agree



You will get this page



Go to VPN settings



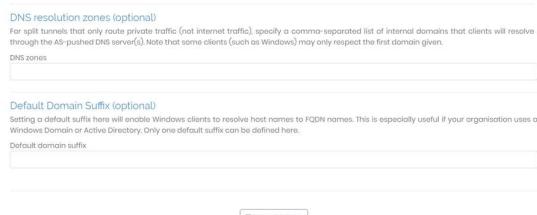
By default in VPN settings



Enable client Internet traffic be routed through VPN?



Click on Save Settings



Search in chrome: <https://13.58.6.67/>

Implement **Zero Trust Security Model (ZTNA)** for remote access, credentials which you gave in creating Instance in AWS as openvpn and enter password (which you gave in command prompt) this OpenVPN always follow ZTNA – Never Trust Always Verify policy

The image consists of three vertically stacked screenshots from a web browser and a mobile application interface.

Screenshot 1: User Login Page
A screenshot of a web browser showing the "User Login" page for "OPENVPN Access Server". The URL is https://13.58.6.67/zsc-connect. The page contains fields for "username" (openvpn) and "password" (represented by a masked field). A "Sign In" button is at the bottom.

Screenshot 2: Device Connection Options
A screenshot of the "OPENVPN Access Server" website. It displays download links for "OpenVPN Connect Recommended for your device:" (Windows), "OpenVPN Connect for all Platforms:" (Windows, macOS, Linux, iOS, Android), and "OpenVPN Connect v2:" (Windows, macOS).

Screenshot 3: OpenVPN Connect App Interface
A screenshot of the "OpenVPN Connect" mobile application. The top bar shows "OpenVPN Connect" and "Profiles". The main area indicates a "CONNECTED" status with the message "OpenVPN Profile openvpn@13.58.6.67 [bundled]". Below this, "CONNECTION STATS" show "40B/s" (down) and "0B/s" (up). The "DURATION" is listed as "00:45:57" and "PACKET RECEIVED" as "3 sec ago". At the bottom, it says "YOU openvpn" and features a large orange "+" button.

PART 6

Zeek (formerly Bro) - Network Security Monitoring Tool

- **Network Traffic Analysis** – Zeek monitors and logs network activity for security analysis.
- **Deep Packet Inspection** – Extracts detailed metadata from network packets.
- **Flexible Scripting** – Uses Zeek scripting language for custom security policies.
- **Protocol Detection** – Supports HTTP, DNS, SSL/TLS, and many more.
- **Security Event Detection** – Identifies anomalies, intrusions, and threats.
- **Log Generation** – Creates structured logs for further analysis in SIEMs.
- **Open Source & Scalable** – Used in large-scale network monitoring setups.

The `apt-get update` command updates the local package index by fetching the latest package lists from the repositories. This ensures the system is aware of available updates but does not install them.

```
root@agent:/home/lokesh# apt-get update
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
```

.

.

The `apt-get upgrade` command installs the latest versions of all installed packages without removing any existing ones. It updates only those packages that do not require dependency changes.

```
root@agent:/home/lokesh# apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
```

.

Downloading `zeek-7.0.5.tar.gz` zip file from zeek official website

```
root@agent:/home/lokesh# wget https://download.zeek.org/zeek-7.0.5.tar.gz
```

```
--2025-02-28 07:44:33-- https://download.zeek.org/zeek-7.0.5.tar.gz
Resolving download.zeek.org (download.zeek.org)... 52.84.45.124, 52.84.45.34, 52.84.45.68, ...
Connecting to download.zeek.org (download.zeek.org)|52.84.45.124|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 95847393 (91M) [application/x-gzip]
Saving to: 'zeek-7.0.5.tar.gz'

zeek-7.0.5.tar.gz
100%[=====] 91.41M 3.79MB/s in 25s
```

```
root@agent:/home/lokesh# ls
wazuh-agent_4.9.2-1_amd64.deb zeek-7.0.5.tar.gz
```

