

Project: Segregation of Management Traffic via VPC Peering in AWS

Description:

Designed and implemented a secure network architecture using Amazon VPC Peering to isolate management traffic from application traffic. This separation enhanced security by enforcing network segmentation, reduced the risk of lateral movement in case of a breach, and optimized traffic flow between critical infrastructure components. The solution involved:

- Creating separate VPCs for management and application layers
- Establishing VPC Peering connections with controlled route table propagation
- Implementing strict security group to enforce least privilege access
- Monitoring and validating traffic flows using VPC Flow Logs

Goal:

Create two VPCs:

VPC-A (Management VPC)

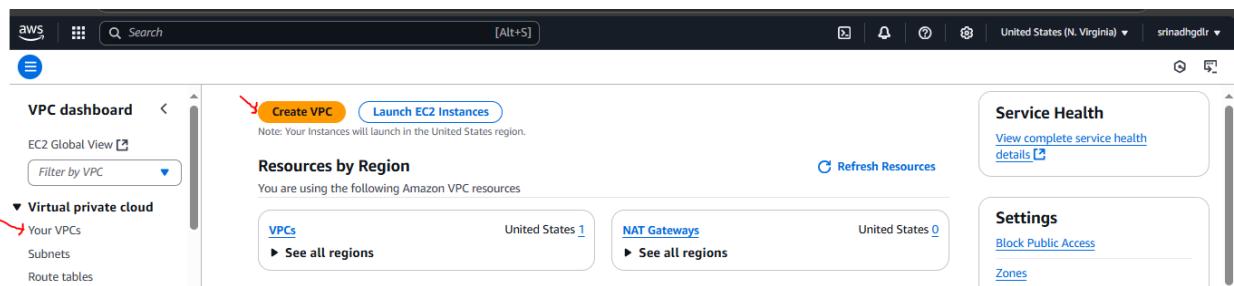
VPC-B (Application VPC)

Then, establish a VPC Peering Connection between them to allow controlled communication, maintaining traffic separation.

Implementation Steps

Step 1: Create VPC-A (Management VPC)

1. In the AWS Console, Go to **VPC Console** → **Your VPCs** → **Create VPC**
2. Choose **VPC only**
3. Fill in:
 - **Name tag:** Management-VPC
 - **IPv4 CIDR block:** 10.0.0.0/16
 - Leave the rest default
4. 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.

**Name tag - optional**

Creates a tag with a key of 'Name' and a value that you specify.

Management-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

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

Name

Value - optional

Management-VPC



You can add 49 more tags

**VPC dashboard**

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

You successfully created vpc-0d67c9cd66e84856c / Management-VPC

vpc-0d67c9cd66e84856c / Management-VPC**Details** Info

VPC ID

vpc-0d67c9cd66e84856c

State

Available

Block Public Access

Off

DNS hostnames

Disabled

DNS resolution

Enabled

DHCP option set

dopt-0ab5c96a33ae0222f

Main route table

rtb-0da9ca1e067a2141b

Main network ACL

acl-03e2c46853b79bab

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

-

Owner ID

284514300790

- From the Management-VPC Actions drop down, select Edit VPC settings and Enable DNS hostnames in DNS Settings

The screenshot shows the AWS VPC console with the 'Management-VPC' selected. The 'Details' tab is active. A red arrow points to the 'DNS hostnames' section, which is set to 'Enabled'. Other visible settings include VPC ID (vpc-0d67c9cd6e84856c), State (Available), Block Public Access (Off), and Main route table (rtb-0da9ca1e067a2141b).

VPC ID	State	Block Public Access	DNS hostnames
vpc-0d67c9cd6e84856c	Available	Off	Enabled

Step 2: Create VPC-B (Application VPC)

- Go to **VPC Console** → **Your VPCs** → **Create VPC**
- Choose **VPC only**
- Fill in:
 - Name tag:** Application-VPC
 - IPv4 CIDR block:** 192.38.0.0/16
 - Keep default settings
- Click **Create VPC**

The screenshot shows the AWS VPC dashboard with the 'Your VPCs' list. A red arrow points to the 'Create VPC' button in the top right corner of the list table.

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
-	vpc-0f982f9178eb91a4f	Available	Off	172.31.0.0/16	-
Management-VPC	vpc-0d67c9cd6e84856c	Available	Off	10.0.0.0/16	-

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.

Application-VPC

IPv4 CIDR block Info

- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block

IPv4 CIDR

192.38.0.0/16

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

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

Name

Value - optional

Application-VPC

[Remove tag](#)[Add tag](#)

You can add 49 more tags

[Cancel](#)[Preview code](#)[Create VPC](#)

You successfully created vpc-027cdfe62d7267514 / Application-VPC

vpc-027cdfe62d7267514 / Application-VPC

Details <small>Info</small>			
VPC ID vpc-027cdfe62d7267514	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-0ab5c96a33ae022f	Main route table rtb-000971ed61159c69f
Main network ACL acl-058b174c63ebc43ab	Default VPC No	IPv4 CIDR 192.38.0.0/16	IPv6 pool -
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 284514300790

- From the Application-VPC Actions drop down, select Edit VPC settings and Enable DNS hostnames in DNS Settings

Your VPCs (1/3) Info

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
Application-VPC	vpc-027ccfe62d7267514	Available	Off	192.38.0.0/16	-
-	vpc-0f982f9178eb91a4f	Available	Off	172.31.0.0/16	-

Details

VPC ID vpc-027ccfe62d7267514	State Available	Block Public Access Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-0ab5c96a33ae0222f	Main route table rtb-000971ed61159c69f
Main network ACL acl-058b174c63ebc43ab	Default VPC No	IPv4 CIDR 192.38.0.0/16	IPv6 pool -
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 284514300790

Step 3: Create Subnets in Each VPC

- In the VPC Dashboard Go to **Subnets** → **Create Subnet**
- Select Management-VPC
 - Name: Management-Subnet
 - AZ: Choose us-east-1a
 - CIDR block: 10.0.1.0/24

Subnets (6) Info

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-076f0f5174b0ac6b6	Available	vpc-0f982f9178eb91a4f	Off	172.31.0
-	subnet-0fd4378f1620ca82a	Available	vpc-0f982f9178eb91a4f	Off	172.31.4
-	subnet-0cb926956dd951379	Available	vpc-0f982f9178eb91a4f	Off	172.31.6
-	subnet-093c7d1039efc1ff6	Available	vpc-0f982f9178eb91a4f	Off	172.31.3
-	subnet-0c5aa83413bd06ff2	Available	vpc-0f982f9178eb91a4f	Off	172.31.1

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

vpc-0d67c9cd66e84856c (Management-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.

