Record SSH Sessions Established Through a Bastion Host

Let’s the Bastion Journey begins

Contents

1. High-level Description
2. Benefits/Necessity of Bastion Host
3. Demo of Bastion Solution
4. Low-level (deeper level) Architecture
5. Things I learnt

High-level Description

What is a Bastion host?

Bastion host or the jump server is an entry point to the actual server in the private network (or private subnet). In this way, bastion host provides an additional layer of protection to the actual server from any external harmful actors on the internet.

The Bastion host is in a public subnet, so using Bastion host, we can access private EC2 instance within same VPC by SSH connection.

Let's see how to implement this with following diagram:

AWS Console Implementation: — A AWS diagram explains more than a detailed paragraph.

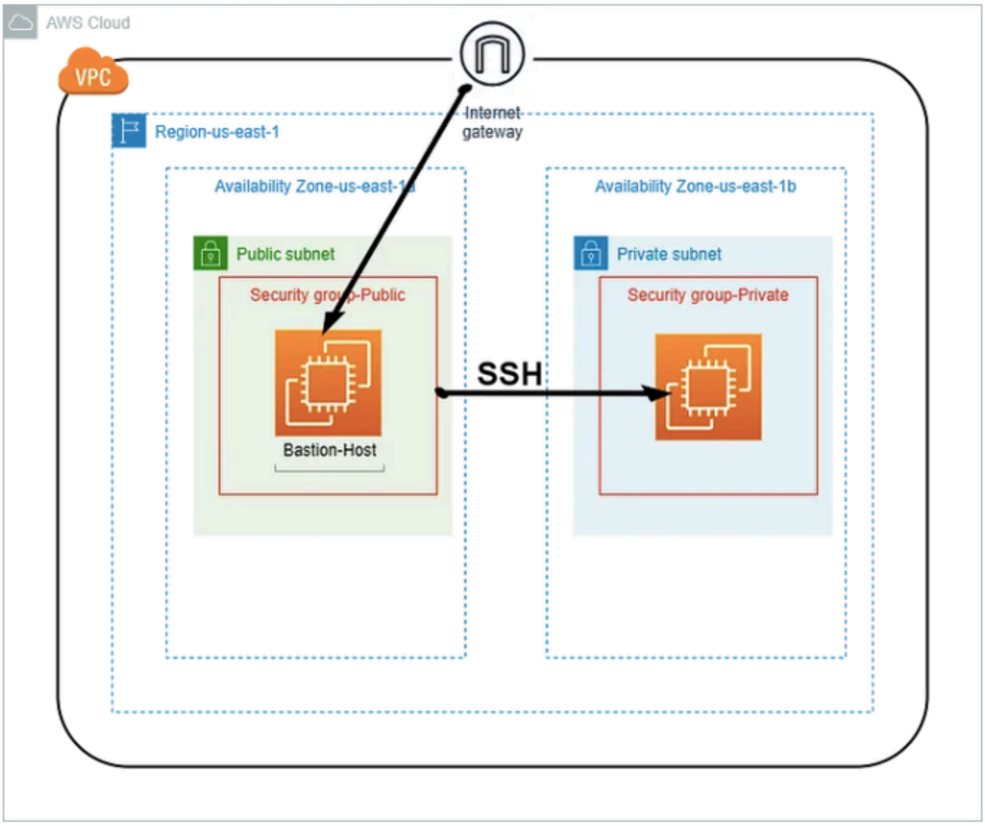
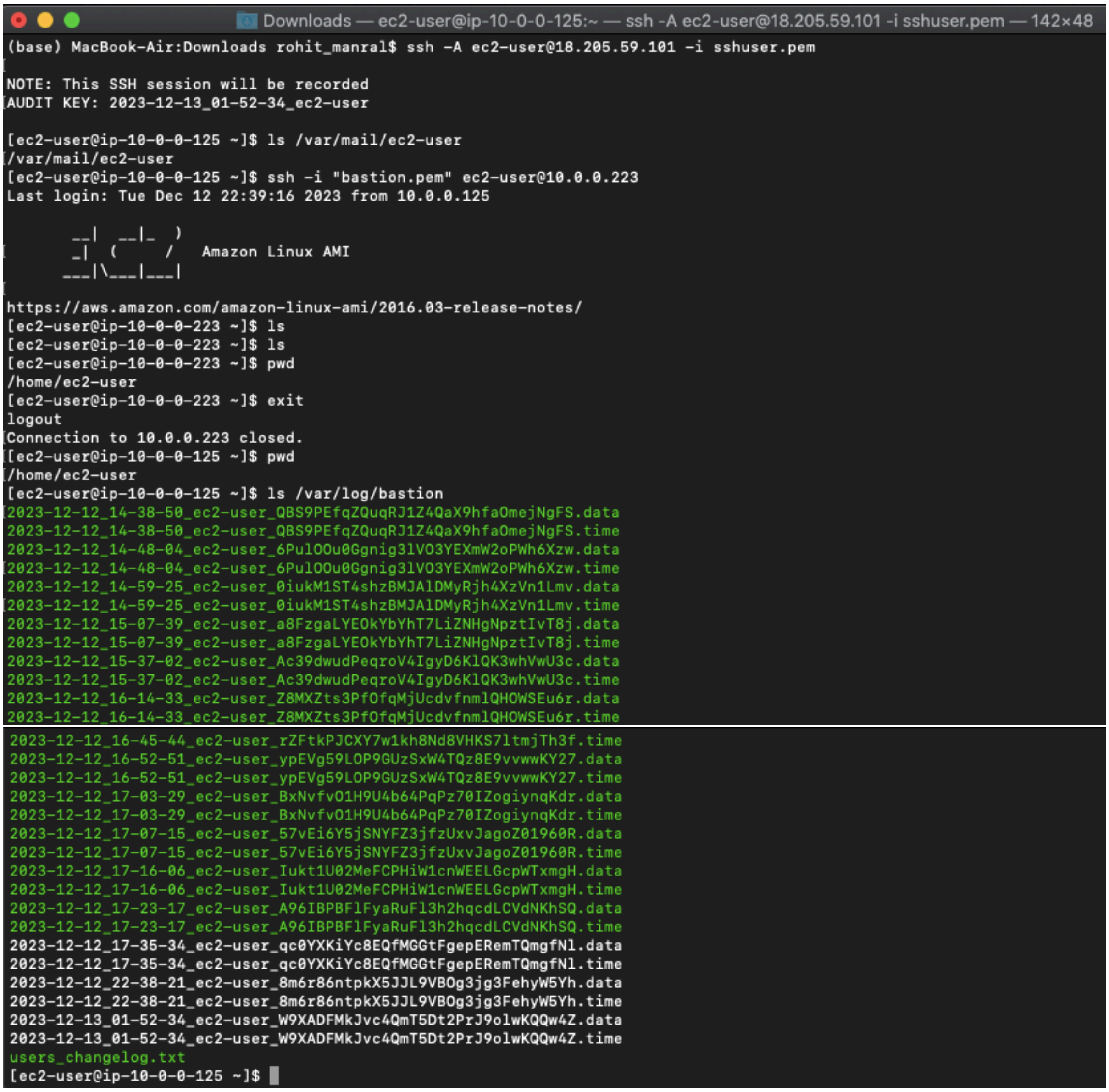


