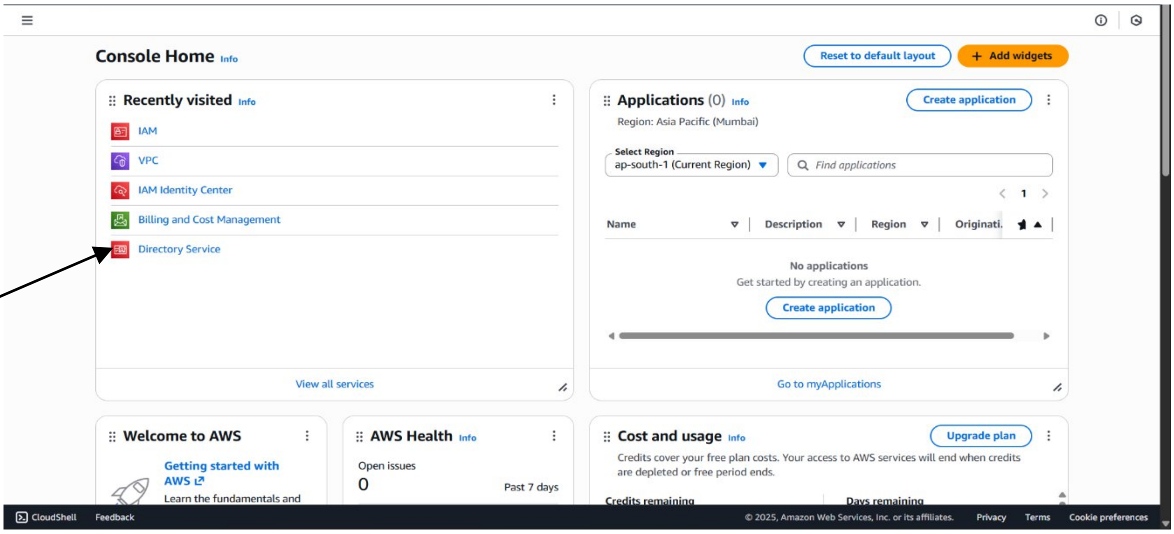
AWS ASSIGNMENT 1
EC2 Instance Craetion

CREATE A AWS FREE TIER ACCOUNT AS A ROOT USER SO THAT WE CAN WORK IN GROUPS AND ALSO TO CREATE SUB ACCOUNTS FOR WORK MANAGEMENT

ROOT USER



Console Home Info

Reset to default layout | + Add widgets

Recently visited Info
- IAM
- VPC
- IAM Identity Center
- Billing and Cost Management
- Directory Service

View all services

Applications (0) Info | Create application

Region: Asia Pacific (Mumbai)

Select Region: ap-south-1 (Current Region) | Find applications

Name	Description	Region	Originati..

No applications
Get started by creating an application.

Create application

Go to myApplications

Welcome to AWS
Getting started with AWS
Learn the fundamentals and

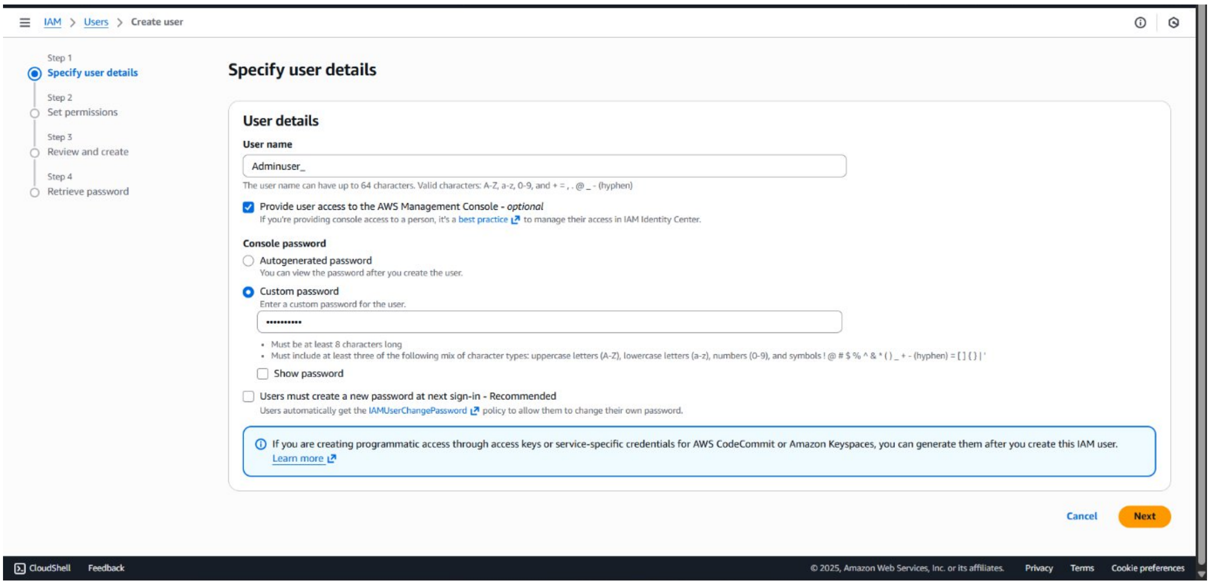
AWS Health Info
Open issues: 0 | Past 7 days

Cost and usage Info | Upgrade plan
Credits cover your free plan costs. Your access to AWS services will end when credits are depleted or free period ends.
Credits remaining | Days remaining

IAM

NOW WE GO TO IAM AND CREATE A USER THERE TO WORK WITH WE DON’T USE OUR ROOT ACCOUNT FOR WORKING WE CREATE USERS THERE FOR WORK WE USE DIFFERENT USERS FOR DIFFERENT WORK THIS WILL HELP US TO MANAGE THE BILLING AND POLICIES EASILY

ROOT IS UESD TO MANAGE THOSE IAM ACCOUNT IT’S LIKE A BOSS IS RUNNING THE COMPANY HE WILL PAY AND GET THE WORK DONE BUT HE WILL NOT WORK



IAM > Users > Create user

Step 1
● Specify user details

Step 2
○ Set permissions

Step 3
○ Review and create

Step 4
○ Retrieve password

Specify user details

User details

User name: Adminuser_

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Console password

○ Autogenerated password
You can view the password after you create the user.

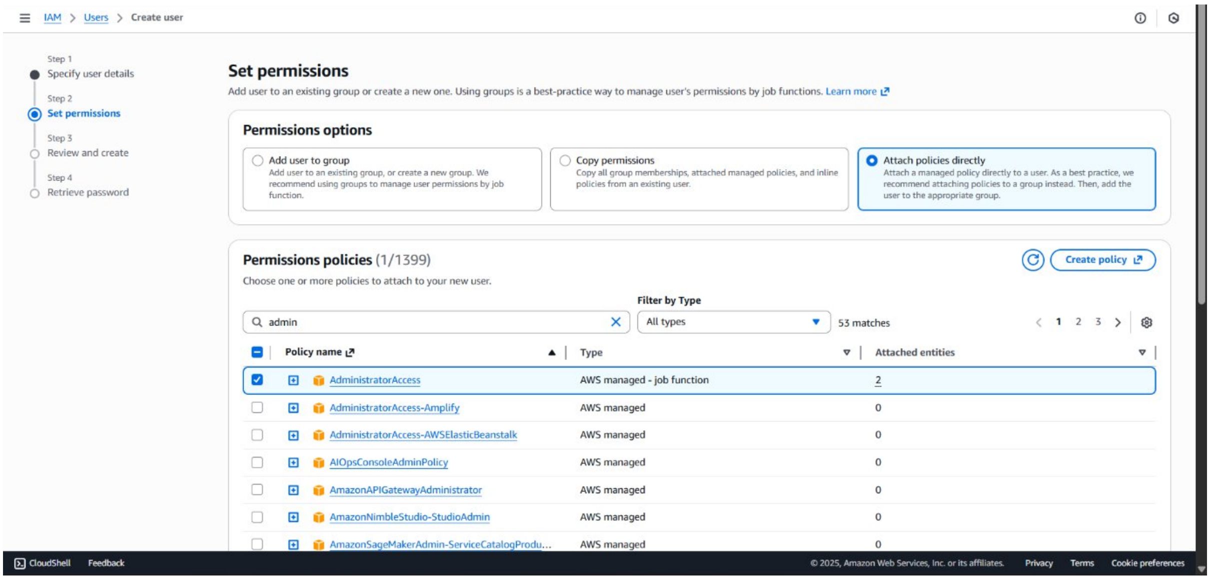
● Custom password
Enter a custom password for the user.
••••••••••

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

□ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.
Learn more



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1399)

Create policy

Choose one or more policies to attach to your new user.

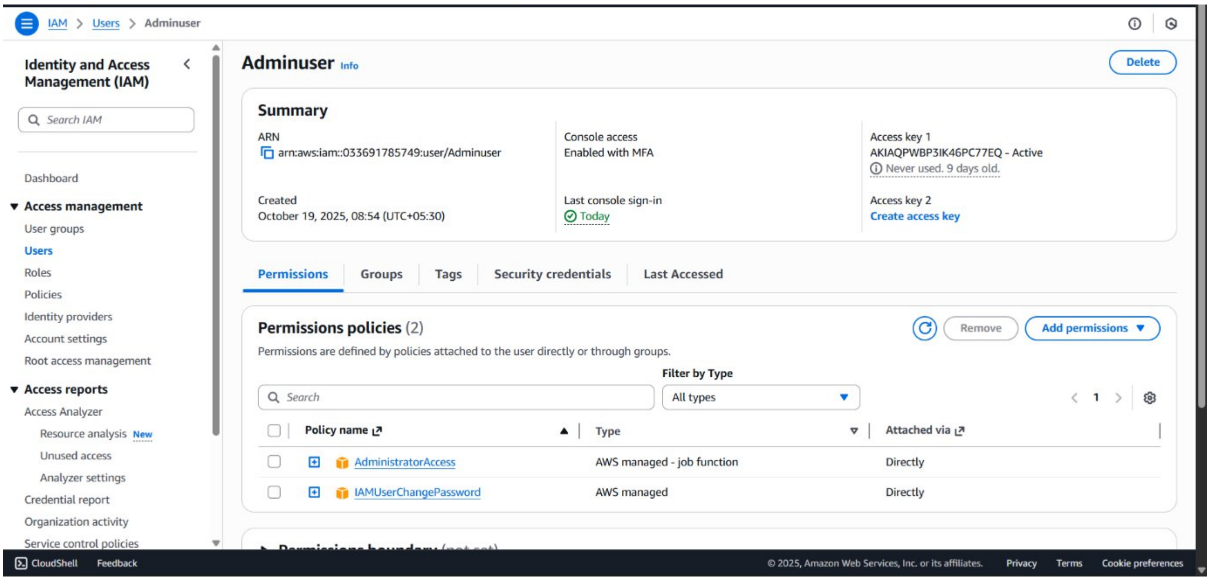
Filter by Type

admin ✕ | All types ▼ | 53 matches | < 1 2 3 >

	Policy name	Type	Attached entities
☑	AdministratorAccess	AWS managed - job function	2
□	AdministratorAccess-Amplify	AWS managed	0
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
□	AIOpsConsoleAdminPolicy	AWS managed	0
□	AmazonAPIGatewayAdministrator	AWS managed	0
□	AmazonNimbleStudio-StudioAdmin	AWS managed	0
□	AmazonSageMakerAdmin-ServiceCatalogProdu...	AWS managed	0

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- HERE WE CREATE AN ADMINUSER IAM USER IN OUR ROOT ACCOUNT WE GIVE IT PERMISSIONS OF ADMINISTRATORACCESS AND ALSO WE ADD A MFA IN IT AND ALSO A ACCESS KEY FOR SAFETY AND NOW OUR STEP 1ST AND 2ND ARE COMPLETED NOW LET'S MOVE TO STEP 3RD FOR STEP 3RD WE WILL USE THE ADMINUSER ACCOUNT WE JUST CREATED BY OUR ROOT ACCOUNT



IAM > Users > Adminuser

Identity and Access Management (IAM)

Search IAM

Dashboard
▼ Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
▼ Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies

Adminuser Info

Delete

Summary

ARN
arn:aws:iam::033691785749:user/Adminuser

Created
October 19, 2025, 08:54 (UTC+05:30)

Console access
Enabled with MFA

Last console sign-in
Today

Access key 1
AKIAQPWBP3IK46PC77EQ - Active
Never used. 9 days old.