Management-Subnet

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.

United States (N. Virginia) / us-east-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

Tags - optional

Add new subnet

Cancel **Create subnet**

Subnets (1) <small>Info</small>						
You have successfully created 1 subnet: subnet-085cd32eb9c9b0834						
Last updated	less than a minute ago	Actions	Create subnet			
Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	
Management-Subnet	subnet-085cd32eb9c9b0834	Available	vpc-0d67c9cd66e84856c Man...	Off	10.0.1.0/24	

3. Create the subnet for Application-VPC

- Name: Application-Subnet
- AZ: Choose us-east-1a
- CIDR block: 192.38.1.0/24

The screenshot shows the AWS VPC Subnets list page. A red arrow points from the left sidebar to the 'Subnets' link under the 'Virtual private cloud' section. Another red arrow points to the 'Create subnet' button at the top right of the list table.

Subnets (1) <small>Info</small>						
Last updated 7 minutes ago <small>C</small> Actions <small>▼</small> Create subnet						
Find resources by attribute or tag						
Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	
Management-Subnet	subnet-085cd32eb9c9b0834	Available	vpc-0d67c9cd66e84856c Man...	Off	10.0.1.0/24	

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-027cdfe62d7267514 (Application-VPC)

Associated VPC CIDRs

IPv4 CIDRs
192.38.0.0/16

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.

Application-Subnet

The name can be up to 256 characters long.

Availability Zone Info

Availability Zone Info

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

United States (N. Virginia) / us-east-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.

192.38.0.0/16

IPv4 subnet CIDR block

192.38.1.0/24

Tags - optional

Key

Name

Value - optional

Application-Subnet

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create subnet

The screenshot shows the AWS VPC Subnets list page after creating a new subnet. A green success message at the top states: "You have successfully created 1 subnet: subnet-0c174e12ec924ce46". A red arrow points to this message. Another red arrow points to the 'Create subnet' button at the top right of the list table.

Subnets (1) <small>Info</small>						
Last updated less than a minute ago <small>C</small> Actions <small>▼</small> Create subnet						
Find resources by attribute or tag						
Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	
Application-Subnet	subnet-0c174e12ec924ce46	Available	vpc-027cdfe62d7267514 Appl...	Off	192.38.1.0/24	

Step 4: Create Internet Gateways

1. Go to **Internet Gateways** → **Create Internet Gateway**
2. Name: Management-IGW, click on Create internet gateway
3. From the Actions drop down choose Attach to VPC and select Management-VPC
4. Repeat the above three steps for Application-VPC

Internet Gateway (Management-IGW) for Management-VPC

VPC dashboard < Internet gateways (1) Info

Actions **Create internet gateway**

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-05c7588c4bbc24bd9	Attached	vpc-0f982f9178eb91a4f	284514300790

VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

Management-IGW

Tags - optional

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 internet gateway**

VPC dashboard < Internet gateways > igw-0856f89c762c89f30

The following internet gateway was created: igw-0856f89c762c89f30 - Management-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet. **Attach to a VPC**

igw-0856f89c762c89f30 / Management-IGW

Details Info

Internet gateway ID: igw-0856f89c762c89f30 | State: Detached | VPC ID: - | Owner: 284514300790

Tags

Search tags

Key	Value
Name	Management-IGW

Actions ▾

- Attach to VPC
- Detach from VPC
- Manage tags
- Delete

Manage tags

VPC > Internet gateways > Attach to VPC (igw-0856f89c762c89f30)

Attach to VPC (igw-0856f89c762c89f30) Info

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 X

▶ AWS Command Line Interface command

Cancel **Attach internet gateway**

VPC dashboard < X

EC2 Global View Actions ▾

Filter by VPC ▾

Virtual private cloud Actions ▾

Your VPCs
Subnets
Route tables

Internet gateways Actions ▾

Egress-only internet gateways
Carrier gateways
DHCP option sets

igw-0856f89c762c89f30 / Management-IGW

Details Info

Internet gateway ID <input type="text" value="igw-0856f89c762c89f30"/>	State Attached	VPC ID <input type="text" value="vpc-0d67c9cd66e84856c Management-VPC"/>	Owner <input type="text" value="284514300790"/>				
Tags							
<input type="text" value="Search tags"/> <table border="1"> <tr> <th>Key</th> <th>Value</th> </tr> <tr> <td>Name</td> <td>Management-IGW</td> </tr> </table> Manage tags				Key	Value	Name	Management-IGW
Key	Value						
Name	Management-IGW						

Tags

Search tags

Key | Value

Name Management-IGW

Internet Gateway (Application-IGW) for Application-VPC

VPC dashboard < Actions ▾ **Create internet gateway**

EC2 Global View Actions ▾

Filter by VPC ▾

Virtual private cloud Actions ▾

Your VPCs
Subnets
Route tables

Internet gateways Actions ▾

Internet gateways (2) Info

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-05c7588c4bbc24bd9	Attached	vpc-0f982f9178eb91a4f	284514300790
Management-IGW	igw-0856f89c762c89f30	Attached	vpc-0d67c9cd66e84856c Managemen...	284514300790

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

Application-IGW

Tags - optional
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 internet gateway**

The following internet gateway was created: igw-0c69a5a72c14db090 - Application-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

igw-0c69a5a72c14db090 / Application-IGW

Details [Info](#)

Internet gateway ID igw-0c69a5a72c14db090	State Detached	VPC ID -	Owner 284514300790
--	-------------------	-------------	-----------------------

Tags

Search tags	
Key	Value
Name	Application-IGW

Actions ▾

- [Attach to VPC](#)
- [Detach from VPC](#)
- [Manage tags](#)
- [Delete](#)

[VPC](#) > [Internet gateways](#) > Attach to VPC (igw-0c69a5a72c14db090) [Info](#)

Attach to VPC (igw-0c69a5a72c14db090)

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.

