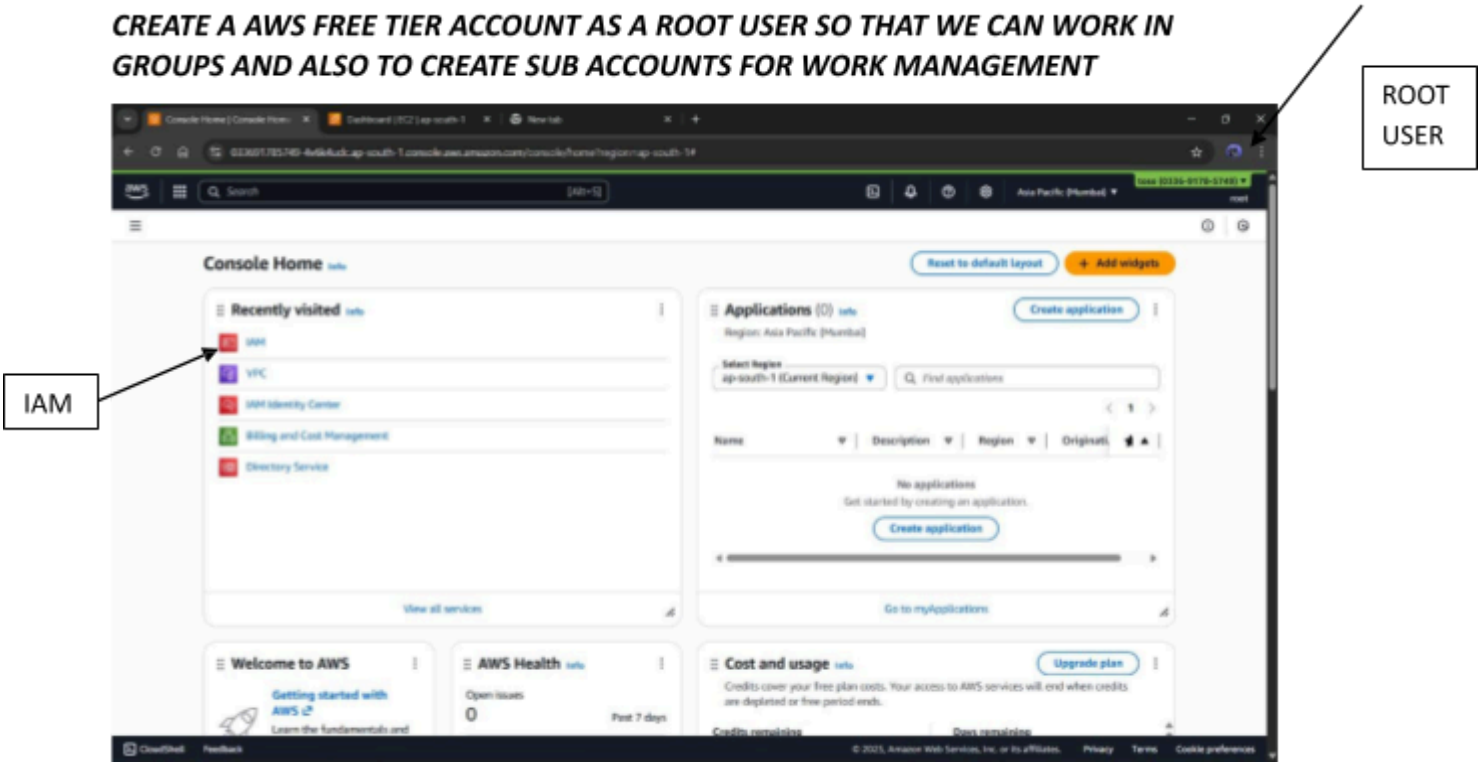