Access key 2
Create access key

Permissions | Groups | Tags | Security credentials | Last Accessed

Permissions policies (2)

Remove | Add permissions ▼

Permissions are defined by policies attached to the user directly or through groups.

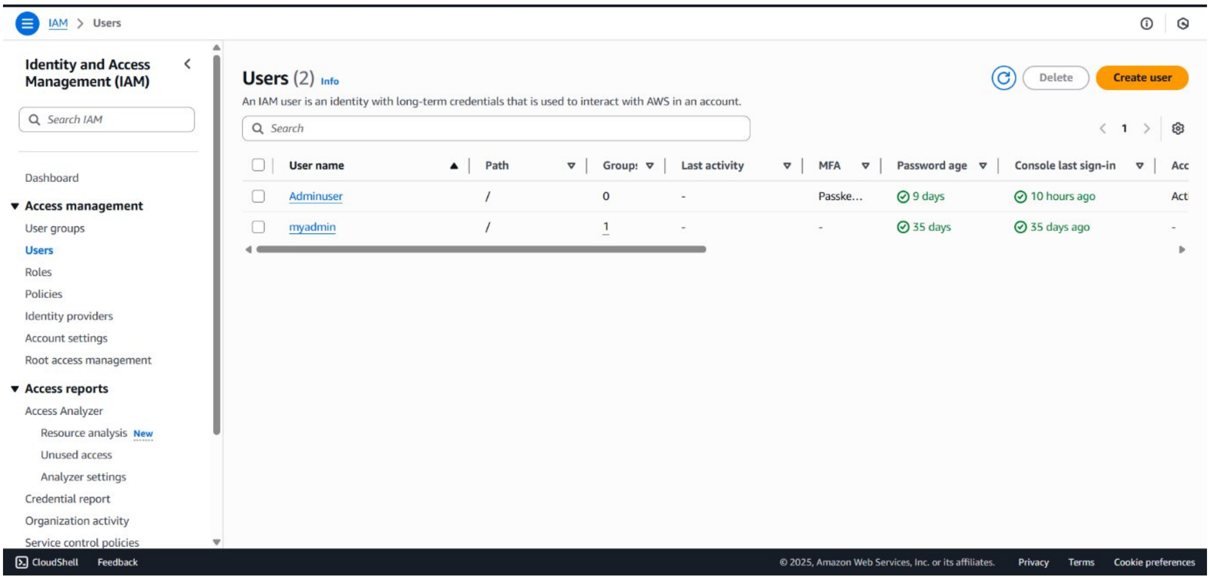
Filter by Type

Search | All types ▼ | < 1 >

	Policy name	Type	Attached via
□	AdministratorAccess	AWS managed - job function	Directly
□	IAMUserChangePassword	AWS managed	Directly

▶ Permissions boundary (not set)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



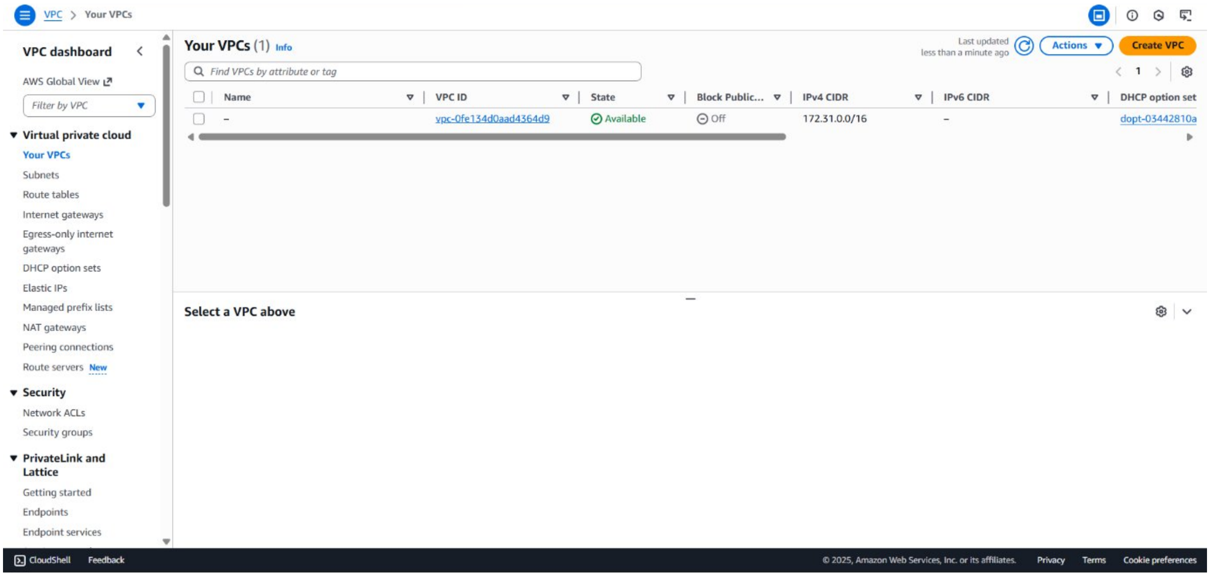
Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Acc
□	Adminuser	/	0	-	Passke...	9 days	10 hours ago	Act
□	myadmin	/	1	-	-	35 days	35 days ago	-

STEP 3

HERE WE ARE IN OUR ADMINUSER ACCOUNT NOW WE GO TO THE VPC SECTION AND HERE WE SAW THAT THERE IS ALREADY A VPC AVAILABLE IN OUR ACCOUNT IT'S A DEFAULT VPC BY AWS IF YOU WANT TO CREATE YOUR OWN SO YOU CAN BUT FOR WE ARE GOING WITH THIS

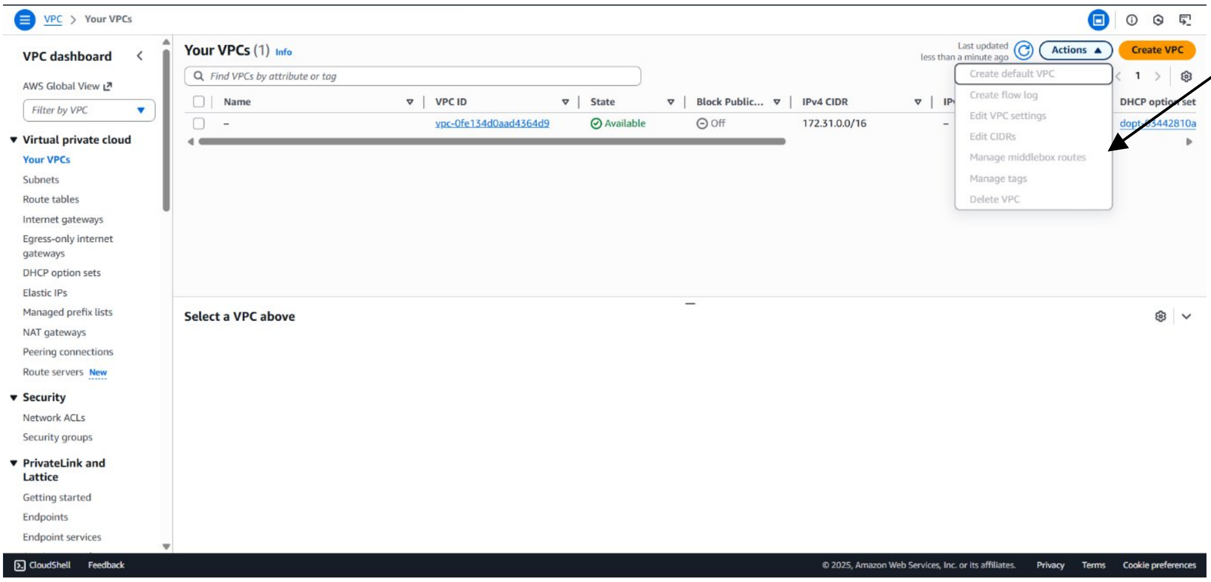


Your VPCs (1) Info

□	Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option set
□	–	vpc-0fe134d0aad4364d9	Available	Off	172.31.0.0/16	–	dopt-03442810a

Select a VPC above

- IF YOU DELETED THE VPC AND WANT TO CREATE YOU OWN SO YOU CAN DO THAT AND IF YOU AREN'T ABLE TO CREATE VPC SO YOU CAN CREATE A DEFAULT VPC AGAIN YOU CAN SEE IT HERE

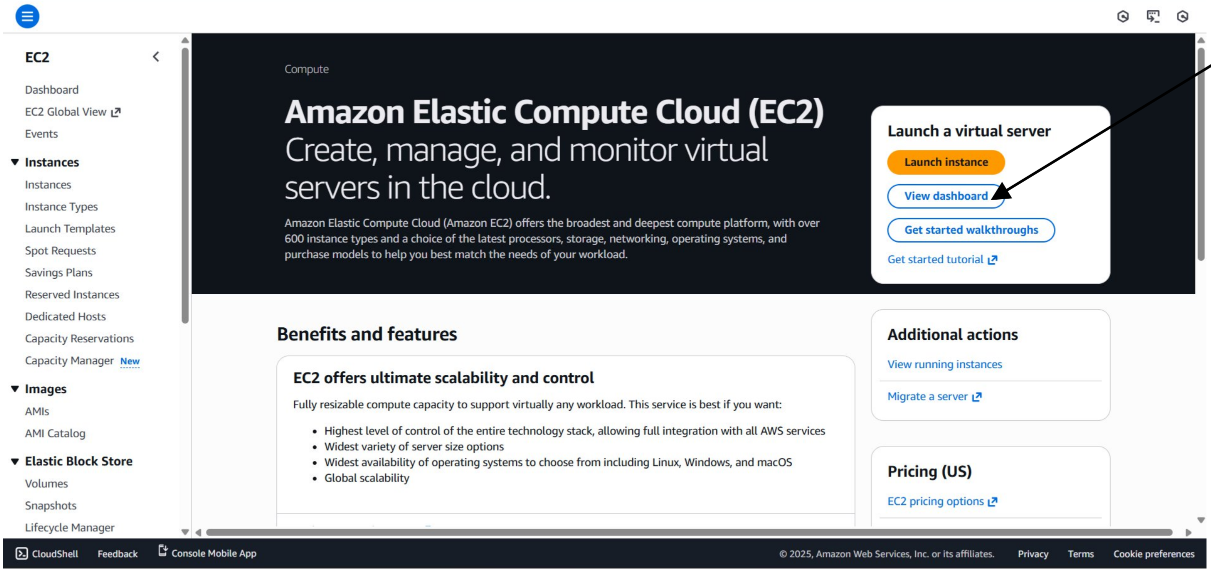


Name	VPC ID	State	Block Public...	IPv4 CIDR	IP	DHCP option set
–	vpc-0fe134d0aad4364d9	Available	Off	172.31.0.0/16	–	dopt-03442810a

DEFAULT VPC

STEP 4 ,5 & 6

IN THIS WE WILL CREATE A EC2 INSTANCE TO RUN OUR WEBSITE AND ALSO WE PERFORM RDP WITH ACCESS KEY PAIR AND BY FLEET MANAGER



Amazon Elastic Compute Cloud (EC2)

Create, manage, and monitor virtual servers in the cloud.