[X](#)

[▶ AWS Command Line Interface command](#)

[Cancel](#) [Attach internet gateway](#)

[VPC dashboard](#) <

The following internet gateway was created: igw-0c69a5a72c14db090 successfully attached to vpc-027cdfe62d7267514

igw-0c69a5a72c14db090 / Application-IGW

Details [Info](#)

Internet gateway ID igw-0c69a5a72c14db090	State Attached	VPC ID vpc-027cdfe62d7267514 Application-VPC	Owner 284514300790
--	-------------------	---	-----------------------

Tags

Search tags	
Key	Value
Name	Application-IGW

Actions ▾

Step 5: Create VPC Peering Connection

1. In the VPC Dashboard, Go to **Peering Connections** → **Create Peering Connection**
2. Name tag: Management-Application-Peering
3. Requester VPC: Management-VPC
4. Acceptor VPC: Application-VPC (same account)
5. Click **Create Peering Connection**
6. Go back → Select the connection → Click **Actions** → **Accept request**

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections**

Peering connections Info

No peering connection found

Create peering connection

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Info

Peering connection settings

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

Management-Application-Peering

Select a local VPC to peer with

VPC ID (Requester)
vpc-0d67c9cd66e84856c (Management-VPC)

VPC CIDRs for vpc-0d67c9cd66e84856c (Management-VPC)

CIDR	Status	Status reason
10.0.0.0/16	Associated	-

Select another VPC to peer with

Account
 My account
 Another account

Region

This Region (us-east-1)
 Another Region

VPC ID (Acceptor)
vpc-027cdf62d7267514 (Application-VPC)

VPC CIDRs for vpc-027cdf62d7267514 (Application-VPC)

CIDR	Status	Status reason
192.38.0.0/16	Associated	-

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.

Create peering connection

VPC > Peering connections > pcx-01320dd221914ce5d

A VPC peering connection pcx-01320dd221914ce5d / Management-Application-Peering has been requested.

pcx-01320dd221914ce5d / Management-Application-Peering

Pending acceptance
You can accept or reject this peering connection request using the 'Actions' menu. You have until Friday, April 11, 2025 at 11:37:03 GMT+1 to accept or otherwise it expires.

Accept request (highlighted with a red arrow)

Actions ▾

Details **Info**

Requester owner ID 284514300790	Acceptor owner ID 284514300790	VPC Peering connection ARN arn:aws:ec2:us-east-1:284514300790:vpc-peering-connection/pcx-01320dd221914ce5d
Peering connection ID pcx-01320dd221914ce5d	Requester VPC vpc-0d67c9cd66e84856c / Management-VPC	Acceptor VPC vpc-027cdfe62d7267514 / Application-VPC
Status Pending Acceptance by 284514300790	Requester CIDRs 10.0.0.0/16	Acceptor CIDRs -
Expiration time Friday, April 11, 2025 at 11:37:03 GMT+1	Requester Region N. Virginia (us-east-1)	Acceptor Region N. Virginia (us-east-1)

DNS | **Route tables** | **Tags**

Accept VPC peering connection request [Info](#)

Are you sure you want to accept this VPC peering connection request? (pcx-01320dd221914ce5d / Management-Application-Peering)

Requester VPC vpc-0d67c9cd66e84856c / Management-VPC	Acceptor VPC vpc-027cdfe62d7267514 / Application-VPC	Requester CIDRs 10.0.0.0/16
Acceptor CIDRs -	Requester Region N. Virginia (us-east-1)	Acceptor Region N. Virginia (us-east-1)
Requester owner ID 284514300790 (This account)	Acceptor owner ID 284514300790 (This account)	

Cancel **Accept request** (highlighted with a red arrow)

VPC > Peering connections > pcx-01320dd221914ce5d

Your VPC peering connection (pcx-01320dd221914ce5d | Management-Application-Peering) has been established.
To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables.

Info

pcx-01320dd221914ce5d / Management-Application-Peering

Actions ▾

Details **Info**

Requester owner ID 284514300790	Acceptor owner ID 284514300790	VPC Peering connection ARN arn:aws:ec2:us-east-1:284514300790:vpc-peering-connection/pcx-01320dd221914ce5d
Peering connection ID pcx-01320dd221914ce5d	Requester VPC vpc-0d67c9cd66e84856c / Management-VPC	Acceptor VPC vpc-027cdfe62d7267514 / Application-VPC
Status Active	Requester CIDRs 10.0.0.0/16	Acceptor CIDRs 192.38.0.0/16
Expiration time -	Requester Region N. Virginia (us-east-1)	Acceptor Region N. Virginia (us-east-1)

DNS | **Route tables** | **Tags**

Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups

DNS | Route tables | Tags

DNS settings

Requester VPC (vpc-0d67c9cd66e84856c / Management-VPC) Info

Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses
 Disabled

Acceptor VPC (vpc-027cdfe62d7267514 / Application-VPC) Info

Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses
 Disabled

[Edit DNS settings](#)

Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups

DNS | Route tables | Tags

DNS settings

Requester VPC (vpc-0d67c9cd66e84856c / Management-VPC) Info

Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses
 Disabled

Acceptor VPC (vpc-027cdfe62d7267514 / Application-VPC) Info

Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses
 Disabled

[Edit DNS settings](#)

VPC > Peering connections > pxc-01320dd221914ce5d > Edit DNS settings



Edit DNS settings Info

Summary

Peering connection ID
 pxc-01320dd221914ce5d

Name
 Management-Application-Peering

Requester VPC
 vpc-0d67c9cd66e84856c

Acceptor VPC
 vpc-027cdfe62d7267514

Edit DNS settings

The settings below control how your peered VPCs will work with DNS resolution.