Figure: SSH into a private EC2 instance through Bastion host

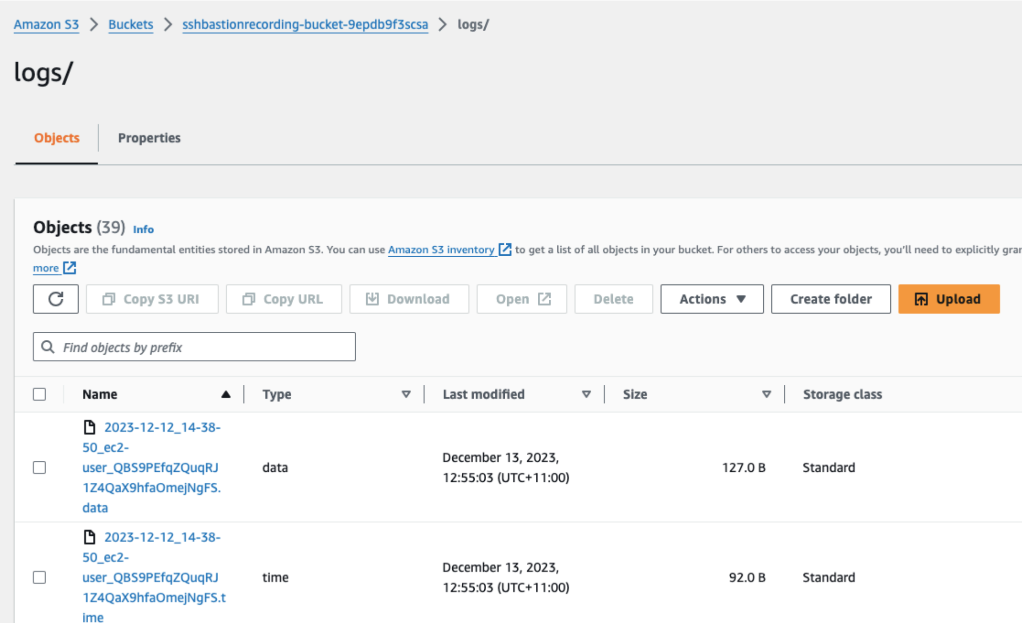
Results of SSH sessions recorded by Bastion Host?