Amazon Elastic Compute Cloud (Amazon EC2) offers the broadest and deepest compute platform, with over 600 instance types and a choice of the latest processors, storage, networking, operating systems, and purchase models to help you best match the needs of your workload.

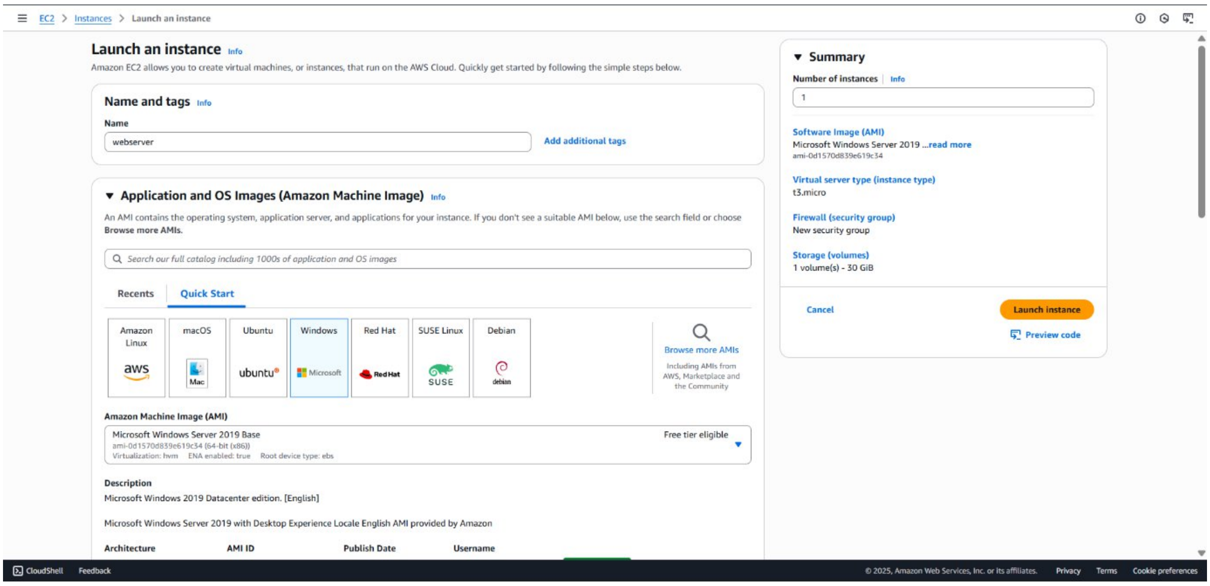
Benefits and features

EC2 offers ultimate scalability and control

Fully resizable compute capacity to support virtually any workload. This service is best if you want:

- Highest level of control of the entire technology stack, allowing full integration with all AWS services
- Widest variety of server size options
- Widest availability of operating systems to choose from including Linux, Windows, and macOS
- Global scalability

LAUNCH INSTANCE



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: webserver

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

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

Amazon Machine Image (AMI)

Microsoft Windows Server 2019 Base — Free tier eligible
ami-0d1570d839e619c34 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Microsoft Windows 2019 Datacenter edition. [English]

Microsoft Windows Server 2019 with Desktop Experience Locale English AMI provided by Amazon

Architecture AMI ID Publish Date Username

Summary

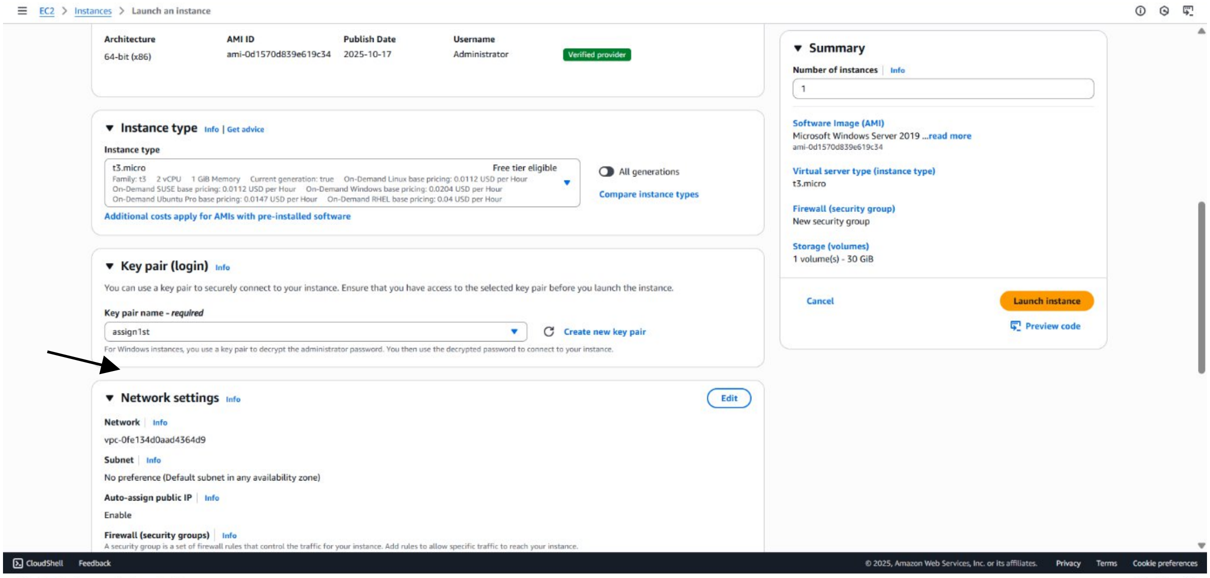
Number of instances: 1

Software Image (AMI)
Microsoft Windows Server 2019 ...read more
ami-0d1570d839e619c34

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 30 GiB



EC2 > Instances > Launch an instance

Architecture	AMI ID	Publish Date	Username	
64-bit (x86)	ami-0d1570d839e619c34	2025-10-17	Administrator	Verified provider

Instance type

Instance type

t3.micro — Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0112 USD per Hour
On-Demand SUSE base pricing: 0.0112 USD per Hour On-Demand Windows base pricing: 0.0204 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0147 USD per Hour On-Demand RHEL base pricing: 0.04 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login)

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*: assign1st

Create new key pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

Network settings

Network: vpc-0fe134d0aad4364d9

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enable

Firewall (security groups)
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.

Summary

Number of instances: 1

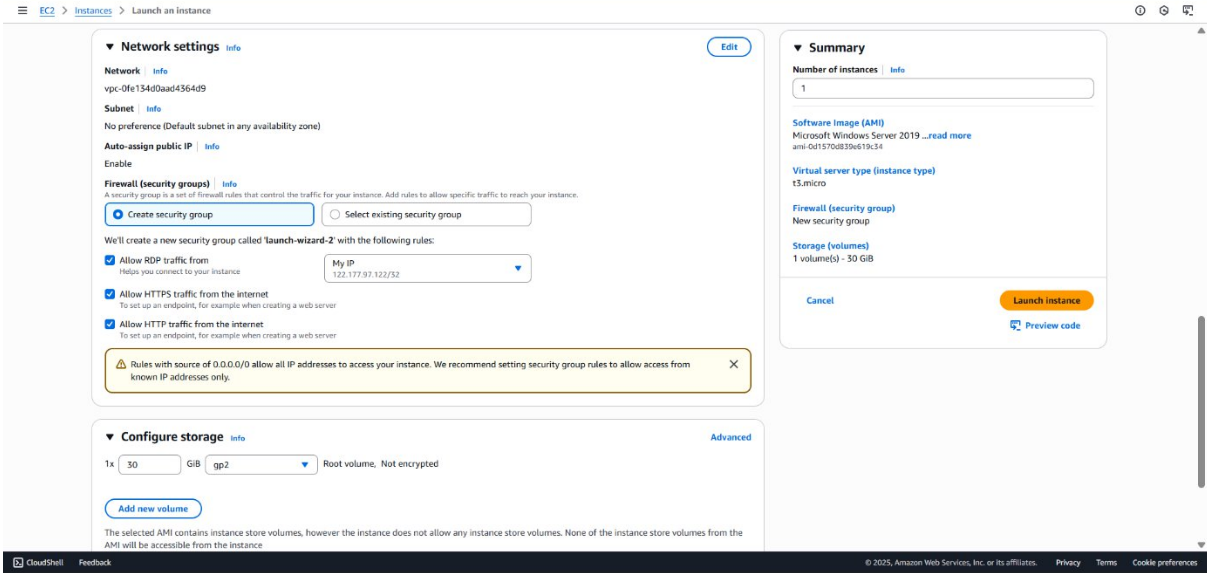
Software Image (AMI)
Microsoft Windows Server 2019 ...read more
ami-0d1570d839e619c34

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 30 GiB

CREATE NEW KEY PAIR



EC2 > Instances > Launch an instance

Network settings

Network: vpc-0fe134d0aad4364d9

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enable

Firewall (security groups)
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-2**' with the following rules:

☑ Allow RDP traffic from — My IP 122.177.97.122/32
Helps you connect to your instance

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

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

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Configure storage

1x 30 GiB gp2 Root volume, Not encrypted

Add new volume

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the instance store volumes from the AMI will be accessible from the instance

Summary

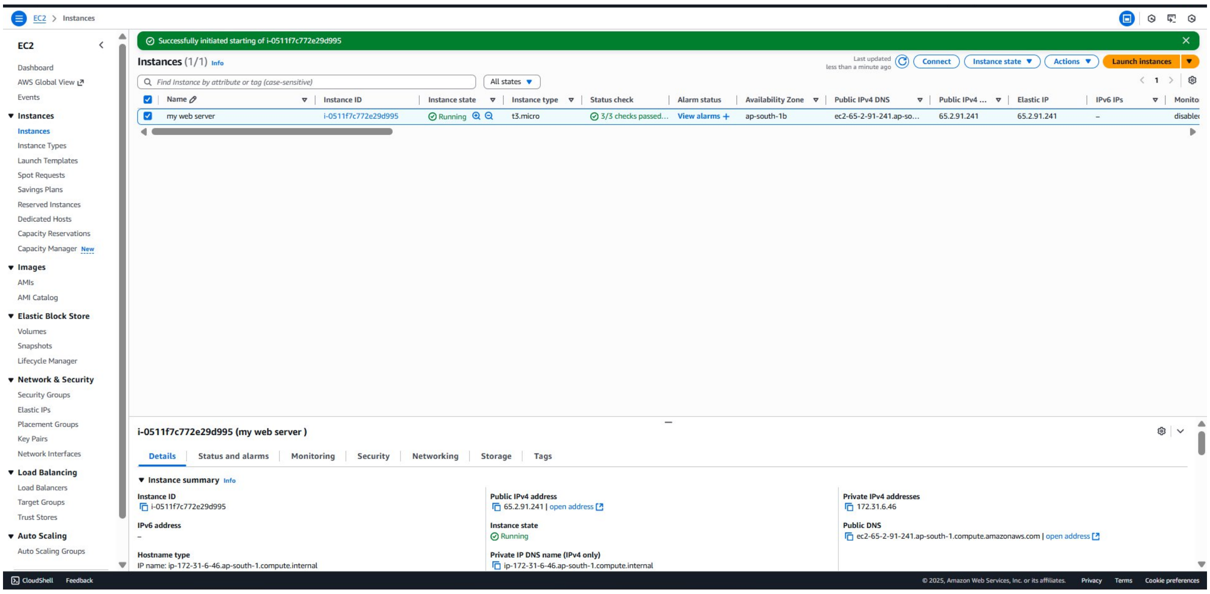
Number of instances: 1

Software Image (AMI)
Microsoft Windows Server 2019 ...read more
ami-0d1570d839e619c34