Requester DNS resolution

If enabled, the DNS hostname of an instance in the requester VPC resolves to its private IP address when queried from instances in the accepter VPC.

Allow accepter VPC (vpc-027cdfe62d7267514 / Application-VPC) to resolve DNS of requester VPC (vpc-0d67c9cd66e84856c / Management-VPC) hosts to private IP.

Acceptor DNS resolution

If enabled, the DNS hostname of an instance in the accepter VPC resolves to its private IP address when queried from instances in the requester VPC.

Allow requester VPC (vpc-0d67c9cd66e84856c / Management-VPC) to resolve DNS of accepter VPC (vpc-027cdfe62d7267514 / Application-VPC) hosts to private IP.

(i) To use DNS resolution over peering you must enable 'DNS Hostname' on the VPCs involved in peering [Learn more](#)

AWS Command Line Interface command

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



VPC > Your VPCs > vpc-027cdfe62d7267514 > Edit VPC settings

Edit VPC settings Info

VPC details

VPC ID [vpc-027cdfe62d7267514](#)
 Name [Application-VPC](#)

DHCP settings

DHCP option set [Info](#)
[dopt-0ab5c96a33ae0222f](#)

DNS settings

Enable DNS resolution [Info](#)
 Enable DNS hostnames [Info](#)

Network Address Usage metrics settings

Enable Network Address Usage metrics [Info](#)

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

VPC > Peering connections > pcx-01320dd221914ce5d

You have successfully modified the settings for pcx-01320dd221914ce5d / Management-Application-Peering.

pcx-01320dd221914ce5d / Management-Application-Peering

Details Info

Requester owner ID	284514300790
Peering connection ID	pcx-01320dd221914ce5d
Status	Active
Expiration time	-

DNS [Edit DNS settings](#)

DNS settings

Requester VPC ([vpc-0d67c9cd66e84856c / Management-VPC](#)) [Info](#)

Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses
 Enabled

Acceptor VPC ([vpc-027cdfe62d7267514 / Application-VPC](#)) [Info](#)

Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses
 Enabled

VPC Peering connection ARN
[arn:aws:ec2:us-east-1:284514300790:vpc-peering-connection/pcx-01320dd221914ce5d](#)

Acceptor VPC
[vpc-027cdfe62d7267514 / Application-VPC](#)

Acceptor CIDRs
[192.38.0.0/16](#)

Acceptor Region
 N. Virginia (us-east-1)

Step 6: Create Route tables

1. Navigate to VPC Dashboard, go to **Route tables** under the **Virtual Private Cloud** section
 - Click on Create route table button.
 - In the **Create Route Table** wizard:
 - **Name tag:** Management-VPC-table.
 - **VPC:** Select the Management-VPC from the dropdown list.
 - 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
<input type="text" value="Name"/>	<input type="text" value="Management-VPC-table"/> X Remove

Add new tag
You can add 49 more tags.

Cancel Create route table

rtb-0c9d0bef9e712666d / Management-VPC-table

Details Info

Route table ID <input type="text" value="rtb-0c9d0bef9e712666d"/>	Main <input checked="checked" type="checkbox"/>	Explicit subnet associations -	Edge associations -
VPC <input type="text" value="vpc-0d67c9cd66e84856c Management-VPC"/>	Owner ID <input type="text" value="284514300790"/>		

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes		Both		Edit routes	
Destination	Target	Status	Propagated		
10.0.0.0/16	local	Active	No		

2. Add Routes to the Route Table

- Under the **Routes** tab, click **Edit routes** and then **Add route**.
- Specify the destination and target for the route. Common destinations include:
 - For local traffic within the VPC, the destination would be 0.0.0.0/0 (or a specific IP range for the network you wish to route).
 - To route traffic to the Internet Gateway (for internet-bound traffic), the target will be the **Internet Gateway** (igw-0856f89c762c89f30).
 - For VPC peering, choose the **VPC Peering Connection** as the target.
- After adding the desired routes, click **Save changes**.

rtb-0c9d0bef9e712666d / Management-VPC-table

Details

Route table ID	rtb-0c9d0bef9e712666d	Main	No
VPC	vpc-0d67c9cd66e84856c Management-VPC	Owner ID	284514300790
		Explicit subnet associations	-
		Edge associations	-

Routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q 0.0.0.0/0	Internet Gateway	-	No
Q 192.38.0.0/16	Peering Connection	-	No

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q 0.0.0.0/0	local	Active	No
Q 192.38.0.0/16	Internet Gateway	-	No
Q igw-0856f89c762c89f30	igw-0856f89c762c89f30	Active	No
Q pcx-01320dd221914ce5d	Peering Connection	-	No

Add route

Save changes

rtb-0c9d0bef9e712666d / Management-VPC-table

Details

Route table ID	rtb-0c9d0bef9e712666d	Main	No
VPC	vpc-0d67c9cd66e84856c Management-VPC	Owner ID	284514300790
		Explicit subnet associations	-
		Edge associations	-

Routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0856f89c762c89f30	Active	No
10.0.0.0/16	local	Active	No
192.38.0.0/16	pcx-01320dd221914ce5d	Active	No

3. Associate the Route Table with a Subnet

- Go to the **Subnet associations** tab in the route table.
- Click **Edit subnet associations**.

- Select the subnets that you want to associate with the route table. If you want a subnet to route traffic via this route table, select it from the list.
- Click **Save associations**.

