

Placement Empowerment Program

Cloud Computing and DevOps Centre

Secure Access with a Bastion Host Set up a bastion host in a public subnet to securely access instances in a private subnet.

Name: CHANDRU S

Department: INFORMATION TECHNOLOGY

Introduction

In cloud environments, securing access to private instances is essential. A **Bastion Host** (also known as a **Jump Box**) acts as a secure gateway to access **EC2 instances in a private subnet**. Instead of exposing private instances directly to the internet, users first connect to the Bastion Host, which then allows access to the private instances.

This setup enhances security by **restricting direct SSH access**, enforcing **strict security controls**, and reducing exposure to potential threats.

Overview

In this guide, we will set up a Bastion Host in a public subnet to provide controlled SSH access to instances inside a private subnet.

What We Will Do

1. Create a VPC with Public and Private subnets.
2. Set up a Bastion Host in the Public Subnet.
3. Launch a Private EC2 Instance in the Private Subnet.
4. Configure secure SSH access via the Bastion Host.
5. Enhance security by restricting SSH access and considering AWS Systems Manager (SSM) as an alternative.

Step-by-Step Overview

Step 1: Create a VPC with Public and Private Subnets

1.1 Create a VPC

- Open the [AWS Management Console](#) → Navigate to **VPC Dashboard**.

- Click Create VPC and name it **my_vpc**.
- Set **IPv4 CIDR Block**: 10.0.0.0/16.
- Click **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 Info
Creates a tag with a key of 'Name' and a value that you specify.

my_vpc

IPv4 CIDR block Info
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
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

Tenancy Info
Default

Tags Info
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
Name my_vpc Remove tag

Add tag

You can add 49 more tags.

Cancel Preview code Create 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

Endpoints Updated

Endpoint services

Service networks Updated

VPC details Info

Details Info

VPC ID vpc-0f58aa06f22820522

State Available

Block Public Access Off

DNS hostnames Disabled

DNS resolution Enabled

Tenancy default

DHCP option set dopt-090e3f629a763f52e

Main network ACL acl-0d670084bf12066c

IPv6 CIDR (Network border group) -

Default VPC No

Network Address Usage metrics Disabled

IPv4 CIDR 10.0.0.0/16

Route 53 Resolver DNS Firewall rule groups -

Main route table rtb-089f0292009eb81d9

Owner ID 463470937078

Resource map Info

VPC Show details
Your AWS virtual network
my_vpc

Subnets (0)
Subnets within this VPC

Route tables (1)
Route network traffic to resources
rtb-089f0292009eb81d9

Network connections (0)
Connections to other networks

1.2 Create a Public Subnet

- Go to Subnets → Create Subnet.
- Select **my_vpc** and set **CIDR block**: 10.0.1.0/24.
- Enable **Auto-Assign Public IP**.

aws [Search] [Alt+S] Asia Pacific (Mumbai) Chandru S

VPC > Subnets > Create subnet

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-0f58aa06f22820522 (my_vpc)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

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

public_sub

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.

Asia Pacific (Mumbai) / ap-south-1a

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.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.1.0/24 256 IPs

Tags - optional

Key	Value - optional
Q Name	Q public_sub (Remove)

aws [Search] [Alt+S] Asia Pacific (Mumbai) Chandru S

VPC > Subnets > subnet-0e8af461161d706fc > Edit subnet settings

Edit subnet settings [Info](#)

Subnet

Subnet ID
subnet-0e8af461161d706fc

Name
public_sub

Auto-assign IP settings [Info](#)

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

☒ Enable auto-assign public IPv4 address [Info](#)

☐ Enable auto-assign customer-owned IPv4 address [Info](#)
Option disabled because no customer-owned pools found.