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 30 GiB



EC2 > Instances

Successfully initiated starting of i-0511f7c772e29d995

EC2

- Dashboard
- AWS Global View
- Events
- Instances
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity Reservations
  - Capacity Manager New
- Images
  - AMIs
  - AMI Catalog
- Elastic Block Store
  - Volumes
  - Snapshots
  - Lifecycle Manager
- Network & Security
  - Security Groups
  - Elastic IPs
  - Placement Groups
  - Key Pairs
  - Network Interfaces
- Load Balancing
  - Load Balancers
  - Target Groups
  - Trust Stores
- Auto Scaling
  - Auto Scaling Groups

Instances (1/1) Info

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

All states

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monito
☑	my web server	i-0511f7c772e29d995	Running	t3.micro	3/3 checks passed...	View alarms +	ap-south-1b	ec2-65-2-91-241.ap-so...	65.2.91.241	65.2.91.241	–	disablec

i-0511f7c772e29d995 (my web server)

Instance summary Info

Instance ID
i-0511f7c772e29d995

IPv6 address
–

Hostname type
IP name: ip-172-31-6-46.ap-south-1.compute.internal

Public IPv4 address
65.2.91.241 | open address

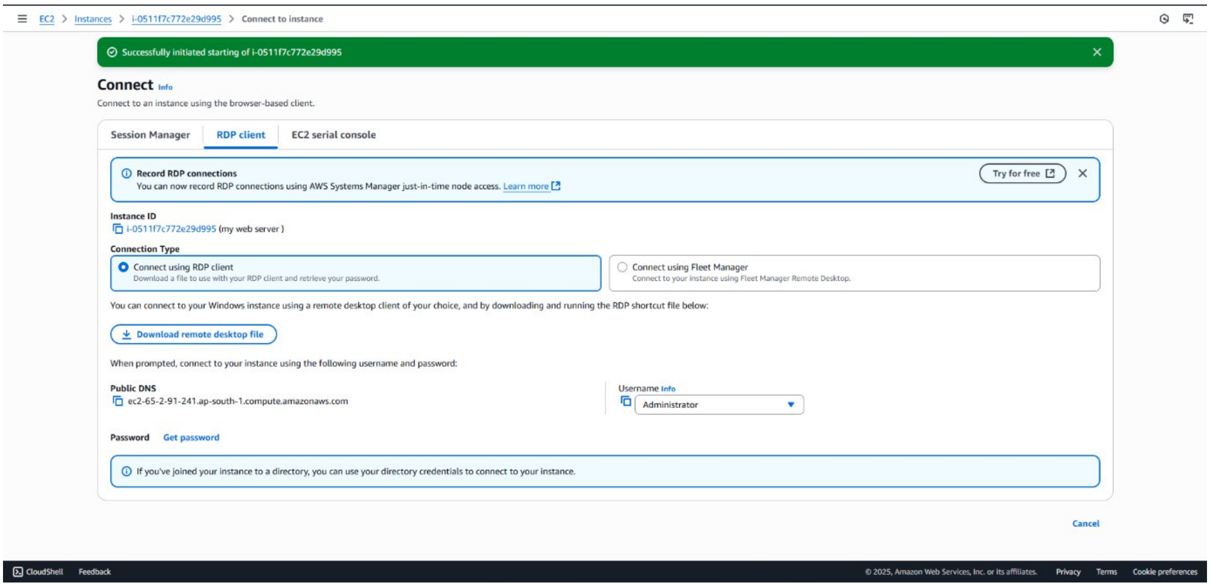
Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-6-46.ap-south-1.compute.internal

Private IPv4 addresses
172.31.6.46

Public DNS
ec2-65-2-91-241.ap-south-1.compute.amazonaws.com | open address

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



EC2 > Instances > i-0511f7c772e29d995 > Connect to instance

Successfully initiated starting of i-0511f7c772e29d995

Connect Info

Connect to an instance using the browser-based client.

Record RDP connections
You can now record RDP connections using AWS Systems Manager just-in-time node access. Learn more

Instance ID
i-0511f7c772e29d995 (my web server)

Connection Type

● Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

○ Connect using Fleet Manager
Connect to your instance using Fleet Manager Remote Desktop.

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following username and password:

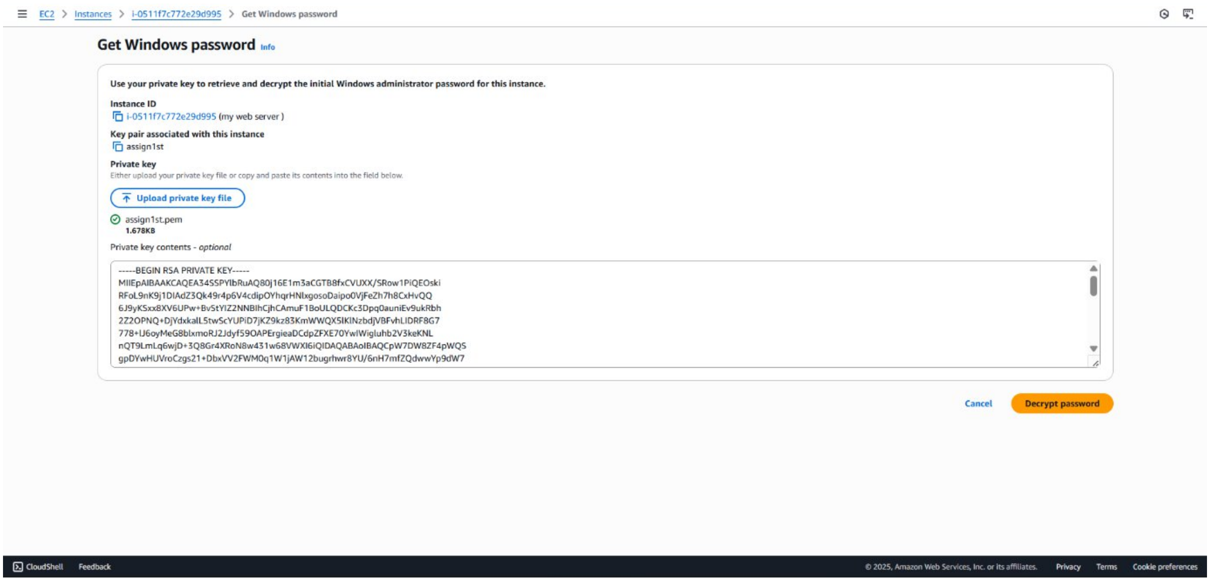
Public DNS
ec2-65-2-91-241.ap-south-1.compute.amazonaws.com

Username Info
Administrator

Password Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



EC2 > Instances > i-0511f7c772e29d995 > Get Windows password

Get Windows password Info

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID
i-0511f7c772e29d995 (my web server)

Key pair associated with this instance
assign1st

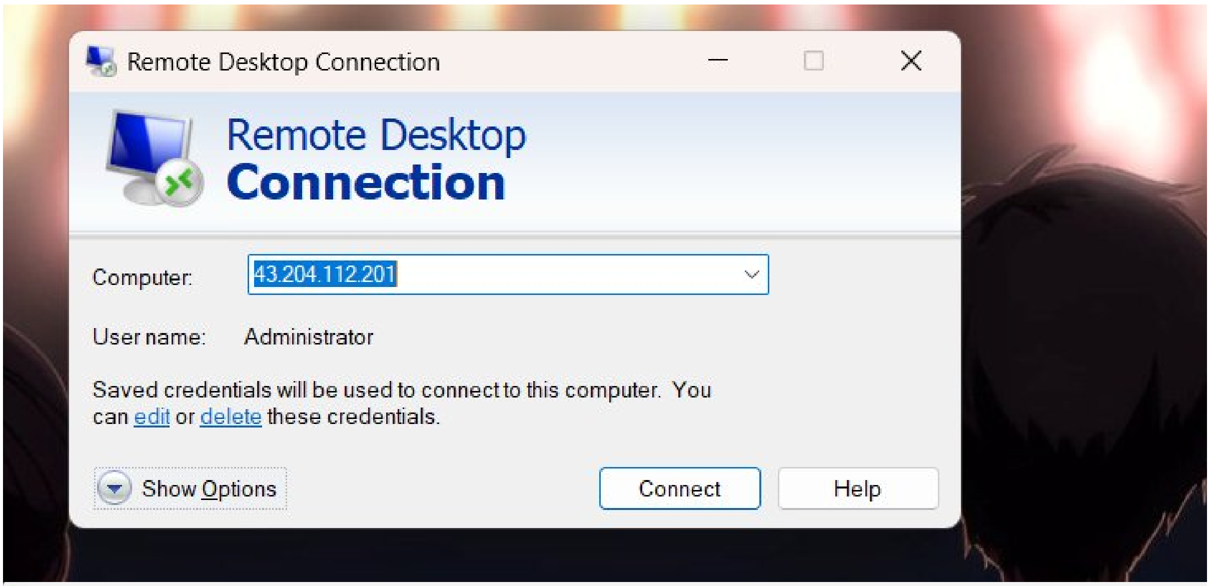
Private key
Either upload your private key file or copy and paste its contents into the field below.