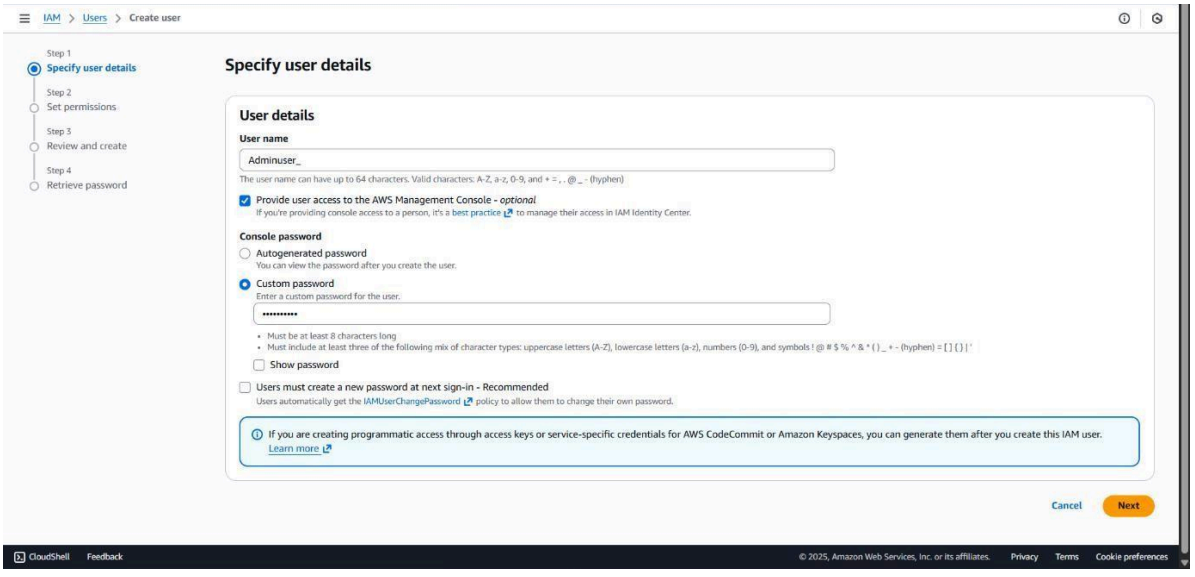
AWS ASSIGNMENT 1ST