Resource-based name (RBN) settings [Info](#)

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

☐ Enable resource name DNS A record on launch [Info](#)

☐ Enable resource name DNS AAAA record on launch [Info](#)

Hostname type [Info](#)

☐ Resource name

☒ IP name

DNS64 settings

Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

☐ Enable DNS64 [Info](#)

Cancel Save

1.3 Create a Private Subnet

- Repeat the same process, but set **CIDR block**: 10.0.2.0/24.
- **Do not enable Auto-Assign Public IP.**

aws [Search] [Alt+S] Asia Pacific (Mumbai) Chandru S

VPC > Subnets > Create subnet

Create subnet

VPC

VPC ID
Create subnets in this VPC
vpc-0f58aa06f22820522 (my_vpc)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private_sub
The name can be up to 256 characters long.

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Mumbai) / ap-south-1b

IPv4 VPC CIDR block
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.2.0/24 256 IPs

Tags - optional

Key Value - optional
Name private_sub Remove

aws [Search] [Alt+S] Asia Pacific (Mumbai) Chandru S

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

You have successfully created 1 subnet: subnet-0ad96ccae6cda1ed0

Subnets (1)

Find resources by attribute or tag

Subnet ID: subnet-0ad96ccae6cda1ed0 Clear filters

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CI
<input type="checkbox"/>	private_sub	subnet-0ad96ccae6cda1ed0	Available	vpc-0f58aa06f22820522 my_...	Off	10.0.2.0/24	-	-

Step 2: Configure Public Subnet for Internet Access

2.1 Create an Internet Gateway (IGW)

- Go to Internet Gateways → Click Create Internet Gateway.
- Name it **my_gate**, attach it to **my_vpc**.

aws [Search] [Alt+S] Asia Pacific (Mumbai) Chandru S

VPC > Internet gateways > igw-0f850cb4177cea432

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

igw-0f850cb4177cea432 / my_gate

Details

Internet gateway ID
igw-0f850cb4177cea432

State
Attached

VPC ID
vpc-0f58aa06f22820522 | my_vpc

Owner
463470937078

Tags

Search tags

Key	Value
Name	my_gate

2.2 Update Public Route Table

- Go to Route Tables → Create Route Table → Name it **my_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** [Remove](#)

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

[Cancel](#) [Create route table](#)

- Associate it with **PublicSubnet**.
- Add a route:
 - Destination: **0.0.0.0/0**
 - Target: Internet Gateway (**my_gate**)

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="Internet Gateway"/>	-	No

[Add route](#) [Remove](#)

[Cancel](#) [Preview](#) [Save changes](#)

Updated routes for rtb-0c7ff3e3206563483 / my_table successfully

rtb-0c7ff3e3206563483 / my_table [Actions](#)

Details

Route table ID: [rtb-0c7ff3e3206563483](#)
VPC: [vpc-0f58aa06f22820522 \(my_vpc\)](#)
Main: No
Owner ID: [463470937078](#)

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f850cb4177cea432	Active	No
10.0.0.0/16	local	Active	No

Step 3: Launch a Bastion Host in the Public Subnet

1. Go to **EC2 Dashboard** → Launch Instance.
2. Select **Amazon Linux 2 (or Ubuntu)**.

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: [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.

Recents **Quick Start**

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible

ami-0c50b6f7dc3701ddd (64-bit (x86), uefi-preferred) / ami-098a9403eae2749f1 (64-bit (Arm), uefi)
Virtualization: hvm ENA-enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20250203.1 x86_64 HVM kernel-6.1

Architecture **Boot mode** **AMI ID** **Username**

64-bit (x86) uefi-preferred ami-0c50b6f7dc3701ddd ec2-user Verified provider

Summary

Number of instances:

Software Image (AMI)

Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-0c50b6f7dc3701ddd

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#) [Launch instance](#) [Preview code](#)

3. Choose **t2.micro** (Free Tier Eligible).
4. Place it in **PublicSubnet** with Auto-Assign Public IP **enabled**.

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

Instance type: **t2.micro** Free tier eligible [Compare instance types](#)

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

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](#)

Network settings [Info](#)

VPC - required: [Create new VPC](#)

Subnet: [Create new subnet](#)

Auto-assign public IP: ☒ Enable

Firewall (security groups) [Info](#)

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

☒ Create security group ☐ Select existing security group

Security group name - required:

Summary

Number of instances:

Software Image (AMI)

Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-0c50b6f7dc3701ddd

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#) [Launch instance](#) [Preview code](#)

5. Create a Security Group (**BastionSG**):
 - Allow **SSH** (Port 22) from **Your IP** (xx.xx.xx.xx/32).
6. Create or use an existing key pair (e.g., **bastion-key.pem**).
7. Click **Launch**.