assign1st.pem
1.678KB

Private key contents - *optional*

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA34SSPYlbRuAQ80j16E1m3aCGTB8fxCVUXX/SRow1PiQEOski
RFoL9nK9j1DIAdZ3Qk49r4p6V4cdipOYhqrHNlxgosoDaipo0VjFeZh7h8CxHvQQ
6J9yKSxx8XV6UPw+BvStYIZ2NNBIhCjhCAmuF1BoULQDCKc3Dpq0auniEv9ukRbh
2Z2OPNQ+DjYdxkalL5twScYUPiD7jKZ9kz83KmWWQX5IKINzbdjVBFvhLIDRF8G7
778+IJ6oyMeG8blxmoRJ2Jdyf59OAPErgieaDCdpZFXE70YwlWigluhb2V3keKNL
nQT9LmLq6wjD+3Q8Gr4XRoN8w431w68VWXI6iQIDAQABAoIBAQCpW7DW8ZF4pWQS
gpDYwHUVroCzgs21+DbxVV2FWM0q1W1jAW12bugrhwr8YU/6nH7mfZQdwwYp9dW7
```

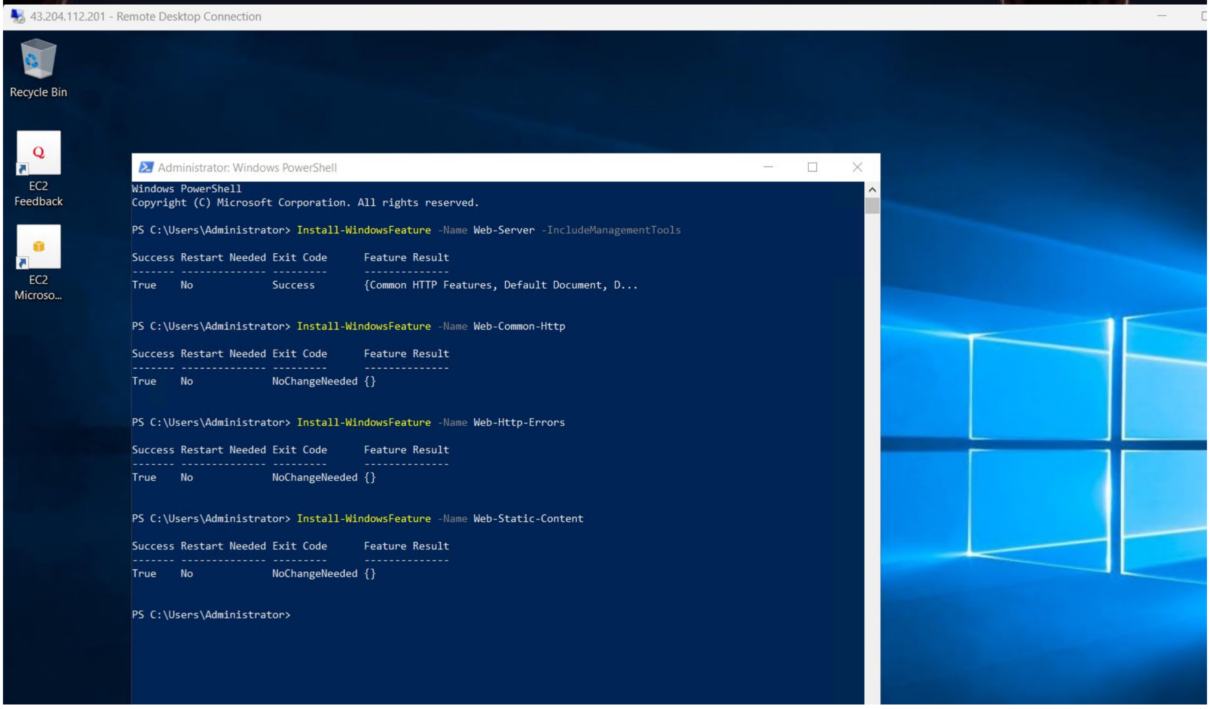
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



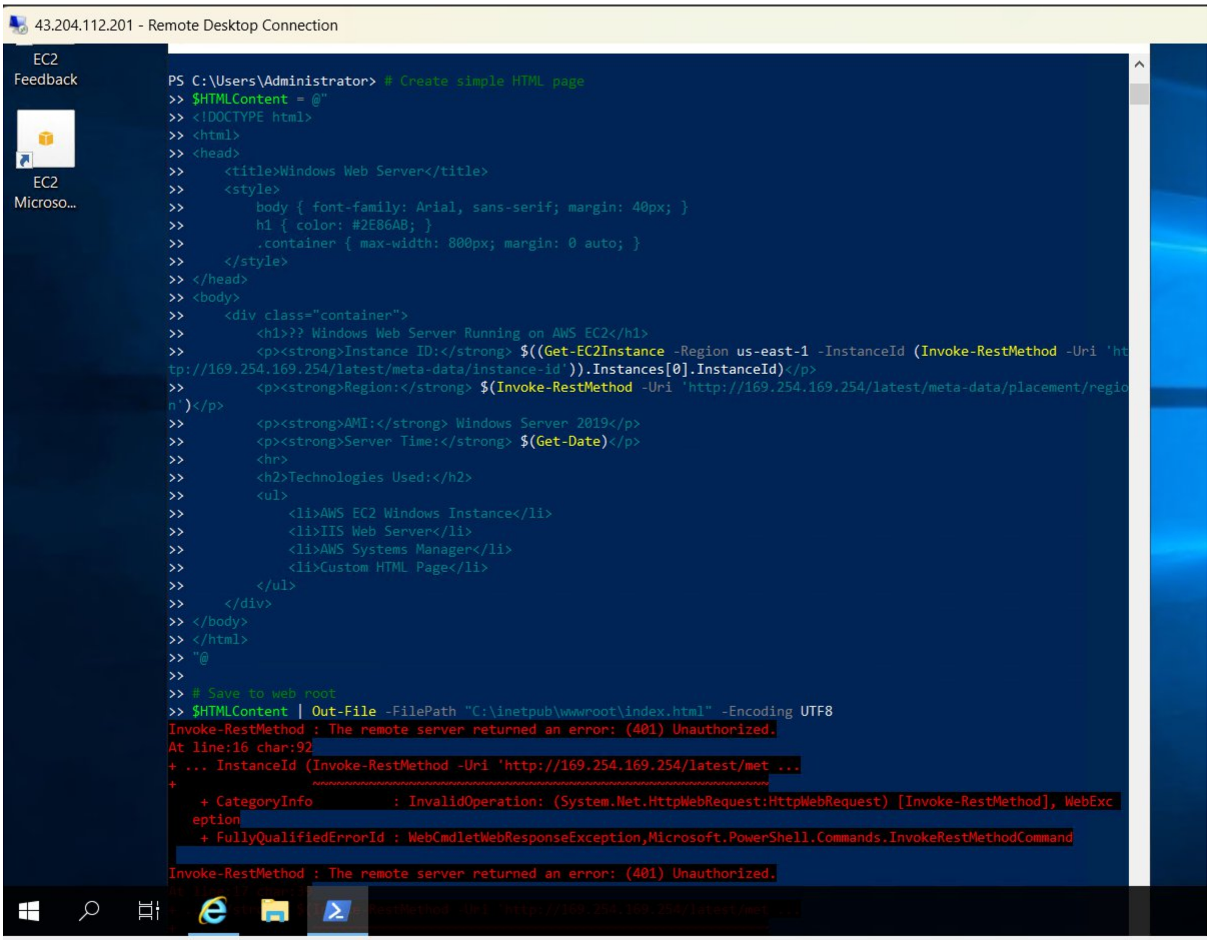
Computer: 43.204.112.201

User name: Administrator

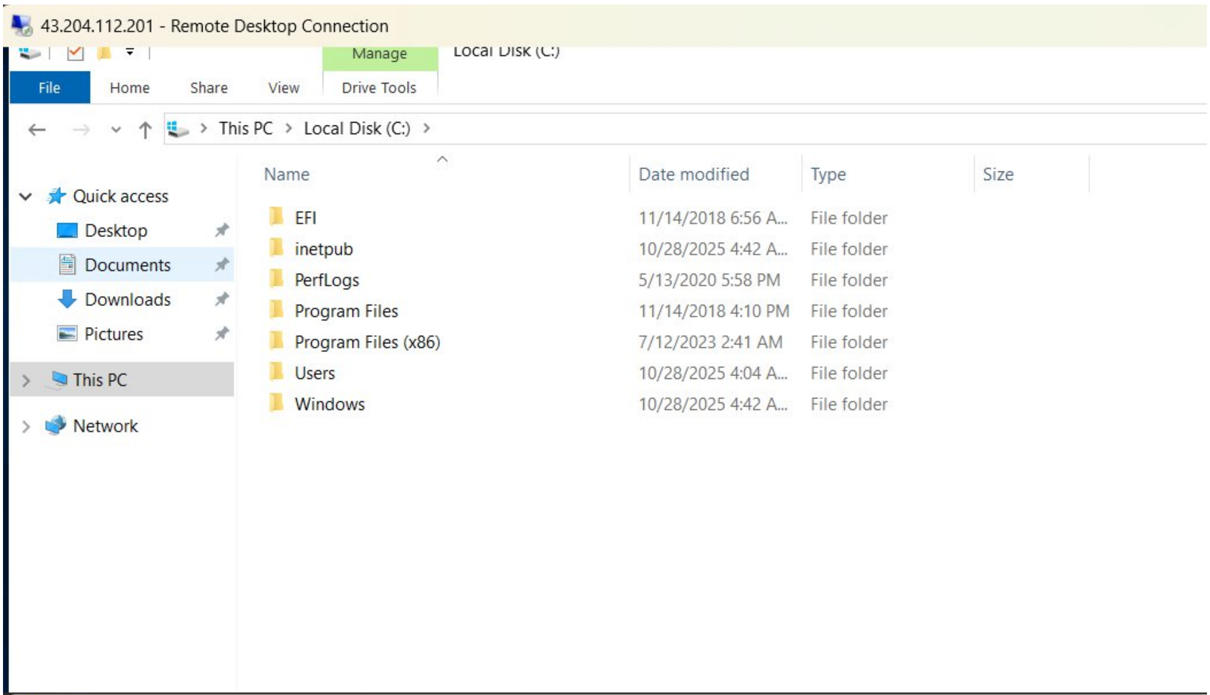
Saved credentials will be used to connect to this computer. You can edit or delete these credentials.


43.204.112.201 - Remote Desktop Connection
Recycle Bin
EC2
Feedback
EC2
Microso...
Administrator: Windows PowerShell

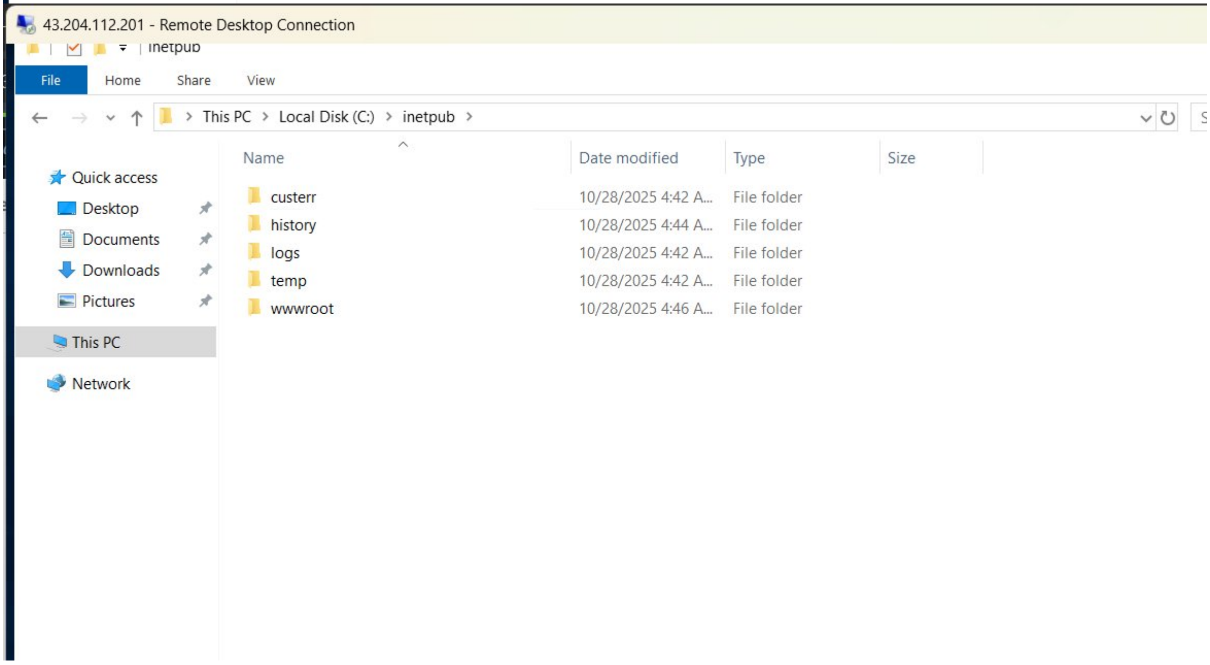
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Install-WindowsFeature -Name Web-Server -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Common HTTP Features, Default Document, D...


PS C:\Users\Administrator> Install-WindowsFeature -Name Web-Common-Http

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}


PS C:\Users\Administrator> Install-WindowsFeature -Name Web-Http-Errors

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}


PS C:\Users\Administrator> Install-WindowsFeature -Name Web-Static-Content

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}


PS C:\Users\Administrator>
```