VPC dashboard < rtb-0c9d0bef9e712666d / Management-VPC-table Actions ▾

Virtual private cloud

Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New

Details Info

Route table ID	rtb-0c9d0bef9e712666d	Main	No
VPC	vpc-0d67c9cd66e84856c Management-VPC	Owner ID	284514300790

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (0)

Find subnet association

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

Edit subnet associations

Edit subnet associations

Available subnets (1/1)

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
Management-Subnet	subnet-085cd32eb9c9b0834	10.0.1.0/24	-	Main (rtb-0da9ca1e067a2141b)

Selected subnets

subnet-085cd32eb9c9b0834 / Management-Subnet X

Cancel Save associations

You have successfully updated subnet associations for rtb-0c9d0bef9e712666d / Management-VPC-table. Actions ▾

VPC dashboard < rtb-0c9d0bef9e712666d / Management-VPC-table Actions ▾

Virtual private cloud

Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New

Details Info

Route table ID	rtb-0c9d0bef9e712666d	Main	No
VPC	vpc-0d67c9cd66e84856c Management-VPC	Owner ID	284514300790

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (1)

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
Management-Subnet	subnet-085cd32eb9c9b0834	10.0.1.0/24	-	-

Subnets without explicit associations (0)

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

Find subnet association

Cancel Edit subnet associations

Repeat the above steps for creation of route table (Application-VPC-table) for Application-VPC

VPC > Route tables > 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.

VPC > Route tables > rtb-0aefdf4701df79fc3c

rtb-0aefdf4701df79fc3c / Application-VPC-table

Details Info

Route table ID <input type="text" value="rtb-0aefdf4701df79fc3c"/>	Main <input type="checkbox"/> No	Explicit subnet associations -	Edge associations -
VPC <input type="text" value="vpc-027cdfe62d7267514 Application-VPC"/>	Owner ID <input type="text" value="284514300790"/>		

Routes (1)

Destination	Target	Status	Propagated
192.38.0.0/16	local	<input checked="" type="checkbox"/> Active	No

VPC > Route tables > rtb-0aefdf4701df79fc3c > Edit routes

Edit routes

Destination	Target	Status	Propagated
192.38.0.0/16	local	<input checked="" type="checkbox"/> Active	No
0.0.0.0/0	local	-	No
0.0.0.0/0	Internet Gateway	-	No
0.0.0.0/0	igw-0c69a5a72c14db090	-	No
10.0.0.0/16	Peerings Connection	-	No
10.0.0.0/16	pco-01320dd221914ce5d	-	No

VPC > Route tables > rtb-0aefd4701df79fc3c

Updated routes for rtb-0aefd4701df79fc3c / Application-VPC-table successfully

rtb-0aefd4701df79fc3c / Application-VPC-table

Details

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0aefd4701df79fc3c	No	-	-
VPC	Owner ID		
vpc-027cdfe62d7267514 Application-VPC	284514300790		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (3)

Destination	Target	Status	Propagated
0.0.0.0	igw-0c69a5a72c14db090	Active	No
10.0.0.0/16	pxc-01320dd221914ce5d	Active	No
192.38.0.0/16	local	Active	No

VPC > Route tables > rtb-0aefd4701df79fc3c

rtb-0aefd4701df79fc3c / Application-VPC-table

Details

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0aefd4701df79fc3c	No	-	-
VPC	Owner ID		
vpc-027cdfe62d7267514 Application-VPC	284514300790		

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.

VPC > Route tables > rtb-0aefd4701df79fc3c > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

Selected subnets

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

You have successfully updated subnet associations for rtb-0aefd4701df79fc3c / Application-VPC-table.

rtb-0aefd4701df79fc3c / Application-VPC-table

Details **Info**

Route table ID rtb-0aefd4701df79fc3c	Main No	Explicit subnet associations subnet-0c174e12ec924ce46 / Application-Subnet	Edge associations -
VPC vpc-027cdfe62d7267514 Application-VPC	Owner ID 284514300790		

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

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Application-Subnet	subnet-0c174e12ec924ce46	192.38.1.0/24	-

4. Verify the Route Table Association

- You can confirm that the subnets are properly associated by navigating to **Subnets** under the **VPC** dashboard and checking which route table is listed for each subnet.
- You can also see the active routes by selecting the route table and checking the **Routes** tab.

Step 7: Create Security Groups

Allow only necessary traffic between VPCs:

1. Go to **Security Groups**
2. For Management-VPC-SecurityGroup, allow inbound traffic:
 - Source: Anywhere
 - Protocol: As required (All ICMP-IPv4, SSH, HTTP)
3. Similarly, configure Application-VPC-SecurityGroup to allow only required inbound connections

EC2 Global View

Virtual private cloud

Security

Network ACLs

Security groups

Security Groups (4) Info

Create security group

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0edf7b06775654ad8	default	vpc-0d67c9cd66e84856c	default VP
-	sg-0b4024219fbf57905	default	vpc-0f982f9178eb91a4f	default VP

VPC > Security Groups > Create security group

Basic details

Security group name [Info](#)
Management-VPC-SecurityGroup
Name cannot be edited after creation.

Description [Info](#)
Allow traffic

VPC [Info](#)
vpc-0d67c9cd6e84856c (Management-VPC)

Inbound rules

Type	Protocol	Port range	Source	Description - optional
All ICMP - IPv4	ICMP	All	Anyw... Delete	0.0.0.0/0 X
SSH	TCP	22	Anyw... Delete	0.0.0.0/0 X
HTTP	TCP	80	Anyw... Delete	

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Anyw... Delete	0.0.0.0/0 X

Tags - optional
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.
No tags associated with the resource.

[Add new tag](#)
You can add up to 50 more tags

[Cancel](#) **Create security group**

sg-08e40592ba04834cf - Management-VPC-SecurityGroup

Actions ▾

Details

Security group name	Management-VPC-SecurityGroup	Security group ID	sg-08e40592ba04834cf	Description	Allow traffic	VPC ID	vpc-0d67c9cd66e84856c
Owner	284514300790	Inbound rules count	3 Permission entries	Outbound rules count	1 Permission entry		

[Inbound rules](#) [Outbound rules](#) [Sharing - new](#) [VPC associations - new](#) [Tags](#)

Inbound rules (3)

Search						
	Name	Security group rule ID	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-0e0674ad756ada1e1	IPv4	HTTP	TCP	80
<input type="checkbox"/>	-	sgr-02296867bed02a90f	IPv4	All ICMP - IPv4	ICMP	All
<input type="checkbox"/>	-	sgr-0b1741fc890f53521	IPv4	SSH	TCP	22

Create Application-VPC-Security Group

EC2 Global View ▾ [Filter by VPC](#)

Virtual private cloud [Create security group](#)

Security groups (4) [Actions](#) [Export security groups to CSV](#) [Create security group](#)

Name	Security group ID	Security group name	VPC ID	Description
sg-0edf7b06775654ad8	default	vpc-0d67c9cd66e84856c	default VP	
sg-0b4024219fbf57905	default	vpc-0f982f9178eb91a4f	default VP	
sg-02d5ff0f0371d7cd5	Management-VPC-SecurityGroup	vpc-0d67c9cd66e84856c	Allow traff	
sg-07a2f3709c2ded5a6	default	vpc-027cdfe62d7267514	default VP	

[VPC](#) > [Security Groups](#) > Create security group

Basic details

Security group name [Info](#)
Application-VPC-SecurityGroup
Name cannot be edited after creation.