Description - required Info
Launch-wizard-1 created 2025-02-07T05:54:54Z02

Inbound Security Group Rules
▼ Security group rule 1 (TCP: 22, 182.74.154.218/32) Remove

Type	Protocol	Port range
ssh	TCP	22

Source type: My IP
Name: Add CIDR, prefix list or security group
Description - optional: eg. SSH for admin desktop
182.74.154.218/32

Add security group rule

► Advanced network configuration

▼ Configure storage Info Advanced
1x 8 GB gp3 Root volume 3000 IOPS (Not encrypted)

Free tier eligible customers can get up to 30 GiB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

► Advanced details Info

▼ Summary
Number of instances: 1 Info

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c50b6f7dc3701ddc

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel Launch Instance Preview code

Step 4: Launch a Private EC2 Instance

1. Go to EC2 Dashboard → Launch Instance.
2. Choose Amazon Linux 2 (or Ubuntu).

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: my_ec2pri 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

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

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

Amazon Machine Image (AMI)
Amazon Linux 2023 AMI
ami-0c50b6f7dc3701ddc (64-bit (x86), uefi-preferred) / ami-098a9400eac2749f1 (64-bit (Arm), uefi)
Virtualization: hvm EBS enabled: true Root device type: ebs Free tier eligible

Description
Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20250203.1 x86_64 HVM kernel-6.1

Architecture: 64-bit (x86) Boot mode: uefi-preferred AMI ID: ami-0c50b6f7dc3701ddc Username: ec2-user Verified provider

▼ Summary
Number of instances: 1 Info

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c50b6f7dc3701ddc

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel Launch Instance Preview code

3. Choose t2.micro and place it in **PrivateSubnet**.
4. **Disable** Auto-Assign Public IP.

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

☒ All generations [Compare instance types](#)

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: AK [Create new key pair](#)

Network settings [Info](#)

VPC - required [Info](#): vpc-0f58aa06f22820522 (my_vpc) 10.0.0.0/16

Subnet [Info](#): subnet-0d96ccae6cda1ed0 private_sub
VPC: vpc-0f58aa06f22820522 Owner: 463470937078 Availability Zone: ap-south-1b Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24 [Create new subnet](#)

Auto-assign public IP [Info](#): Disable

Firewall (security groups) [Info](#): Create security group ☒ Select existing security group ☐

Security group name - required: launch-wizard-2
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 _-./[!@#%^&*()+=~`{|}~].

Summary

Number of instances [Info](#): 1

Software Image (AMI) [Info](#): Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c50b6f7dc370168d

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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

[Cancel](#) [Launch instance](#) [Preview code](#)

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

5. Create a Security Group (**PrivateSG**):
 - Allow **SSH** (Port 22) only from **Bastion Host's** Security Group.
6. Use the same key pair (bastion-key.pem).

Description - required [Info](#): launch-wizard-2 created 2025-02-07T05:57:55.474Z

Inbound Security Group Rules

Security group rule 1 (TCP: 22, 182.74.154.218/32) [Remove](#)

Type [Info](#): ssh Protocol [Info](#): TCP Port range [Info](#): 22

Source type [Info](#): My IP Name [Info](#): 182.74.154.218/32 Description - optional [Info](#): e.g. SSH for admin desktop

[Add security group rule](#)

Configure storage [Info](#) [Advanced](#)

1x 8 GiB gp3 Root volume 3000 IOPS (Not encrypted)

[Free tier eligible customers can get up to 30 GiB of EBS General Purpose \(SSD\) or Magnetic storage](#) [X](#)

[Add new volume](#)

[Click refresh to view backup information](#) [Refresh](#)
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

[Advanced details](#) [Info](#)

Summary

Number of instances [Info](#): 1

Software Image (AMI) [Info](#): Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c50b6f7dc370168d

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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

[Cancel](#) [Launch instance](#) [Preview code](#)