use the following commands to add zeek repository into binary packages.

```
root@agent:/home/lokesh# apt-get install cmake make gcc g++ flex bison libpcap-dev libssl-dev
python3-dev swig zlib1g-dev -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Extract zeek-7.0.5.tar.gz
root@agent:/home/lokesh# tar -xzf zeek-7.0.5.tar.gz
root@agent:/home/lokesh# ls
wazuh-agent_4.9.2-1_amd64.deb zeek-7.0.5 zeek-7.0.5.tar.gz

Go to zeek-7.0.5
root@agent:/home/lokesh# cd zeek-7.0.5
root@agent:/home/lokesh/zeek-7.0.5# ls
CHANGES Makefile auxil doc src
CMakeLists.txt NEWS ci docker testing
COPYING README cmake man vcpkg.json
COPYING-3rdparty README.md cmake_templates repo-info.json zeek-path-dev.in
INSTALL VERSION configure scripts

The `./configure` command checks system dependencies and prepares the build environment for compiling Zeek 7.0.5.

```
root@agent:/home/lokesh/zeek-7.0.5# ./configure
```

```
-- Configuring done  
-- Generating done  
-- Build files have been written to: /home/lokesh/zeek-7.0.5/build
```

The command `make install` compiles and installs Zeek 7.0.5 from source in the `/home/lokesh/zeek-7.0.5` directory on the agent system.

```
root@agent:/home/lokesh/zeek-7.0.5# make install
```

```
-- Installing: /usr/local/zeek/share/zeek/cmake/ZeekConfigVersion.cmake  
-- Installing: /usr/local/zeek/share/zeek/cmake/ZeekTargets.cmake  
make[1]: Leaving directory '/home/lokesh/zeek-7.0.5/build'
```

The command `'make'` compiles the Zeek 7.0.5 source code in the `'/home/lokesh/zeek-7.0.5'` directory on the `'agent'` system.

```
root@agent:/home/lokesh/zeek-7.0.5# make
```

```
[100%] Built target rst  
make[2]: Leaving directory '/home/lokesh/zeek-7.0.5/build'  
make[1]: Leaving directory '/home/lokesh/zeek-7.0.5/build'  
root@agent:/home/lokesh/zeek-7.0.5#
```

Go to `/usr/local/zeek/`

```
root@agent:/home/lokesh/zeek-7.0.5# cd /usr/local/zeek/  
root@agent:/usr/local/zeek# ls  
bin etc include lib logs share spool var  
root@agent:/usr/local/zeek# cd bin
```

```
root@agent:/usr/local/zeek/bin#
```

Edit the Bash configuration file for the current user.

```
root@agent:/usr/local/zeek/bin# nano ~/.bashrc
```

```
export PATH=/usr/local/zeek/bin:$PATH #Add this line at last
```

The command source `~/.bashrc` reloads the `.bashrc` file without needing to restart the shell. This applies any changes made, such as new aliases, environment variables, or custom configurations, immediately.

```
root@agent:/usr/local/zeek/bin# source ~/.bashrc
```

Check whether zeek is deployed

```
root@agent:/usr/local/zeek/bin# zeek --version
zeek version 7.0.5
```

Check where zeek installed

```
root@agent:/usr/local/zeek/bin# which zeek
/usr/local/zeek/bin/zeek
root@agent:/usr/local/zeek/bin# cd ..
root@agent:/usr/local/zeek# cd etc
root@agent:/usr/local/zeek/etc#
```

```
root@agent:/usr/local/zeek/etc# ls
networks.cfg node.cfg zeekctl.cfg zkg
```

Edit node.cfg make sure to use standalone , localhost , ethernet of local machine where zeek is hosting

```
root@agent:/usr/local/zeek/etc# nano node.cfg
[zeek]
type=standalone
host=localhost
interface=eth0
```

```
root@agent:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
17: eth0@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc qdisc state UP group default qlen 1000
    link/ether 00:16:3e:09:fcb3 brd ff:ff:ff:ff:ff:ff link-netnsid 0
        inet 10.189.151.4/24 metric 100 brd 10.189.151.255 scope global dynamic eth0
            valid_lft 3147sec preferred_lft 3147sec
        inet6 fd42:71c6:d70c:1045:216:3eff:fe09:fcb3/64 scope global mngtmpaddr noprefixroute
            valid_lft forever preferred_lft forever
        inet6 fe80::216:3eff:fe09:fcb3/64 scope link
            valid_lft forever preferred_lft forever
```

```
root@agent:/usr/local/zeek/etc# zeekctl check
Hint: Run the zeekctl "deploy" command to get started.
zeek scripts are ok.
```