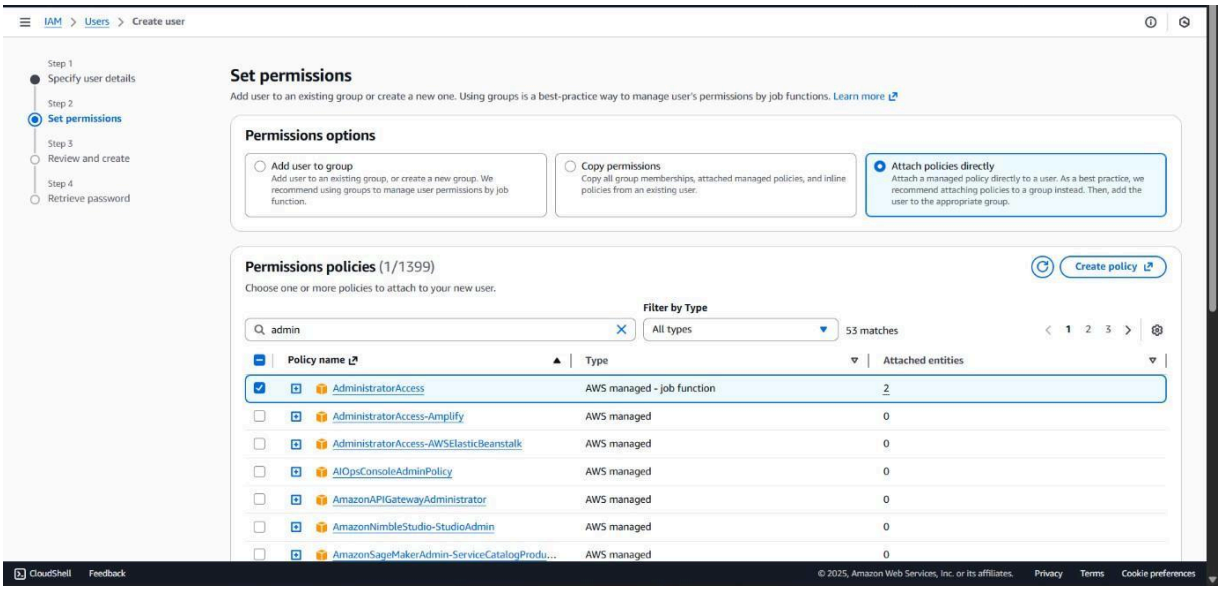
STEP 1 & 2:-

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

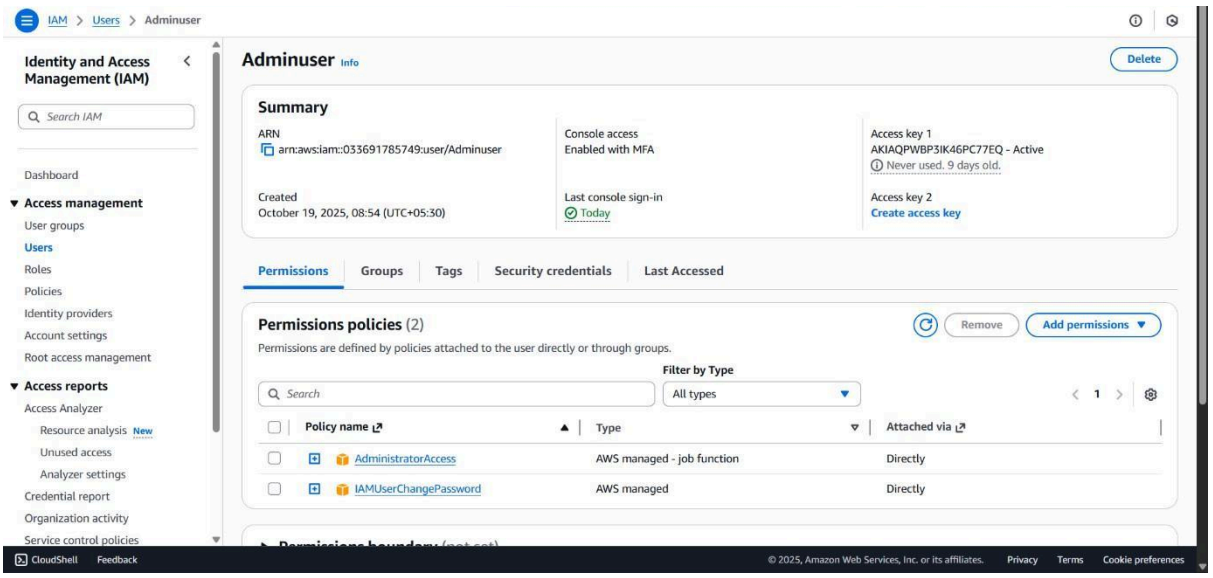


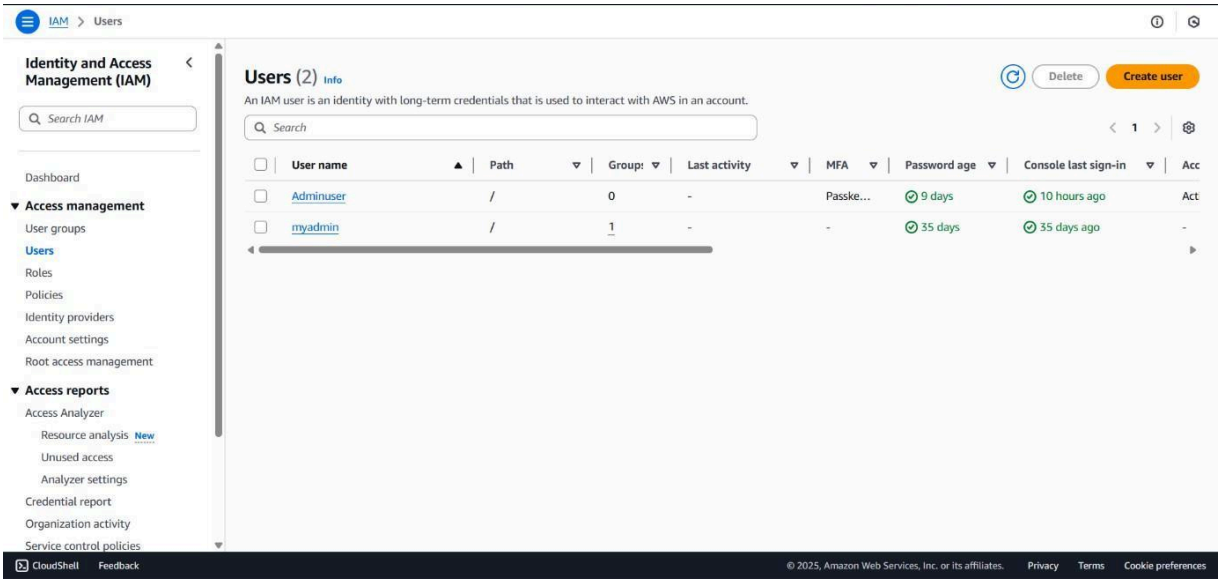
NOW WE GO TO IAM AND CREATE A USER THERE TO WORK WITH WE DON'T USE OUR ROOT ACCOUNT FOR WORKING WE CREATE USERS THERE FOR WORK WE USE DIFFERENT USERS FOR DIFFERENT WORK THIS WILL HELP US TO MANAGE THE BILLING AND POLICIES EASILY ROOT IS UESD TO MANAGE THOSE IAM ACCOUNT IT'S LIKE A BOSS IS RUNNING THE COMPANY HE WILL PAY AND GET THE WORK DONE BUT HE WILL NOT WORK