a) Terminal


Downloads — ec2-user@ip-10-0-0-125:~ — ssh -A ec2-user@18.205.59.101 -i sshuser.pem — 142×48

```
(base) MacBook-Air:Downloads rohit_manral$ ssh -A ec2-user@18.205.59.101 -i sshuser.pem

NOTE: This SSH session will be recorded
AUDIT KEY: 2023-12-13_01-52-34_ec2-user

[ec2-user@ip-10-0-0-125 ~]$ ls /var/mail/ec2-user
/var/mail/ec2-user
[ec2-user@ip-10-0-0-125 ~]$ ssh -i "bastion.pem" ec2-user@10.0.0.223
Last login: Tue Dec 12 22:39:16 2023 from 10.0.0.125

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2016.03-release-notes/
[ec2-user@ip-10-0-0-223 ~]$ ls
[ec2-user@ip-10-0-0-223 ~]$ ls
[ec2-user@ip-10-0-0-223 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-0-223 ~]$ exit
logout
Connection to 10.0.0.223 closed.
[ec2-user@ip-10-0-0-125 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-0-125 ~]$ ls /var/log/bastion
2023-12-12_14-38-50_ec2-user_QBS9PEfqZQuqRJ1Z4QaX9hfaOmejNgFS.data
2023-12-12_14-38-50_ec2-user_QBS9PEfqZQuqRJ1Z4QaX9hfaOmejNgFS.time
2023-12-12_14-48-04_ec2-user_6PulOOu0Ggnig3lVO3YEXmW2oPWh6Xzw.data
2023-12-12_14-48-04_ec2-user_6PulOOu0Ggnig3lVO3YEXmW2oPWh6Xzw.time
2023-12-12_14-59-25_ec2-user_0iukM1ST4shzBMJAlDMyRjh4XzVn1Lmv.data
2023-12-12_14-59-25_ec2-user_0iukM1ST4shzBMJAlDMyRjh4XzVn1Lmv.time
2023-12-12_15-07-39_ec2-user_a8FzgaLYEOkYbYhT7LiZNHgNpztIvT8j.data
2023-12-12_15-07-39_ec2-user_a8FzgaLYEOkYbYhT7LiZNHgNpztIvT8j.time
2023-12-12_15-37-02_ec2-user_Ac39dwudPeqroV4IgyD6KlQK3whVwU3c.data
2023-12-12_15-37-02_ec2-user_Ac39dwudPeqroV4IgyD6KlQK3whVwU3c.time
2023-12-12_16-14-33_ec2-user_Z8MXZts3PfOfqMjUcdvfnmlQHOWSEu6r.data
2023-12-12_16-14-33_ec2-user_Z8MXZts3PfOfqMjUcdvfnmlQHOWSEu6r.time
2023-12-12_16-45-44_ec2-user_rZFtkPJCXY7w1kh8Nd8VHKS7ltmjTh3f.time
2023-12-12_16-52-51_ec2-user_ypEVg59LOP9GUzSxW4TQz8E9vvwwKY27.data
2023-12-12_16-52-51_ec2-user_ypEVg59LOP9GUzSxW4TQz8E9vvwwKY27.time
2023-12-12_17-03-29_ec2-user_BxNvfvO1H9U4b64PqPz70IZogiynqKdr.data
2023-12-12_17-03-29_ec2-user_BxNvfvO1H9U4b64PqPz70IZogiynqKdr.time
2023-12-12_17-07-15_ec2-user_57vEi6Y5jSNYFZ3jfzUxvJagoZ01960R.data
2023-12-12_17-07-15_ec2-user_57vEi6Y5jSNYFZ3jfzUxvJagoZ01960R.time
2023-12-12_17-16-06_ec2-user_Iukt1U02MeFCPHiW1cnWEELGcpWTxmgH.data
2023-12-12_17-16-06_ec2-user_Iukt1U02MeFCPHiW1cnWEELGcpWTxmgH.time
2023-12-12_17-23-17_ec2-user_A96IBPBFlFyaRuFl3h2hqcdLCVdNKhSQ.data
2023-12-12_17-23-17_ec2-user_A96IBPBFlFyaRuFl3h2hqcdLCVdNKhSQ.time
2023-12-12_17-35-34_ec2-user_qc0YXKiYc8EQfMGGtFgepERemTQmgfNl.data
2023-12-12_17-35-34_ec2-user_qc0YXKiYc8EQfMGGtFgepERemTQmgfNl.time
2023-12-12_22-38-21_ec2-user_8m6r86ntpkX5JJL9VBOg3jg3FehyW5Yh.data
2023-12-12_22-38-21_ec2-user_8m6r86ntpkX5JJL9VBOg3jg3FehyW5Yh.time
2023-12-13_01-52-34_ec2-user_W9XADFMkJvc4QmT5Dt2PrJ9olwKQQw4Z.data
2023-12-13_01-52-34_ec2-user_W9XADFMkJvc4QmT5Dt2PrJ9olwKQQw4Z.time
users_changelog.txt
[ec2-user@ip-10-0-0-125 ~]$ 
```

b) **Log activity** files getting saved in **S3 Bucket Logs**



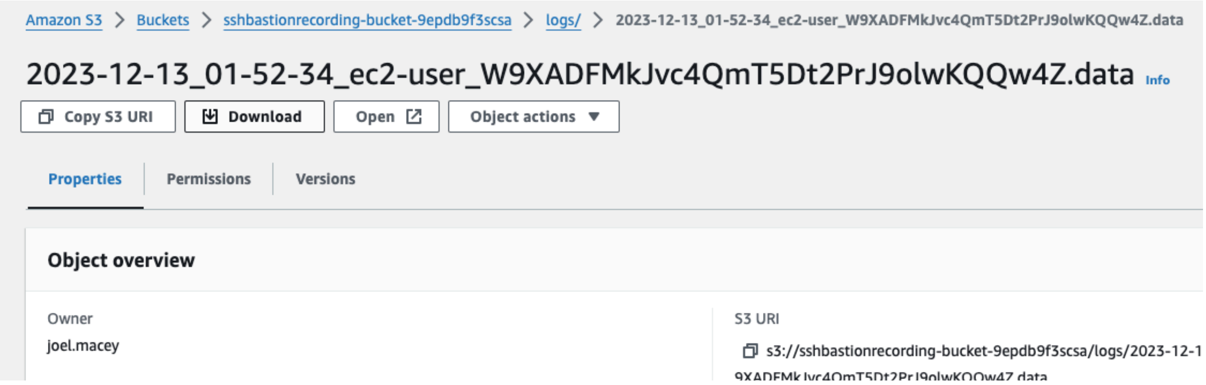
logs/

Objects (39) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grar
more

□	Name ▲	Type	Last modified	Size	Storage class
□	2023-12-12_14-38-50_ec2-user_QBS9PEfqZQuqRJ1Z4QaX9hfaOmejNgFS.data	data	December 13, 2023, 12:55:03 (UTC+11:00)	127.0 B	Standard
□	2023-12-12_14-38-50_ec2-user_QBS9PEfqZQuqRJ1Z4QaX9hfaOmejNgFS.time	time	December 13, 2023, 12:55:03 (UTC+11:00)	92.0 B	Standard

We can download any data object from here


Amazon S3 > Buckets > sshbastionrecording-bucket-9epdb9f3scsa > logs/ > 2023-12-13_01-52-34_ec2-user_W9XADFMkJvc4QmT5Dt2PrJ9olwKQQw4Z.data
Info
Copy S3 URI
Download
Open
Object actions ▼
Properties
Permissions
Versions