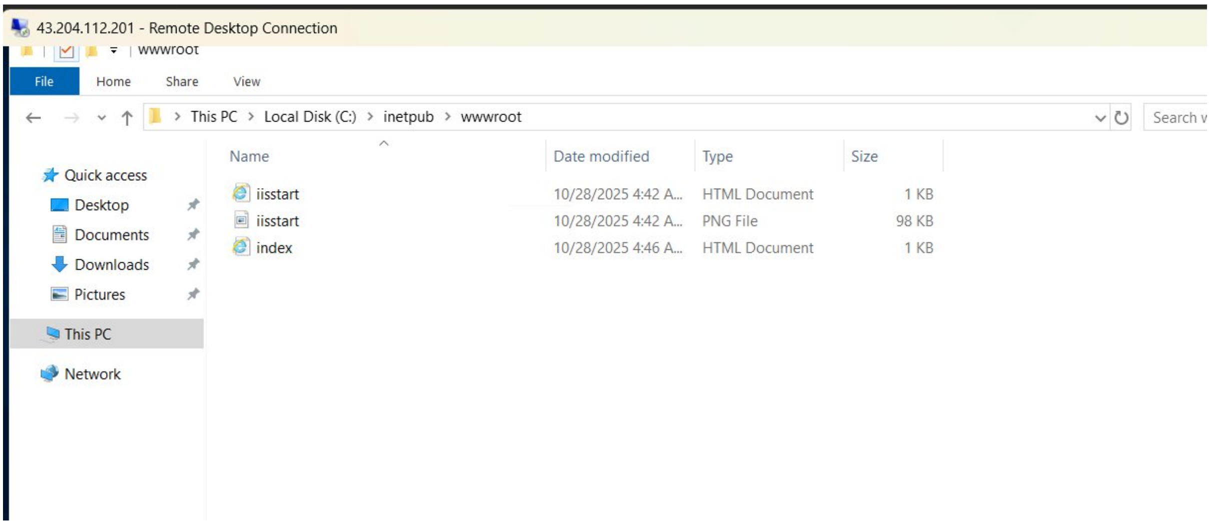
```
PS C:\Users\Administrator> # Create simple HTML page
>> $HTMLContent = @"
>> <!DOCTYPE html>
>> <html>
>> <head>
>>     <title>Windows Web Server</title>
>>     <style>
>>         body { font-family: Arial, sans-serif; margin: 40px; }
>>         h1 { color: #2E86AB; }
>>         .container { max-width: 800px; margin: 0 auto; }
>>     </style>
>> </head>
>> <body>
>>     <div class="container">
>>         <h1>?? Windows Web Server Running on AWS EC2</h1>
>>         <p><strong>Instance ID:</strong> $((Get-EC2Instance -Region us-east-1 -InstanceId (Invoke-RestMethod -Uri 'ht
tp://169.254.169.254/latest/meta-data/instance-id')).Instances[0].InstanceId)</p>
>>         <p><strong>Region:</strong> $(Invoke-RestMethod -Uri 'http://169.254.169.254/latest/meta-data/placement/regio
n')</p>
>>         <p><strong>AMI:</strong> Windows Server 2019</p>
>>         <p><strong>Server Time:</strong> $(Get-Date)</p>
>>         <hr>
>>         <h2>Technologies Used:</h2>
>>         <ul>
>>             <li>AWS EC2 Windows Instance</li>
>>             <li>IIS Web Server</li>
>>             <li>AWS Systems Manager</li>
>>             <li>Custom HTML Page</li>
>>         </ul>
>>     </div>
>> </body>
>> </html>
>> "@
>>
>> # Save to web root
>> $HTMLContent | Out-File -FilePath "C:\inetpub\wwwroot\index.html" -Encoding UTF8
Invoke-RestMethod : The remote server returned an error: (401) Unauthorized.
At line:16 char:92
+ ... InstanceId (Invoke-RestMethod -Uri 'http://169.254.169.254/latest/met ...
+                  ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-RestMethod], WebExc
   eption
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeRestMethodCommand

Invoke-RestMethod : The remote server returned an error: (401) Unauthorized.
```



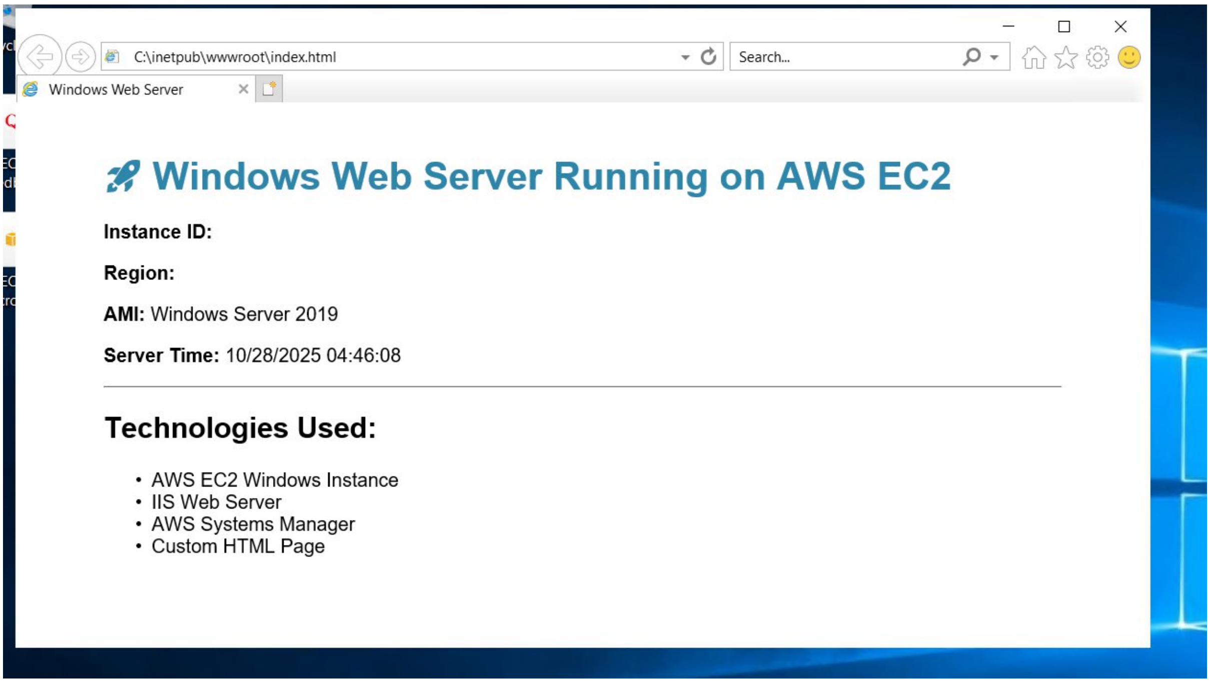
Name	Date modified	Type	Size
EFI	11/14/2018 6:56 A...	File folder	
inetpub	10/28/2025 4:42 A...	File folder	
PerfLogs	5/13/2020 5:58 PM	File folder	
Program Files	11/14/2018 4:10 PM	File folder	
Program Files (x86)	7/12/2023 2:41 AM	File folder	
Users	10/28/2025 4:04 A...	File folder	
Windows	10/28/2025 4:42 A...	File folder	



Name	Date modified	Type	Size
custerr	10/28/2025 4:42 A...	File folder	
history	10/28/2025 4:44 A...	File folder	
logs	10/28/2025 4:42 A...	File folder	
temp	10/28/2025 4:42 A...	File folder	
wwwroot	10/28/2025 4:46 A...	File folder	



Name	Date modified	Type	Size
iisstart	10/28/2025 4:42 A...	HTML Document	1 KB
iisstart	10/28/2025 4:42 A...	PNG File	98 KB
index	10/28/2025 4:46 A...	HTML Document	1 KB



🚀 Windows Web Server Running on AWS EC2

Instance ID:

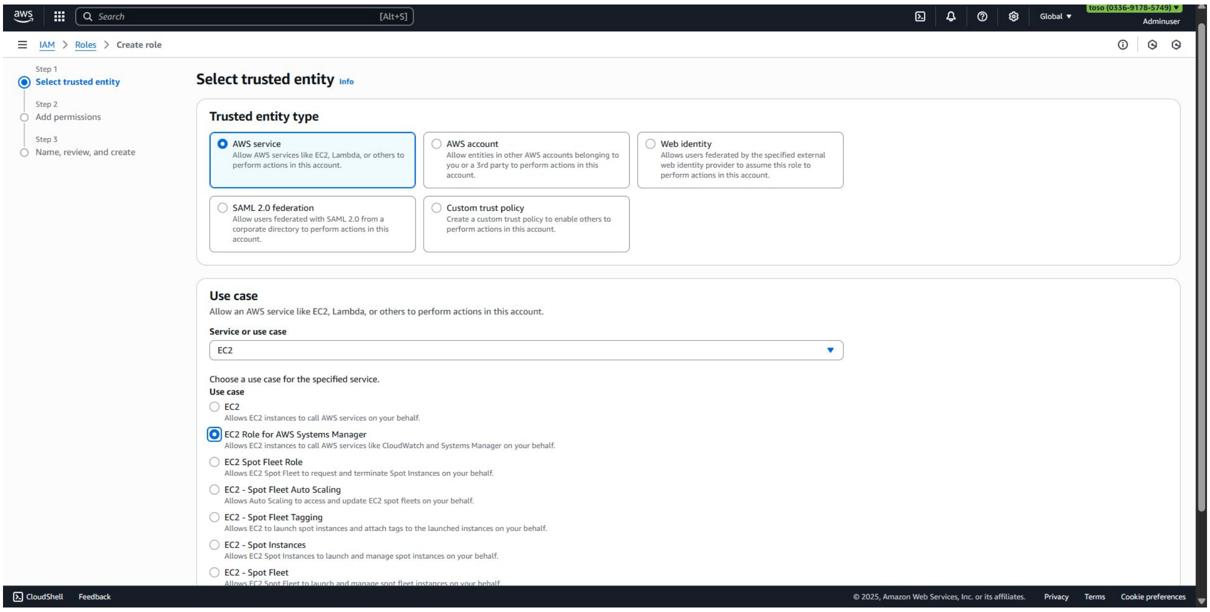
Region:

AMI: Windows Server 2019

Server Time: 10/28/2025 04:46:08

Technologies Used:

- AWS EC2 Windows Instance
- IIS Web Server
- AWS Systems Manager
- Custom HTML Page



Step 1
● Select trusted entity

Step 2
○ Add permissions

Step 3
○ Name, review, and create

Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2 ▾

Choose a use case for the specified service.

Use case

○ EC2
Allows EC2 instances to call AWS services on your behalf.

● EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

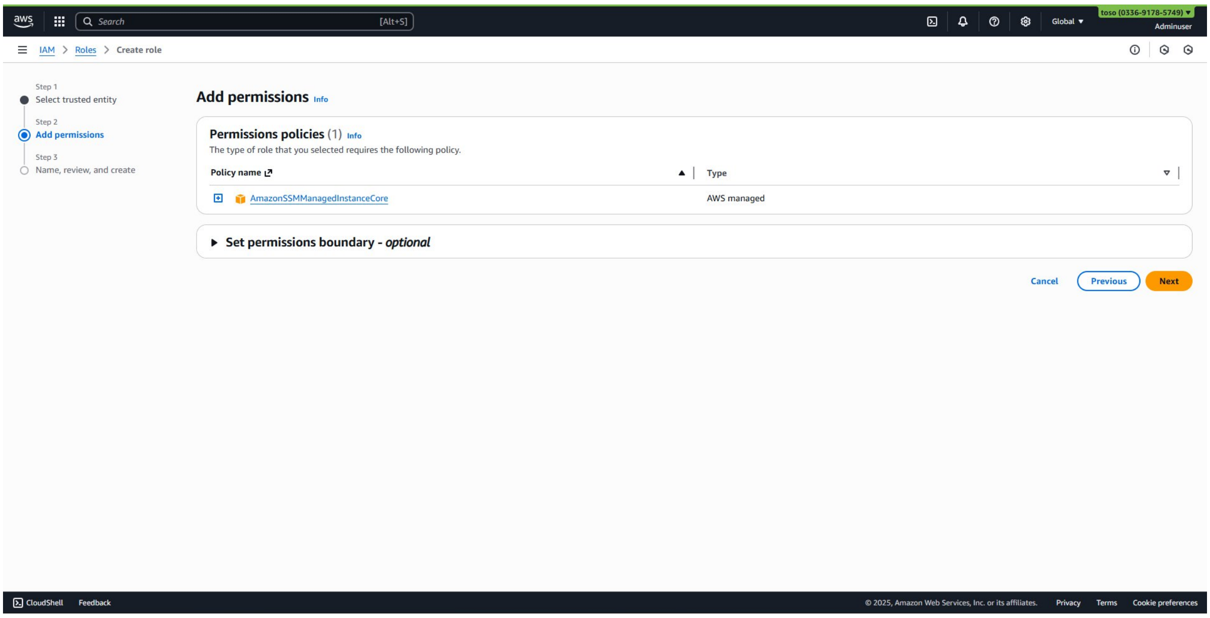
○ EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

○ EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

○ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

○ EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

○ EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.