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

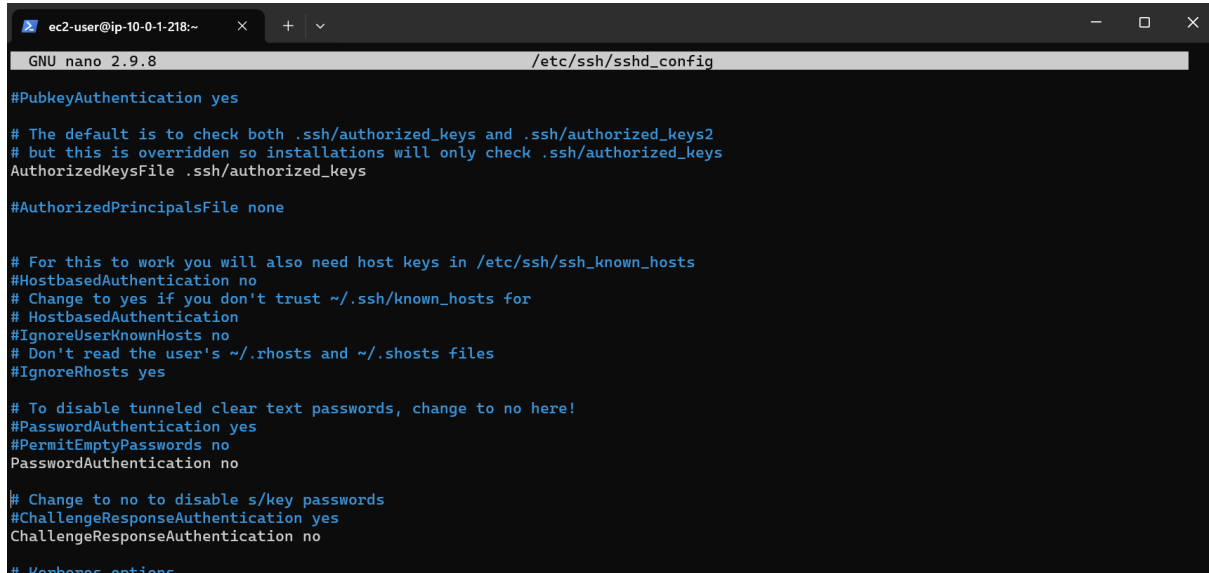
7. Click Launch.

PasswordAuthentication no

PermitRootLogin no

3. Restart SSH service:

sudo systemctl restart sshd



```
ec2-user@ip-10-0-1-218:~  
GNU nano 2.9.8 /etc/ssh/sshd_config  
#PubkeyAuthentication yes  
# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2  
# but this is overridden so installations will only check .ssh/authorized_keys  
AuthorizedKeysFile .ssh/authorized_keys  
#AuthorizedPrincipalsFile none  
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts  
#HostbasedAuthentication no  
# Change to yes if you don't trust ~/.ssh/known_hosts for  
# HostbasedAuthentication  
#IgnoreUserKnownHosts no  
# Don't read the user's ~/.rhosts and ~/.shosts files  
#IgnoreRhosts yes  
# To disable tunneled clear text passwords, change to no here!  
#PasswordAuthentication yes  
#PermitEmptyPasswords no  
PasswordAuthentication no  
# Change to no to disable s/key passwords  
#ChallengeResponseAuthentication yes  
ChallengeResponseAuthentication no  
# Krb5 options
```

Step 7: Alternative - Use AWS Systems Manager (SSM) Instead of SSH

- Attach **AmazonSSMManagedInstanceCore** IAM policy to the EC2 instance role.
- Ensure the **SSM Agent** is enabled (pre-installed on Amazon Linux & Ubuntu).
- Use **AWS Systems Manager > Session Manager** to connect without SSH.

Conclusion

Using a Bastion Host improves security by acting as a controlled access point for private instances. It prevents direct internet exposure, enforces security group rules, and allows monitoring/logging of access attempts.

For even stronger security, consider eliminating SSH access entirely and using AWS Systems Manager (SSM) Session Manager instead.