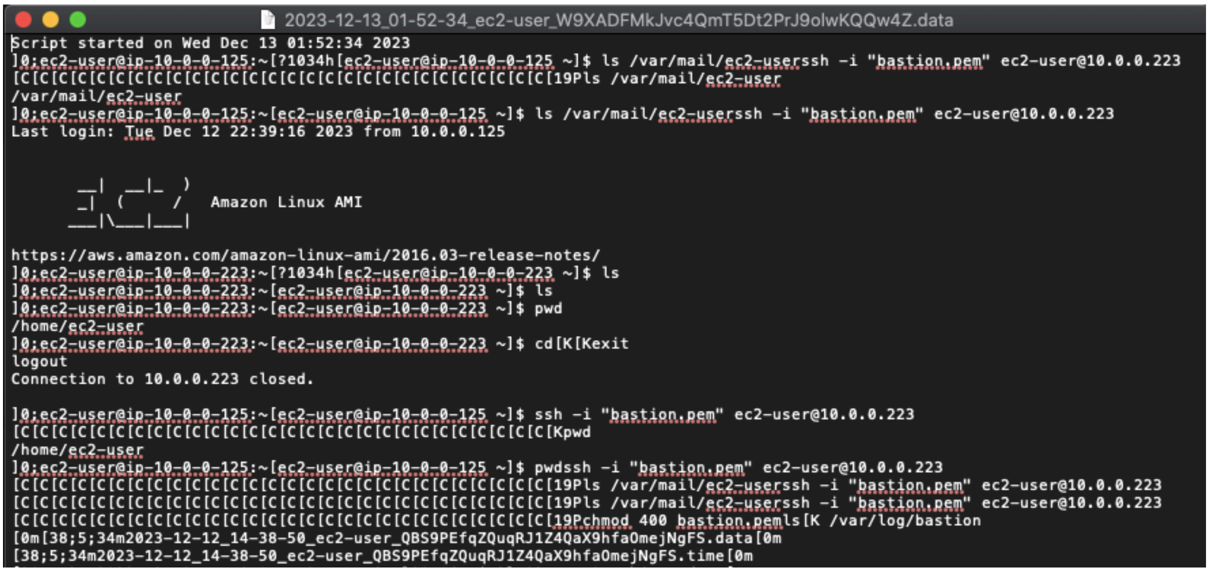
2023-12-13_01-52-34_ec2-user_W9XADFMkJvc4QmT5Dt2PrJ9olwKQQw4Z.data

Object overview

Owner
joel.macey

S3 URI
s3://sshbastionrecording-bucket-9epdb9f3scsa/logs/2023-12-1
9XADFMkJvc4QmT5Dt2PrJ9olwKQQw4Z.data

After downloading this object we will open it.


2023-12-13_01-52-34_ec2-user_W9XADFMkJvc4QmT5Dt2PrJ9olwKQQw4Z.data

```
Script started on Wed Dec 13 01:52:34 2023
]0;ec2-user@ip-10-0-0-125:~[?1034h[ec2-user@ip-10-0-0-125 ~]$ ls /var/mail/ec2-userssh -i "bastion.pem" ec2-user@10.0.0.223
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[19Pls /var/mail/ec2-user
/var/mail/ec2-user
]0;ec2-user@ip-10-0-0-125:~[ec2-user@ip-10-0-0-125 ~]$ ls /var/mail/ec2-userssh -i "bastion.pem" ec2-user@10.0.0.223
Last login: Tue Dec 12 22:39:16 2023 from 10.0.0.125


       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2016.03-release-notes/
]0;ec2-user@ip-10-0-0-223:~[?1034h[ec2-user@ip-10-0-0-223 ~]$ ls
]0;ec2-user@ip-10-0-0-223:~[ec2-user@ip-10-0-0-223 ~]$ ls
]0;ec2-user@ip-10-0-0-223:~[ec2-user@ip-10-0-0-223 ~]$ pwd
/home/ec2-user
]0;ec2-user@ip-10-0-0-223:~[ec2-user@ip-10-0-0-223 ~]$ cd[K[Kexit
logout
Connection to 10.0.0.223 closed.

]0;ec2-user@ip-10-0-0-125:~[ec2-user@ip-10-0-0-125 ~]$ ssh -i "bastion.pem" ec2-user@10.0.0.223
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[Kpwd
/home/ec2-user
]0;ec2-user@ip-10-0-0-125:~[ec2-user@ip-10-0-0-125 ~]$ pwdssh -i "bastion.pem" ec2-user@10.0.0.223
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[19Pls /var/mail/ec2-userssh -i "bastion.pem" ec2-user@10.0.0.223
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[19Pls /var/mail/ec2-userssh -i "bastion.pem" ec2-user@10.0.0.223
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[19Pchmod 400 bastion.pemls[K /var/log/bastion
[0m[38;5;34m2023-12-12_14-38-50_ec2-user_QBS9PEfqZQuqRJ1Z4QaX9hfaOmejNgFS.data[0m
[38;5;34m2023-12-12_14-38-50_ec2-user_QBS9PEfqZQuqRJ1Z4QaX9hfaOmejNgFS.time[0m
```

Here, we can see all the terminal details of this particular SSH session through our Bastion Host

Benefits/Necessity of Bastion Host

- Bastion hosts can be a valuable resource for companies, improving security and limiting access to shared resources.

- Bastion host provides an additional layer of protection to the actual server (residing in a private subnet) from any external harmful actors on the internet.

- The bastion host processes and filters all incoming traffic and prevents malicious traffic from entering into the network by acting much like a gateway.

- The most common examples of bastion hosts are mail, domain name system, Web and File Transfer Protocol (FTP) servers. Firewalls and routers can also become bastion hosts.

- Bastion hosts (also commonly called bastion servers) are typically configured with a bare minimum operating system with protocol-specific servers such as OpenSSH server or RDP gateway.