Step 1
● Select trusted entity

Step 2
● Add permissions

Step 3
○ Name, review, and create

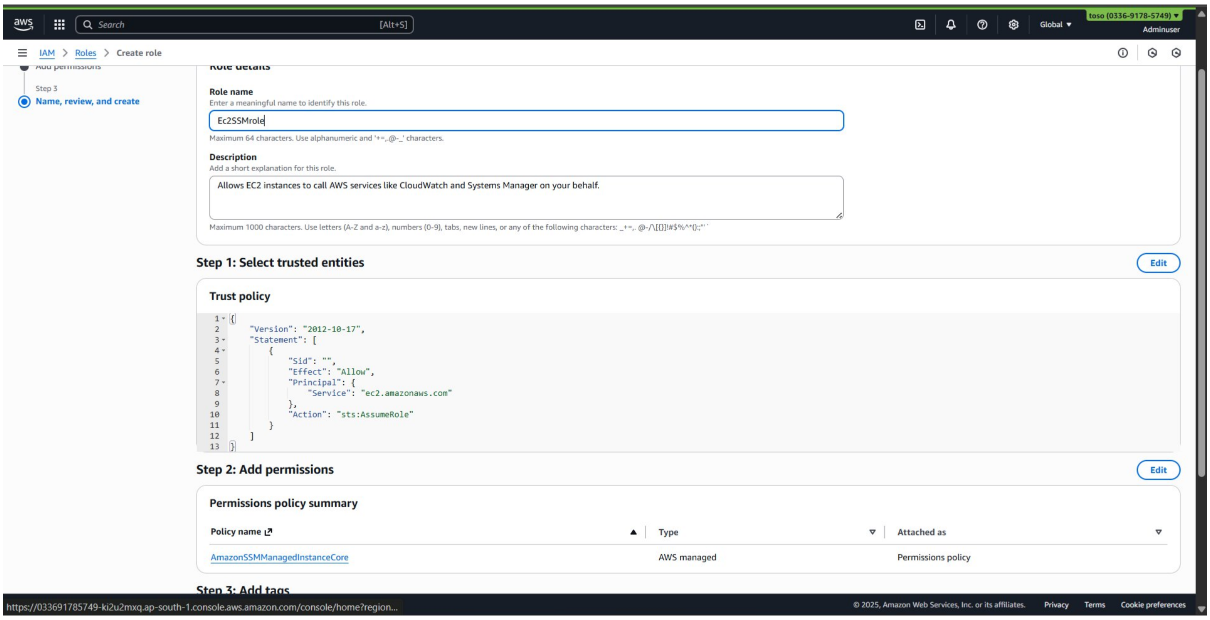
Add permissions Info

Permissions policies (1) Info

The type of role that you selected requires the following policy.

Policy name	Type
AmazonSSMManagedInstanceCore	AWS managed

▶ **Set permissions boundary - *optional***



Role details

Role name
Enter a meaningful name to identify this role.

Ec2SSMrole

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*();:"'`

Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

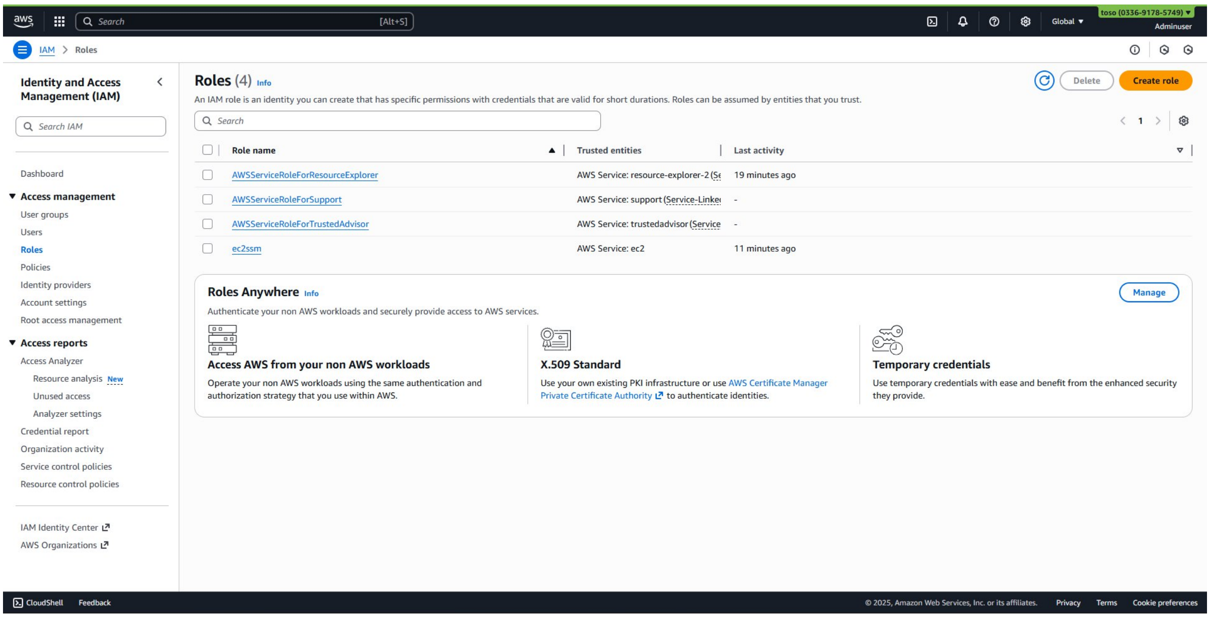
Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonSSMManagedInstanceCore	AWS managed	Permissions policy

Step 3: Add tags

https://033691785749-ki2u2mxq.ap-south-1.console.aws.amazon.com/console/home?region...
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Roles (4) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last activity
□	AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Se	19 minutes ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
□	ec2ssm	AWS Service: ec2	11 minutes ago

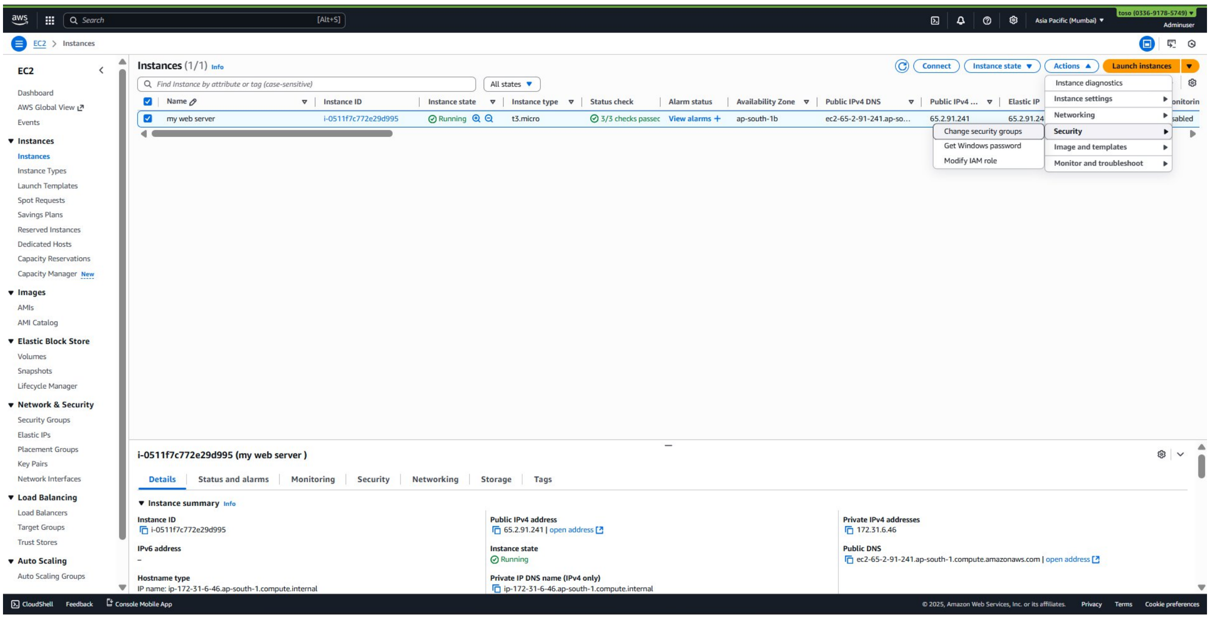
Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.



Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive) | All states

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	onitorin
☑	my web server	i-0511f7c772e29d995	✓ Running	t3.micro	✓ 3/3 checks passec	View alarms +	ap-south-1b	ec2-65-2-91-241.ap-so...	65.2.91.241	65.2.91.24	sabled

i-0511f7c772e29d995 (my web server)

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

Instance summary Info

Instance ID
i-0511f7c772e29d995

IPv6 address
–

Hostname type
IP name: ip-172-31-6-46.ap-south-1.compute.internal

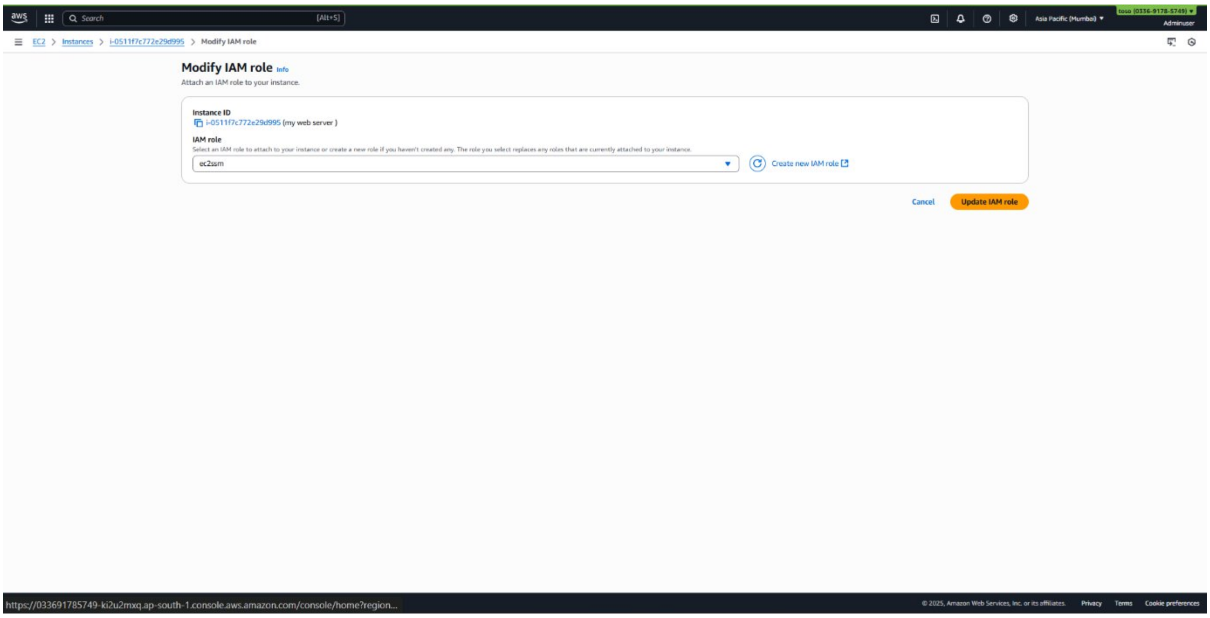
Public IPv4 address
65.2.91.241 | open address