Description [Info](#)
Allow traffic

VPC info
vpc-027cdfe62d7267514 (Application-VPC)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
All ICMP - IPv4	ICMP	All	Any... Delete	0.0.0.0/0 Delete
SSH	TCP	22	Any... Delete	0.0.0.0/0 Delete
HTTP	TCP	80	Any... Delete	0.0.0.0/0 Delete

Outbound rules

Type: All traffic | Protocol: All | Port range: All | Destination: Any... | Description: 0.0.0.0/0

Tags - optional

No tags associated with the resource.

Create security group

sg-0e72149fa010fcc1d - Application-VPC-SecurityGroup

Details

Security group name Application-VPC-SecurityGroup	Security group ID sg-0e72149fa010fcc1d	Description Allow traffic	VPC ID vpc-027cdfe62d7267514
Owner 284514300790	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules (3)

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-07ca5677d91bb3bb2	IPv4	All ICMP - IPv4	ICMP	All
-	sgr-0af9c2e955cb1678a	IPv4	HTTP	TCP	80
-	sgr-095d0aa9fb3b249d0	IPv4	SSH	TCP	22

Step 8: Launch EC2 Instances (for testing) in each VPC

1. Go to **EC2** → Launch Instance
2. Choose Free Tier eligible AMI (Amazon Linux)
3. Instance type: t2.micro
4. Key pair: Proceed without keypair
5. Networking Setting: Edit
 - VPC: choose Management-VPC
 - Subnet: Management-subnet
 - Auto-assign public ip: enable
 - Firewall: Select existing Security Group (Management-VPC-SecurityGroup)

6. Leave default settings
7. Click Launch Instance
8. Use **private IPs** to test connectivity via SSH or ping (if ICMP allowed)

Create Management-instance

[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 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

Recent AMIs: [Amazon Linux](#) (selected), [macOS](#), [Ubuntu](#), [Windows](#), [Red Hat](#), [SUSE Linux](#), [Debian](#)

[Quick Start](#)

[Browse more AMIs](#) Including AMIs from AWS, Marketplace and the Community

Summary

Number of instances [Info](#) 1

Software Image (AMI) Amazon Linux 2023 AMI 2023.7.2...read more [ami-00a929b66ed6e0de6](#)

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 of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable). [X](#)

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

Amazon Machine Image (AMI)

[Amazon Linux 2023 AMI](#) [Free tier eligible](#)

ami-00a929b66ed6e0de6 (64-bit (x86), uefi-preferred) / ami-05f417c208be02d4d (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 2023.7.20250331.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username
64-bit (x86) ▾	uefi-preferred	ami-00a929b66ed6e0de6	2025-03-29	ec2-user

Verified provider

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

Instance type

t2.micro [Free tier eligible](#)

Family: t2 1 vCPU 1 GiB Memory Current generation: true
 On-Demand Windows base pricing: 0.0162 USD per Hour
 On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
 On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour
 On-Demand Linux base pricing: 0.0116 USD per Hour

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

Proceed without a key pair (Not recommended) Default value [▼](#) [Create new key pair](#)

▼ Network settings [Info](#)

Network [Info](#)
vpc-0f982f9178eb91a4f

Subnet [Info](#)
No preference (Default subnet in any availability zone)

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](#)

▼ Network settings [Info](#)

VPC - required [Info](#)
vpc-0d67c9cd66e84856c (Management-VPC)
10.0.0.0/16

Subnet [Info](#)
subnet-085cd32eb9c9b0834 Management-Subnet
VPC: vpc-0d67c9cd66e84856c Owner: 284514300790 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24

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](#)

Common security groups [Info](#)
Select security groups
Management-VPC-SecurityGroup sg-08e40592ba04834cf
VPC: vpc-0d67c9cd66e84856c

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

▼ Summary

Number of instances [Info](#)
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.7.2...[read more](#)

Virtual server type (instance type)
t2.micro

Firewall (security group)
Management-VPC-SecurityGroup

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

(i) Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

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

EC2 > Instances

Instances (3) [Info](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Management-instance	i-08d3022b351d17ed2	Running	t2.micro	Initializing		us-east-1a

EC2 > Instances

Instances (3) [Info](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Management-instance	i-08d3022b351d17ed2	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a

Instances (1/3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Management-instance	i-08d3022b351d17ed2	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a
	i-041147c7600bc3502	Terminated	t2.micro	-	View alarms +	us-east-1a
	i-0c609ab943e144dbb	Terminated	t2.micro	-	View alarms +	us-east-1a

i-08d3022b351d17ed2 (Management-instance)

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

Instance summary

Instance ID i-08d3022b351d17ed2	Public IPv4 address 54.198.240.57 open address	Private IPv4 addresses 10.0.1.150
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-198-240-57.compute-1.amazonaws.com open address
Hostname type IP name: ip-10-0-1-150.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-1-150.ec2.internal	Elastic IP addresses
Answer private resource DNS name	Instance type t2.micro	

Create Application-instance

EC2 > Instances

Instances (3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Management-instance	i-08d3022b351d17ed2	Running	t2.micro	Initializing	View alarms +	us-east-1a
	i-041147c7600bc3502	Terminated	t2.micro	-	View alarms +	us-east-1a
	i-0c609ab943e144dbb	Terminated	t2.micro	-	View alarms +	us-east-1a

EC2 > Instances > Launch an instance

Launch an instance

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

Name
Application-Instance

Application and OS Images (Amazon Machine Image)

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.