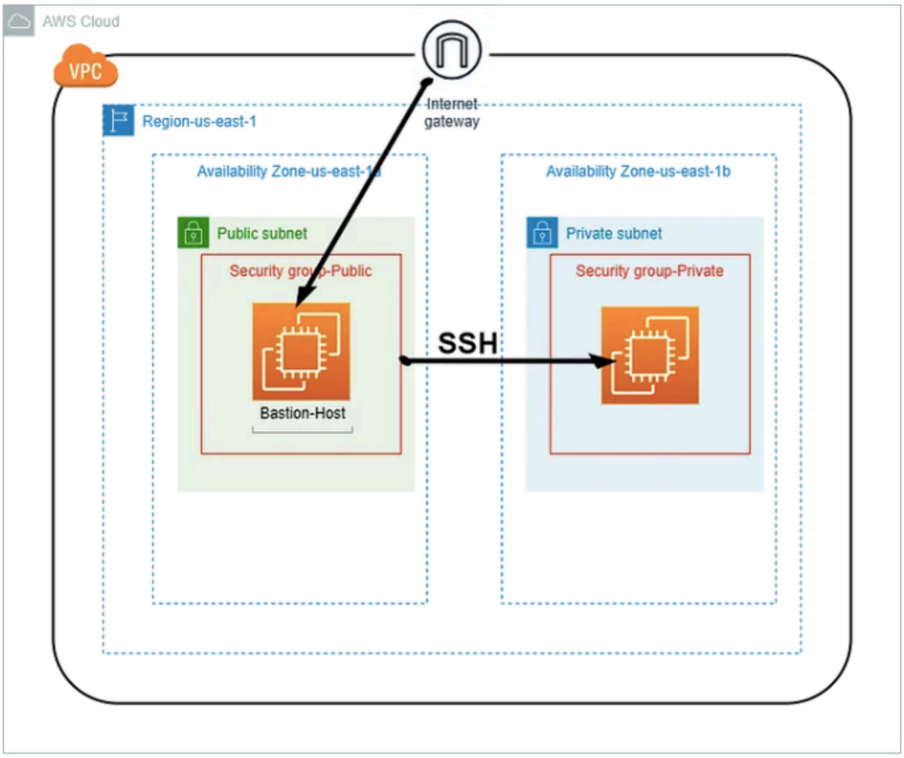
Bastions are not only for SSH!

It is important to mention that Bastions are not only for SSH. Most of the time, people relate to bastion host as an SSH jump server, which is correct but does not cover all use cases. While a Linux server configured with OpenSSH (setup as SSH Jump server) is a typical example of a bastion host, a bastion can sit in front of any protocol. For example, you can use a bastion for database access, RDP access, and internal web application access. In fact, any internal endpoints which should not accept direct network access should be placed behind a bastion for extra security.

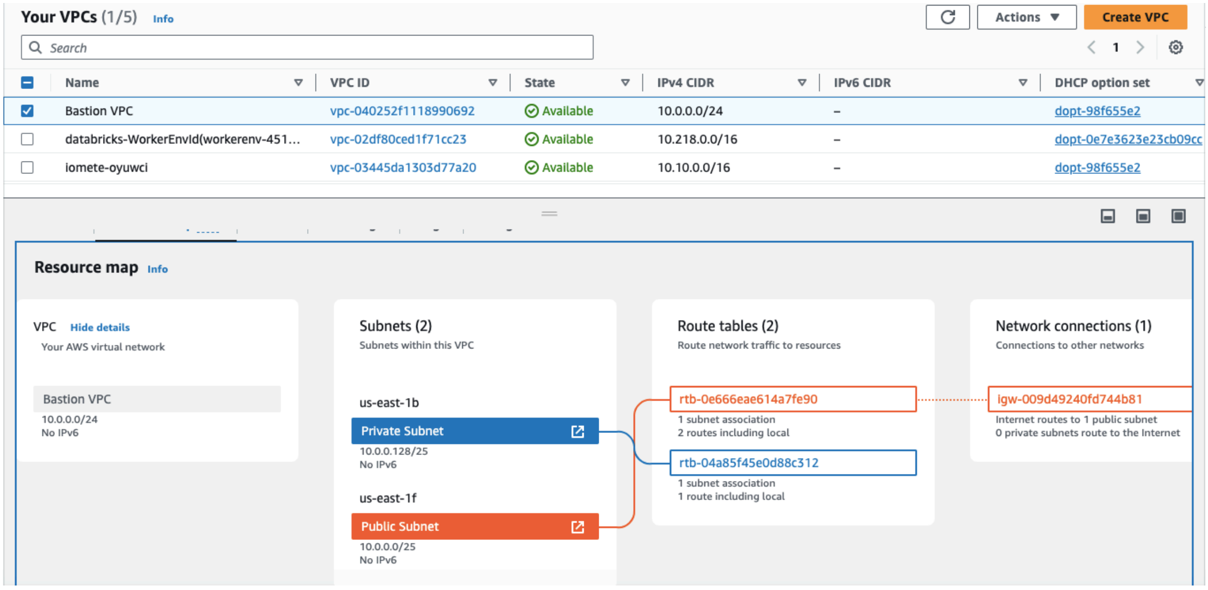
Demo of Bastion Host solution using SSH and AWS console

Bastion Low Level Architecture

AWS Console Implementation: — A AWS diagram explains more than a detailed paragraph.



Setup VPC and subnets



Your VPCs (1/5) Info

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set
☑	Bastion VPC	vpc-040252f1118990692	Available	10.0.0.0/24	–	dopt-98f655e2
□	databricks-WorkerEnvId(workerenv-451...	vpc-02df80ced1f71cc23	Available	10.218.0.0/16	–	dopt-0e7e3623e23cb09cc
□	iomete-oyuwci	vpc-03445da1303d77a20	Available	10.10.0.0/16	–	dopt-98f655e2