```
root@agent:/usr/local/zeek/spool# apt-get install mailutils -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Deploy zeek

```
root@agent:/usr/local/zeek/etc# zeekctl deploy
checking configurations ...
installing ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
```

```
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
starting ...
starting zeek ...
root@agent:/usr/local/zeek/etc# zeekctl status
Name      Type    Host      Status  Pid  Started
zeek      standalone localhost  running 29477 28 Feb 11:17:04
```

Go to logs that captured by zeek

```
root@agent:/usr/local/zeek/etc# cd ..
root@agent:/usr/local/zeek# ls
bin etc include lib logs share spool var
root@agent:/usr/local/zeek# cd logs/
root@agent:/usr/local/zeek/logs# ls
2025-02-28 current

root@agent:/usr/local/zeek/logs# cd current
```

These all are different logs that generated by zeek

```
root@agent:/usr/local/zeek/logs/current# ls
capture_loss.log conn.log loaded_scripts.log notice.log packet_filter.log reporter.log stats.log
stderr.log stdout.log telemetry.log weird.log
```

Printing to the screen conn.log

In Zeek, conn.log is a foundational log file that tracks network connections, providing information about the source and destination hosts, ports, protocols, and connection state, allowing for analysis of network traffic and detection of unusual activity.

```
root@agent:/usr/local/zeek/logs/current# tail -f conn.log
```

```

root@agent:/usr/local/zeek/logs/current# tail -f conn.log
1740741659.305896 Cksz61hJMeFAY7bcB 10.189.151.4 55908 10.189.151.230 1514 tcp - 0.000026 0 0 RSTRH T T 0Cr 0 0 1 40
1740741669.306250 C8LFFayare1d0tSre 10.189.151.4 46112 10.189.151.230 1514 tcp - 0.000022 0 0 RSTRH T T 0Cr 0 0 1 40
1740741679.306527 Cw2l1z1e7MzSUUxrba 10.189.151.4 40226 10.189.151.230 1514 tcp - 0.000020 0 0 RSTRH T T 0Cr 0 0 1 40
1740741689.306831 CHn1nk3ePcnyGnFXh 10.189.151.4 39442 10.189.151.230 1514 tcp - 0.000027 0 0 RSTRH T T 0Cr 0 0 1 40
1740741699.307163 CwmrQ53BR98Agl1Se 10.189.151.4 45062 10.189.151.230 1514 tcp - 0.000020 0 0 RSTRH T T 0Cr 0 0 1 40
1740741699.307548 CRMgMuZBLF1YK67vZ 10.189.151.4 56526 10.189.151.230 1515 tcp - 0.000006 0 0 RSTRH T T 0Cr 0 0 1 40
1740741709.307866 CCaYP73NqSxdwsWCrh 10.189.151.4 42524 10.189.151.230 1514 tcp - 0.000026 0 0 RSTRH T T 0Cr 0 0 1 40

```

I have changed logs format to json

```

root@agent:/usr/local/zeek/logs/current# tail -f conn.log
{"ts":1740954863.250134,"uid":"CyCGXM2n791ANkwBSI","id_orig_h":"fd42:71c6:d70c:1045::1","id_orig_p":5353,"id_resp_h":"ff02::fb","id_resp_p":5353,"proto":"udp","conn_state":"OTH","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"C","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1740954863.250256,"uid":"CUMjeL2eDwRrHbKBa","id_orig_h":"10.189.151.1","id_orig_p":5353,"id_resp_h":"224.0.0.251","id_resp_p":5353,"proto":"udp","conn_state":"OTH","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"C","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1740954872.461894,"uid":"CdVgF23kGRzguGp0v8","id_orig_h":"10.189.151.4","id_orig_p":68,"id_resp_h":"10.189.151.1","id_resp_p":67,"proto":"udp","conn_state":"OTH","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"C","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1740954863.254029,"uid":"CskYGd2bMnUrvMrQ4l","id_orig_h":"fe80::216:3eff:feb7:ca8e","id_orig_p":143,"id_resp_h":"ff02::16","id_resp_p":0,"proto":"icmp","duration":0.27585291862487793,"orig_bytes":40,"resp_bytes":0,"conn_state":"OTH","local_orig":true,"local_resp":false,"missed_bytes":0,"orig_pkts":2,"orig_ip_bytes":152,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}

```