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.7.2...read more

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 of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where applicable).

Launch instance

Amazon Linux 2023 AMI
 ami-0a929b66ed6e0de6 (64-bit (x86), uefi-preferred) / ami-05f417c208be02d4d (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 2023.7.20250331.0.x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username
64-bit (x86)	uefi-preferred	ami-0a929b66ed6e0de6	2025-03-29	ec2-user

Verified provider

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

Instance type

t2.micro
 Family: t2 1 vCPU 1 GiB Memory Current generation: true
 Free tier eligible
 On-Demand Windows base pricing: 0.016 USD per Hour
 On-Demand Ubuntu Pro base pricing: 0.0154 USD per Hour
 On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour
 On-Demand Linux base pricing: 0.0116 USD per Hour

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

Proceed without a key pair (Not recommended) Default value [Create new key pair](#)

Network settings [Info](#)

Network [Info](#)
 vpc-0f982f9178eb91a4f

Subnet [Info](#)
 No preference (Default subnet in any availability zone)

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

We'll create a new security group called 'launch-wizard-1' with the following rules:

Allow SSH traffic from Anywhere

Summary

Number of instances | [Info](#)
 1

Software Image (AMI)
 Amazon Linux 2023 AMI 2023.7.2...[read more](#)
 ami-0a929b66ed6e0de6

Virtual server type (instance type)
 t2.micro

Firewall (security group)
 New security group

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

[Free tier](#)

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

Network settings [Info](#)

VPC - required [Info](#)
 vpc-027cf62d7267514 (Application-VPC)
 192.38.0.0/16

Subnet [Info](#)
 subnet-0c174e12ec924ce46 Application-Subnet
 VPC: vpc-027cf62d7267514 Owner: 284514300790 Availability Zone: us-east-1a
 Zone type: Availability Zone IP addresses available: 251 CIDR: 192.38.1.0/24

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

Common security groups [Info](#)
 Select security groups

Application-VPC-SecurityGroup sg-0e72149fa010fcc1d X
 VPC: vpc-027cf62d7267514

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Summary

Number of instances | [Info](#)
 1

Software Image (AMI)
 Amazon Linux 2023 AMI 2023.7.2...[read more](#)
 ami-0a929b66ed6e0de6

Virtual server type (instance type)
 t2.micro

Firewall (security group)
 Application-VPC-SecurityGroup

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

[Free tier](#)

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

Instances (1/4) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Management-instance	i-08d3022b351d17ed2	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a
Application-instance	i-0d9e77f5835bff175	Running	t2.micro	Initializing	View alarms +	us-east-1a

Instances (1/4) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Management-instance	i-08d3022b351d17ed2	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a
Application-instance	i-0d9e77f5835bff175	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a
	i-041147c7600bc3502	Terminated	t2.micro	-	View alarms +	us-east-1a
	i-0c609ab943e144dbb	Terminated	t2.micro	-	View alarms +	us-east-1a

i-0d9e77f5835bff175 (Application-instance)

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

Instance summary

Instance ID	34.201.140.205 open address	Public IPv4 address
IPv6 address	-	Instance state
Hostname type	ip-192-38-1-198.ec2.internal	Private IP DNS name (IPv4 only)
Answer private resource DNS name		ip-192-38-1-198.ec2.internal
	Instance type	Elastic IP addresses

Step 9: Test and Monitor

- SSH from Management EC2 to Application EC2 (or vice versa, depending on security rules)
- Enable **VPC Flow Logs** for each VPC to monitor traffic

Connect to EC2 instance:

Choose Management-instance and click on connect button

Instances (1/4) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Management-instance	i-08d3022b351d17ed2	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a
Application-instance	i-0d9e77f5835bff175	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a

Click on EC2 Instance Connect tab and click Connect

EC2 > Instances > i-08d3022b351d17ed2 > Connect to instance

Connect to instance Info

Connect to your instance i-08d3022b351d17ed2 (Management-instance) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 serial console

Instance ID [i-08d3022b351d17ed2](#) (Management-instance)

Connection Type

- Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 or IPv6 address.
- Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IPv4 address [54.198.240.57](#)

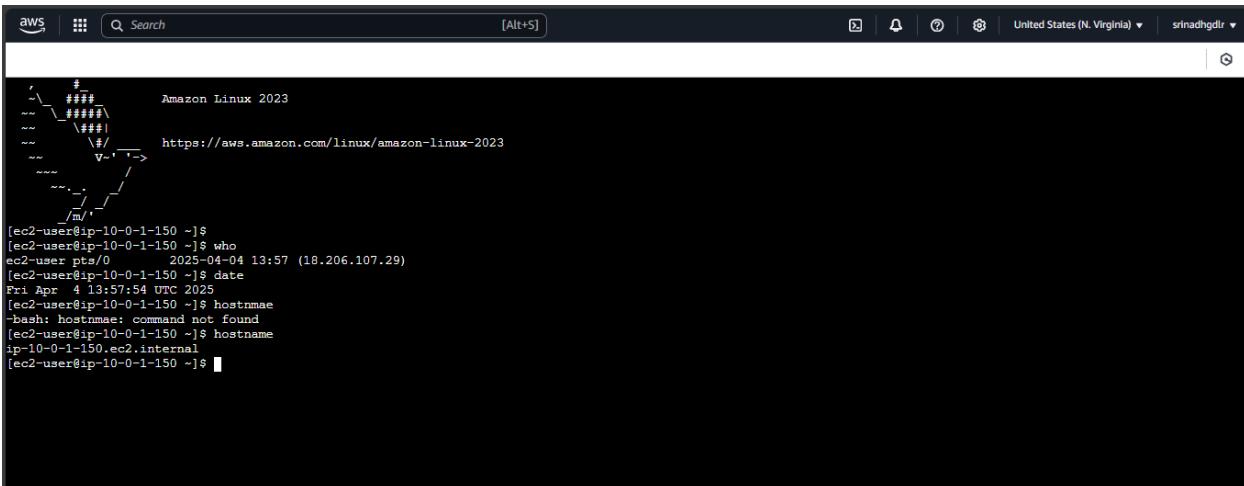
IPv6 address

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

[X](#)

Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

[Cancel](#) [Connect](#)



i-08d3022b351d17ed2 (Management-instance)
PublicIPs: 54.198.240.57 PrivateIPs: 10.0.1.150

Ping Private IPv4 addresses 198.38.1.198 of Application-instance from Management-instance

```
[ec2-user@ip-10-0-1-150 ~]$ ping 192.38.1.198
PING 192.38.1.198 (192.38.1.198) 56(84) bytes of data.
64 bytes from 192.38.1.198: icmp_seq=1 ttl=127 time=1.17 ms
64 bytes from 192.38.1.198: icmp_seq=2 ttl=127 time=1.25 ms
64 bytes from 192.38.1.198: icmp_seq=3 ttl=127 time=0.635 ms
64 bytes from 192.38.1.198: icmp_seq=4 ttl=127 time=0.850 ms
64 bytes from 192.38.1.198: icmp_seq=5 ttl=127 time=0.807 ms
64 bytes from 192.38.1.198: icmp_seq=6 ttl=127 time=0.821 ms
64 bytes from 192.38.1.198: icmp_seq=7 ttl=127 time=0.694 ms

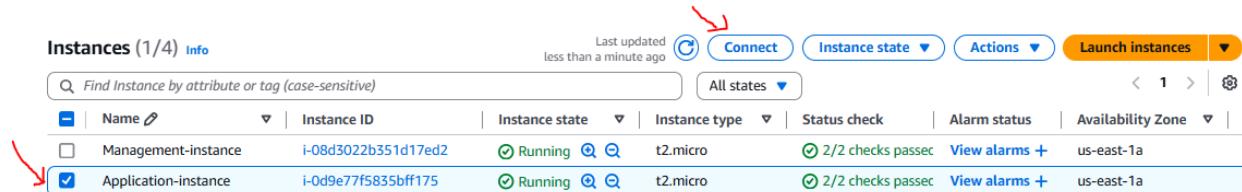
64 bytes from 192.38.1.198: icmp_seq=8 ttl=127 time=1.07 ms
^C
--- 192.38.1.198 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7205ms
rtt min/avg/max/mdev = 0.635/0.912/1.252/0.210 ms
[ec2-user@ip-10-0-1-150 ~]$
```

i-08d3022b351d17ed2 (Management-instance)

PublicIPs: 54.198.240.57 PrivateIPs: 10.0.1.150

So, it is connecting and we can access resources of other VPC

Connect to Application-instance:



Instances (1/4) Info								
Last updated less than a minute ago Connect Instance state Actions Launch instances								
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/> All states								
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	
<input type="checkbox"/>	Management-instance	i-08d3022b351d17ed2	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	
<input checked="" type="checkbox"/>	Application-instance	i-0d9e77f5835bff175	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	

Click on EC2 Instance Connect tab and click Connect

EC2 > Instances > i-0d9e77f5835bff175 > Connect to instance

Connect to instance Info

Connect to your instance i-0d9e77f5835bff175 (Application-instance) using any of these options

EC2 Instance Connect [Session Manager](#) [SSH client](#) [EC2 serial console](#)

Instance ID
i-0d9e77f5835bff175 (Application-instance)

Connection Type

Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 or IPv6 address.

Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IPv4 address
34.201.140.205

IPv6 address

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

[X](#)

ⓘ Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

[Cancel](#) [Connect](#)

AWS Search [Alt+S] United States (N. Virginia) srinadhgdr

```

#          Amazon Linux 2023
# \###\ https://aws.amazon.com/linux/amazon-linux-2023
# \###\ V-->
# / \
# / \
# / \
# / \
# / \
[ec2-user@ip-192-38-1-198 ~]$ who
ec2-user pts/0      2025-04-04 14:02 (18.206.107.29)
[ec2-user@ip-192-38-1-198 ~]$ date
Fri Apr 4 14:02:28 UTC 2025
[ec2-user@ip-192-38-1-198 ~]$ hostname
ip-192-38-1-198.ec2.internal
[ec2-user@ip-192-38-1-198 ~]$ |

```

i-0d9e77f5835bff175 (Application-instance) [X](#)

Public IPs: 34.201.140.205 Private IPs: 192.38.1.198

Ping **Private IPv4 addresses 10.0.1.150** of Management-instance from the Application-instance

```
[ec2-user@ip-192-38-1-198 ~]$ ping 10.0.1.150
PING 10.0.1.150 (10.0.1.150) 56(84) bytes of data.
64 bytes from 10.0.1.150: icmp_seq=1 ttl=127 time=0.658 ms
64 bytes from 10.0.1.150: icmp_seq=2 ttl=127 time=1.06 ms
64 bytes from 10.0.1.150: icmp_seq=3 ttl=127 time=1.60 ms
64 bytes from 10.0.1.150: icmp_seq=4 ttl=127 time=1.15 ms
64 bytes from 10.0.1.150: icmp_seq=5 ttl=127 time=1.18 ms
64 bytes from 10.0.1.150: icmp_seq=6 ttl=127 time=1.01 ms
64 bytes from 10.0.1.150: icmp_seq=7 ttl=127 time=0.776 ms
64 bytes from 10.0.1.150: icmp_seq=8 ttl=127 time=1.13 ms
64 bytes from 10.0.1.150: icmp_seq=9 ttl=127 time=0.491 ms
64 bytes from 10.0.1.150: icmp_seq=10 ttl=127 time=1.42 ms
^C
--- 10.0.1.150 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9168ms
rtt min/avg/max/mdev = 0.491/1.047/1.600/0.318 ms
[ec2-user@ip-192-38-1-198 ~]$
```

i-0d9e77f5835bff175 (Application-instance)

PublicIPs: 34.201.140.205 PrivateIPs: 192.38.1.198

So, it is connecting and we can access resources of other VPC