Resource map Info

VPC Hide details
Your AWS virtual network
Bastion VPC
10.0.0.0/24
No IPv6

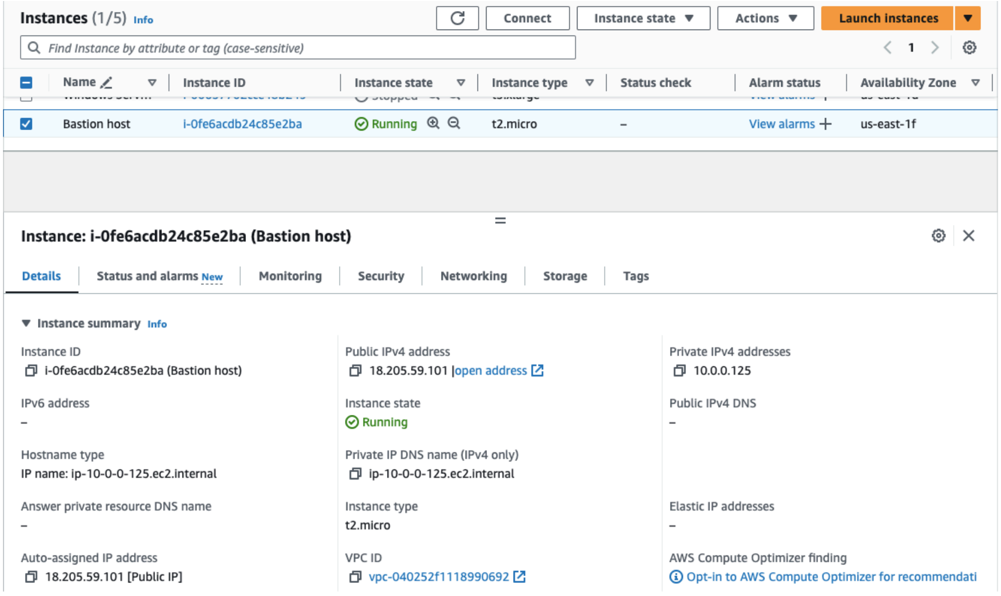
Subnets (2)
Subnets within this VPC
us-east-1b
Private Subnet
10.0.0.128/25
No IPv6
us-east-1f
Public Subnet
10.0.0.0/25
No IPv6

Route tables (2)
Route network traffic to resources
rtb-0e666eae614a7fe90
1 subnet association
2 routes including local
rtb-04a85f45e0d88c312
1 subnet association
1 route including local

Network connections (1)
Connections to other networks
igw-009d49240fd744b81
Internet routes to 1 public subnet
0 private subnets route to the Internet

Bastion host Setup

Network details — Public subnets with route table associated with its project Internet Gateway. For public security group will allow SSH from selected IP address but for this demo it allows from anywhere. Then for the private security group we must allow only the public EC2 instance IP address of the same VPC.



Instances (1/5) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Bastion host	i-0fe6acdb24c85e2ba	Running	t2.micro	–	View alarms +	us-east-1f

Instance: i-0fe6acdb24c85e2ba (Bastion host)

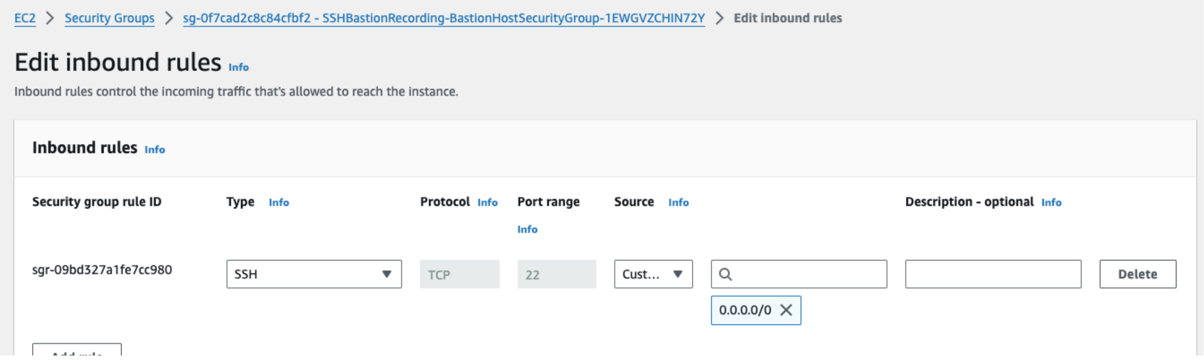
Details | Status and alarms New | Monitoring | Security | Networking | Storage | Tags

Instance summary Info

Instance ID i-0fe6acdb24c85e2ba (Bastion host)	Public IPv4 address 18.205.59.101 |open address	Private IPv4 addresses 10.0.0.125
IPv6 address –	Instance state Running	Public IPv4 DNS –
Hostname type IP name: ip-10-0-0-125.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-0-125.ec2.internal	
Answer private resource DNS name –	Instance type t2.micro	Elastic IP addresses –
Auto-assigned IP address 18.205.59.101 [Public IP]	VPC ID vpc-040252f1118990692	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendati

Figure: Network details of Bastion host

Bastion- Security Group



EC2 > Security Groups > sg-0f7cad2c8c84cfbf2 - SSHBastionRecording-BastionHostSecurityGroup-1EWGVZCHIN72Y > Edit inbound rules

Edit inbound rules Info

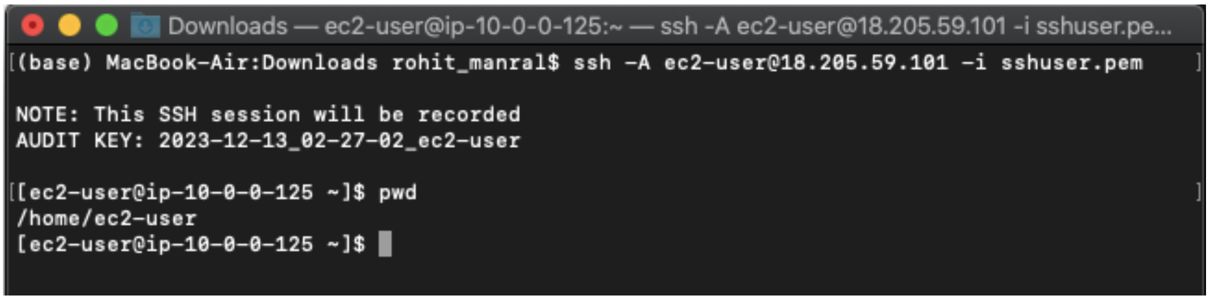
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-09bd327a1fe7cc980	SSH	TCP	22	Cust...	0.0.0.0/0		Delete