Instance state
✓ Running

Private IP DNS name (IPv4 only)
ip-172-31-6-46.ap-south-1.compute.internal

Private IPv4 addresses
172.31.6.46

Public DNS
ec2-65-2-91-241.ap-south-1.compute.amazonaws.com | open address

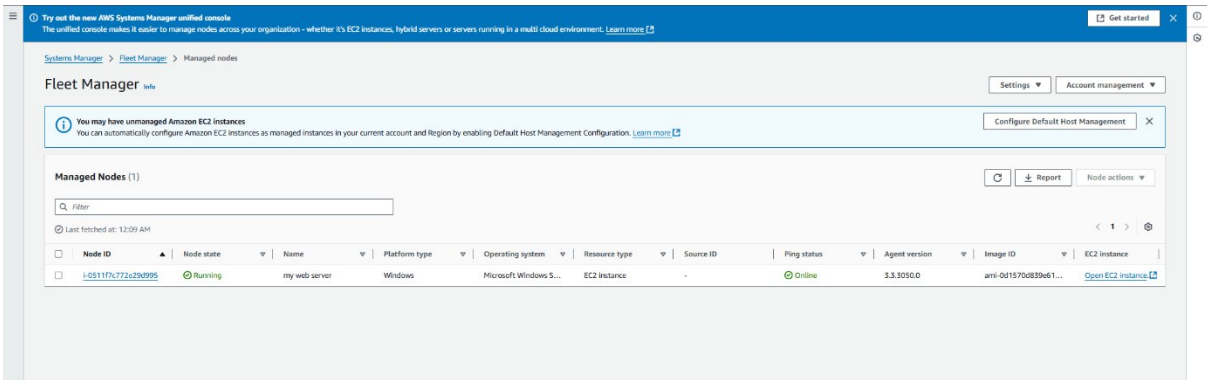

aws
Search [Alt+S]
Asia Pacific (Mumbai)
toso (0336-9178-5749)
Adminuser
EC2 > Instances > i-0511f7c772e29d995 > Modify IAM role
Create new IAM role
Cancel
Update IAM role
https://033691785749-ki2u2mxq.ap-south-1.console.aws.amazon.com/console/home?region...
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Modify IAM role Info

Attach an IAM role to your instance.

Instance ID
i-0511f7c772e29d995 (my web server)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.
ec2ssm


Get started
Systems Manager > Fleet Manager > Managed nodes
Settings
Account management
Configure Default Host Management
Report
Node actions

Try out the new AWS Systems Manager unified console
The unified console makes it easier to manage nodes across your organization - whether it's EC2 instances, hybrid servers or servers running in a multi cloud environment. Learn more

Fleet Manager Info

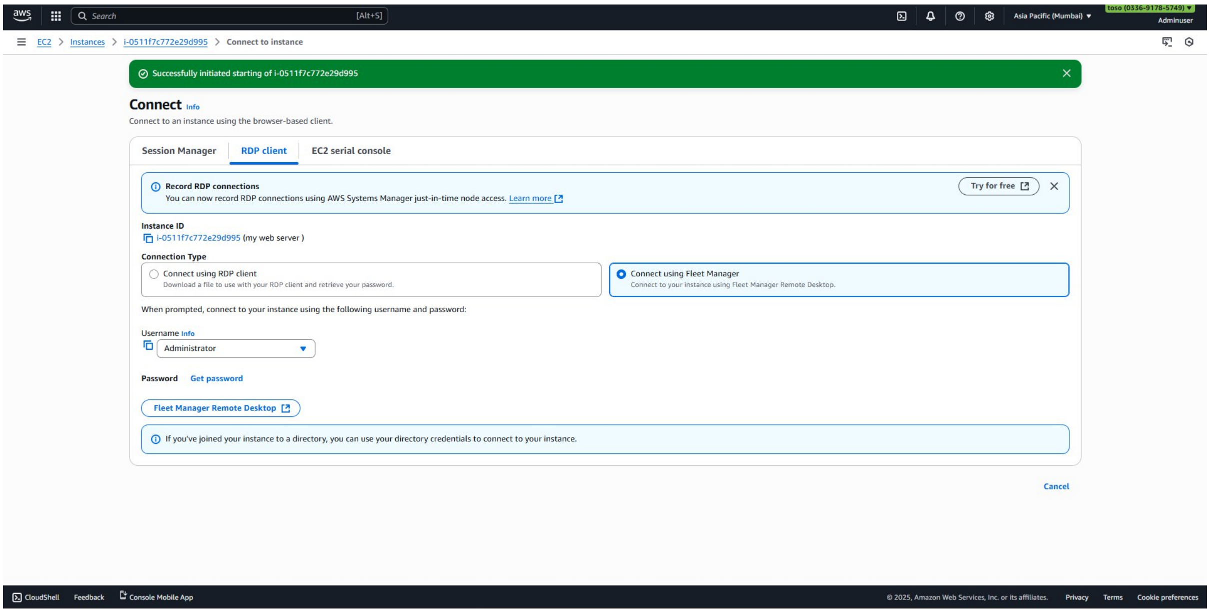
You may have unmanaged Amazon EC2 instances
You can automatically configure Amazon EC2 instances as managed instances in your current account and Region by enabling Default Host Management Configuration. Learn more

Managed Nodes (1)

Filter

Last fetched at: 12:09 AM

□	Node ID	Node state	Name	Platform type	Operating system	Resource type	Source ID	Ping status	Agent version	Image ID	EC2 instance
□	i-0511f7c772e29d995	✓ Running	my web server	Windows	Microsoft Windows S...	EC2 instance	-	✓ Online	3.3.3050.0	ami-0d1570d839e61...	Open EC2 instance



Successfully initiated starting of i-0511f7c772e29d995

Connect Info

Connect to an instance using the browser-based client.

Record RDP connections
You can now record RDP connections using AWS Systems Manager just-in-time node access. Learn more

Instance ID
i-0511f7c772e29d995 (my web server)

Connection Type

○ Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

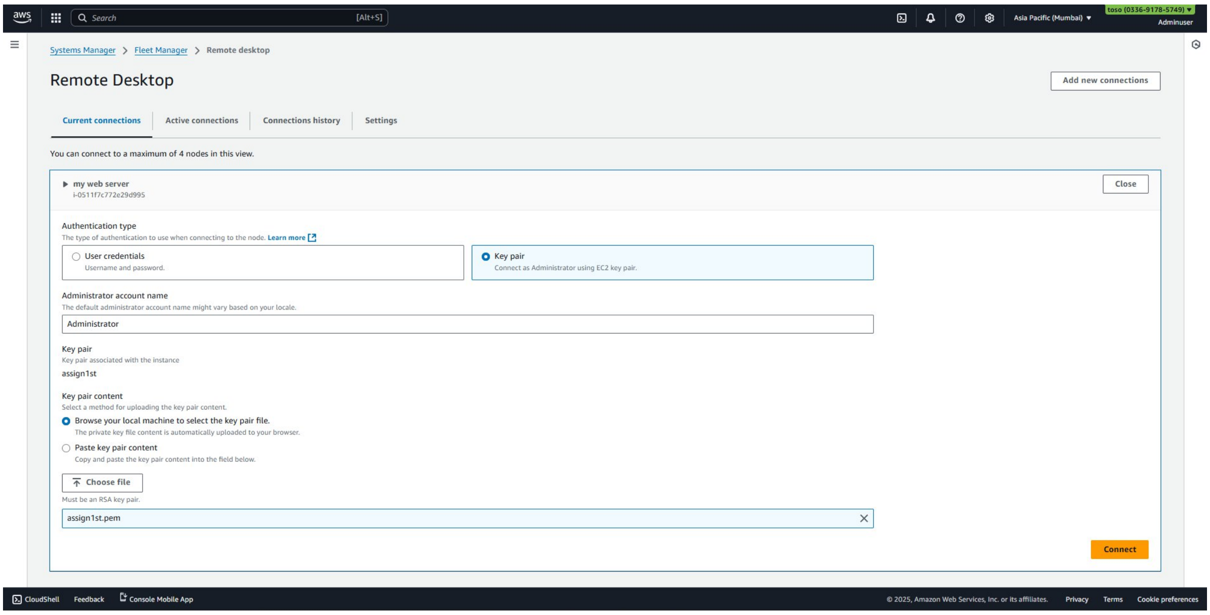
● Connect using Fleet Manager
Connect to your instance using Fleet Manager Remote Desktop.

When prompted, connect to your instance using the following username and password:

Username Info
Administrator ▾

Password Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.



Remote Desktop

You can connect to a maximum of 4 nodes in this view.

▸ my web server
i-0511f7c772e29d995

Authentication type
The type of authentication to use when connecting to the node. Learn more

○ User credentials
Username and password.

● Key pair
Connect as Administrator using EC2 key pair.

Administrator account name
The default administrator account name might vary based on your locale.
Administrator

Key pair
Key pair associated with the instance
assign1st

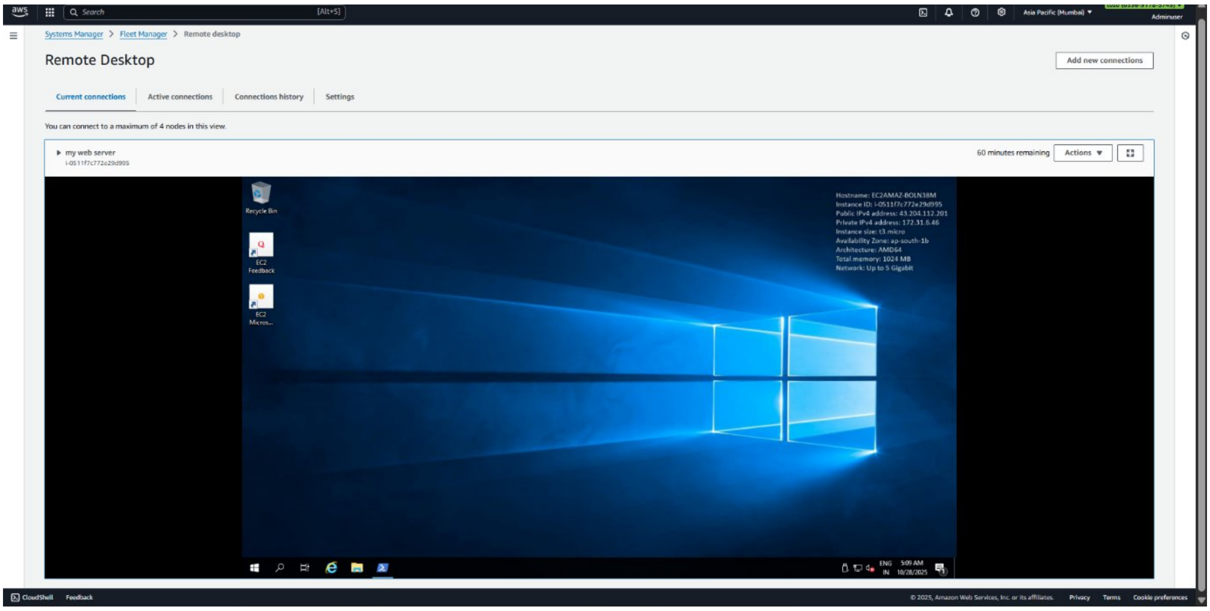
Key pair content
Select a method for uploading the key pair content.

● Browse your local machine to select the key pair file.
The private key file content is automatically uploaded to your browser.

○ Paste key pair content
Copy and paste the key pair content into the field below.

Must be an RSA key pair.

assign1st.pem



Systems Manager > Fleet Manager > Remote desktop

Remote Desktop

You can connect to a maximum of 4 nodes in this view.

my web server
i-0511f7c772e29d995

60 minutes remaining

Hostname: EC2AMAZ-BOLN38M
Instance ID: i-0511f7c772e29d995
Public IPv4 address: 43.204.112.201
Private IPv4 address: 172.31.6.46
Instance size: t3.micro
Availability Zone: ap-south-1b
Architecture: AMD64
Total memory: 1024 MB
Network: Up to 5 Gigabit

© 2025, Amazon Web Services, Inc. or its affiliates.