Connect to Bastion host

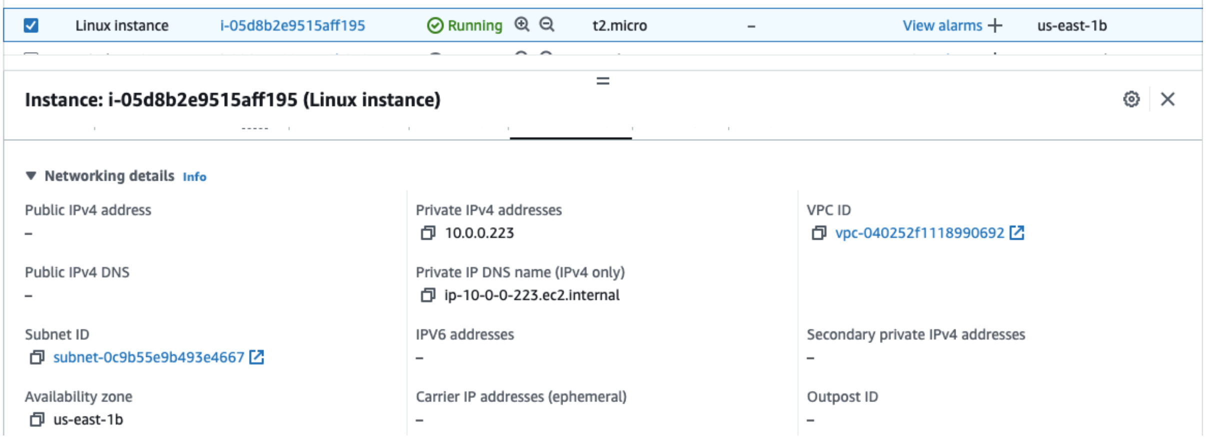
I used Mac Terminal to connect.


Downloads — ec2-user@ip-10-0-0-125:~ — ssh -A ec2-user@18.205.59.101 -i sshuser.pe...

```
[(base) MacBook-Air:Downloads rohit_manral$ ssh -A ec2-user@18.205.59.101 -i sshuser.pem

NOTE: This SSH session will be recorded
AUDIT KEY: 2023-12-13_02-27-02_ec2-user

[[ec2-user@ip-10-0-0-125 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-0-125 ~]$ 
```

Private EC2 Setup

Creating the Private EC2 instance with Project VPC and the private subnet.



☑ Linux instance i-05d8b2e9515aff195 Running t2.micro – View alarms + us-east-1b

Instance: i-05d8b2e9515aff195 (Linux instance)

Networking details Info

Public IPv4 address
–

Public IPv4 DNS
–

Subnet ID
subnet-0c9b55e9b493e4667

Availability zone
us-east-1b

Private IPv4 addresses
10.0.0.223

Private IP DNS name (IPv4 only)
ip-10-0-0-223.ec2.internal

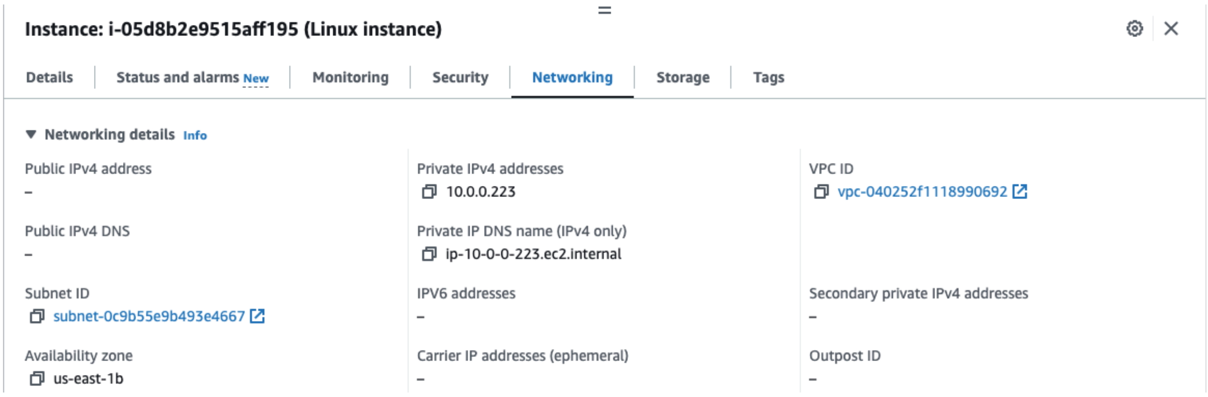
IPV6 addresses
–

Carrier IP addresses (ephemeral)
–

VPC ID
vpc-040252f1118990692

Secondary private IPv4 addresses
–

Outpost ID
–



Instance: i-05d8b2e9515aff195 (Linux instance)

Networking details Info

Public IPv4 address
–

Public IPv4 DNS
–

Subnet ID
subnet-0c9b55e9b493e4667

Availability zone
us-east-1b

Private IPv4 addresses
10.0.0.223

Private IP DNS name (IPv4 only)
ip-10-0-0-223.ec2.internal

IPV6 addresses
–

Carrier IP addresses (ephemeral)
–

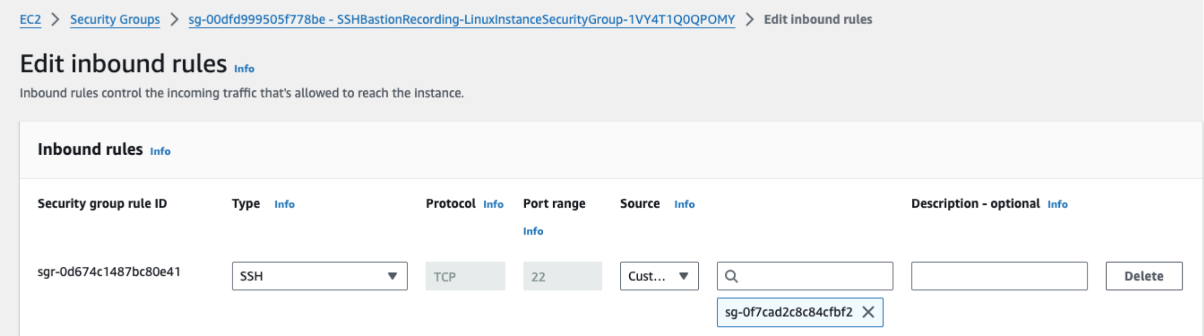
VPC ID
vpc-040252f1118990692

Secondary private IPv4 addresses
–

Outpost ID
–

Yes, we are all done with the setup of private EC2 instance, now let's connect to the instance from Bastion Host instance.

Private Linux- Security Group



EC2 > Security Groups > sg-00dfd999505f778be - SSHBastionRecording-LinuxInstanceSecurityGroup-1VY4T1Q0QPOMY > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0d674c1487bc80e41	SSH	TCP	22	Cust...	sg-0f7cad2c8c84cfbf2		Delete

Steps to connect through the Bastion Host into Private EC2 instance.

1. Connect to Bastion host first by ssh.

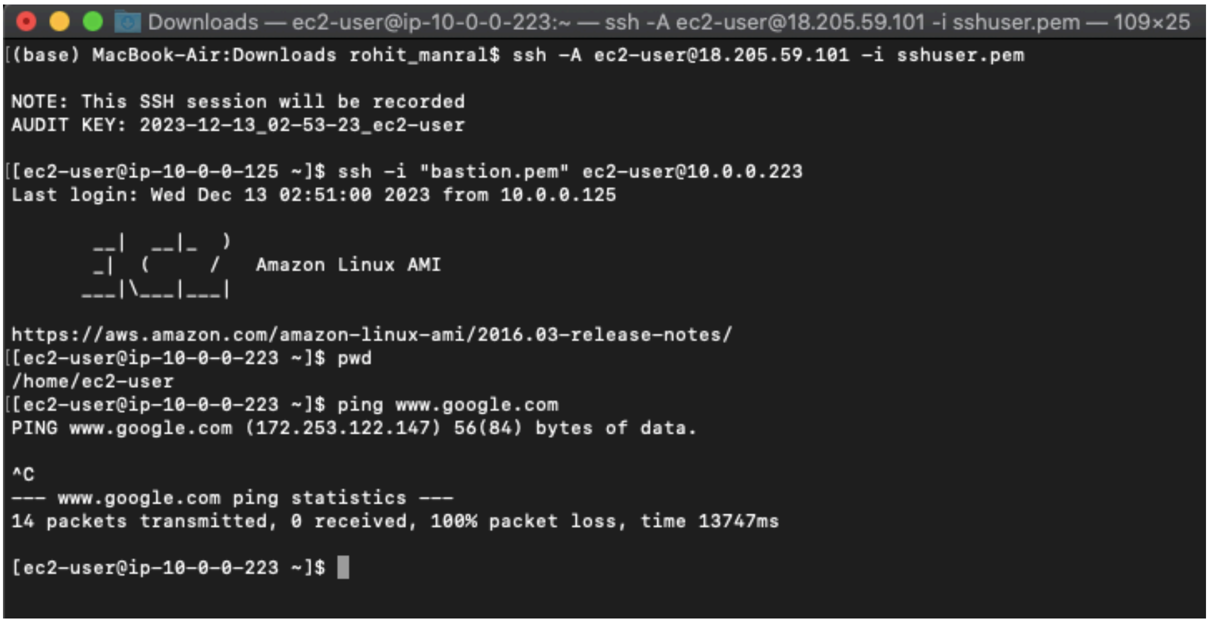
2. Once you're in-Bastion host. Copy your already created key pair for Bastion host.

3. now use nano or vim to create filename-keypair.pem, then paste the copied key into file, save and exit.

4. change permission to the created keypair by using $ chmod 400 <keypair>

5. use the cmd -> ssh -i “Filename-KeyPair.pem” username@Private_IP_address

It's done, connected to the bastion host!



Downloads — ec2-user@ip-10-0-0-223:~ — ssh -A ec2-user@18.205.59.101 -i sshuser.pem — 109×25

```
[(base) MacBook-Air:Downloads rohit_manral$ ssh -A ec2-user@18.205.59.101 -i sshuser.pem

 NOTE: This SSH session will be recorded
 AUDIT KEY: 2023-12-13_02-53-23_ec2-user

[[ec2-user@ip-10-0-0-125 ~]$ ssh -i "bastion.pem" ec2-user@10.0.0.223
 Last login: Wed Dec 13 02:51:00 2023 from 10.0.0.125

        __|  __|_  )
        _|  (     /   Amazon Linux AMI
       ___|\___|___|

 https://aws.amazon.com/amazon-linux-ami/2016.03-release-notes/
[[ec2-user@ip-10-0-0-223 ~]$ pwd
 /home/ec2-user
[[ec2-user@ip-10-0-0-223 ~]$ ping www.google.com
 PING www.google.com (172.253.122.147) 56(84) bytes of data.

 ^C
 --- www.google.com ping statistics ---
 14 packets transmitted, 0 received, 100% packet loss, time 13747ms

 [ec2-user@ip-10-0-0-223 ~]$ 
```

Finally, it worked and verified if the private instance has internet access by using ping. I hope this short article is useful, this is going to be useful for myself for future references.

Any Questions?

References

⇒ https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/

⇒ https://www.strongdm.com/blog/bastion-hosts-ssh-logging

⇒ https://www.ezeelogin.com/blog/how-to-record-terminal-ssh-sessions/

⇒ https://www.youtube.com/watch?v=dyVfnzUy2ys