- 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

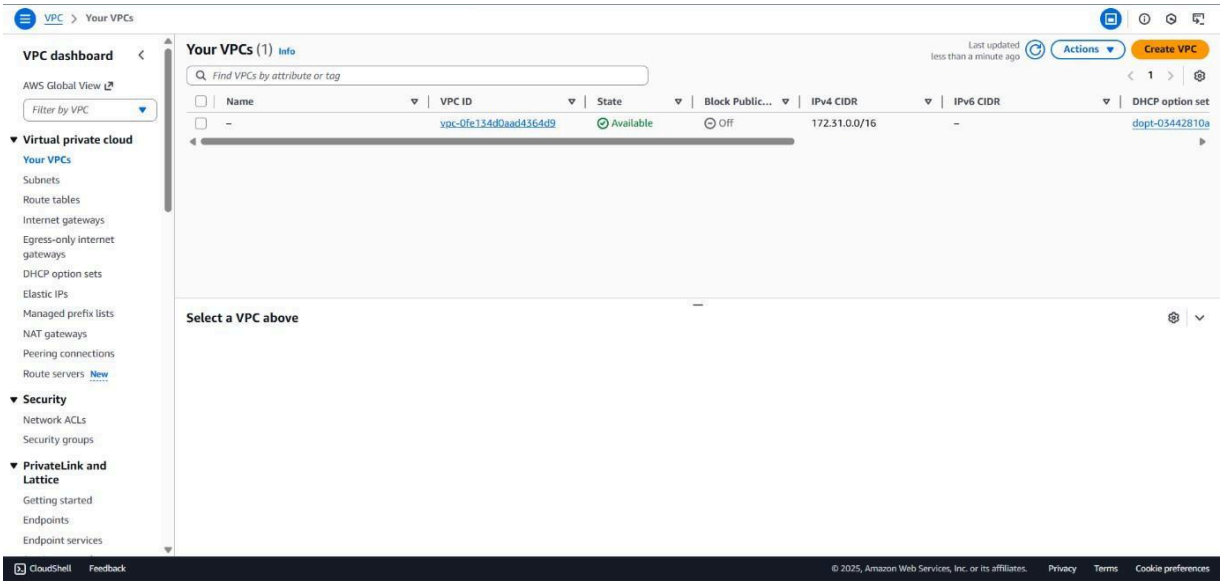




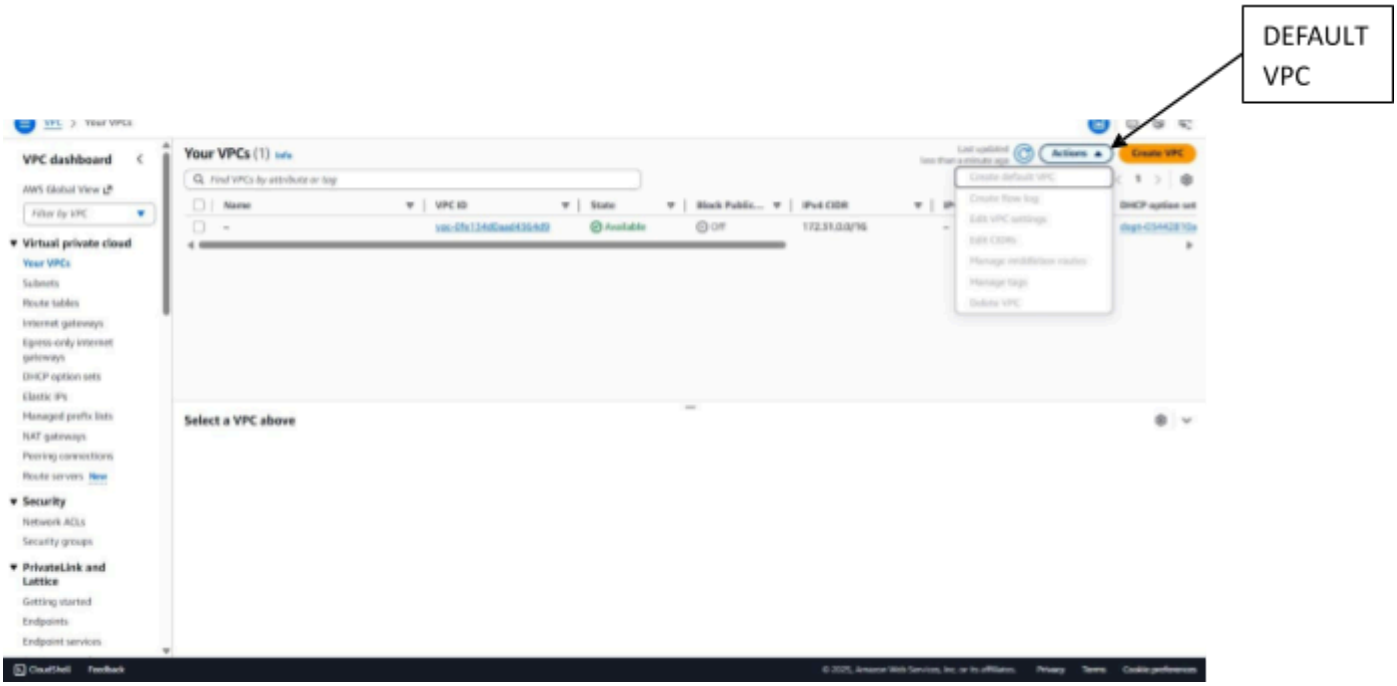
STEP 3

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

- IF YOU DELETED THE VPC AND WANT TO CREATE YOU OWN SO YOU CAN DO THAT

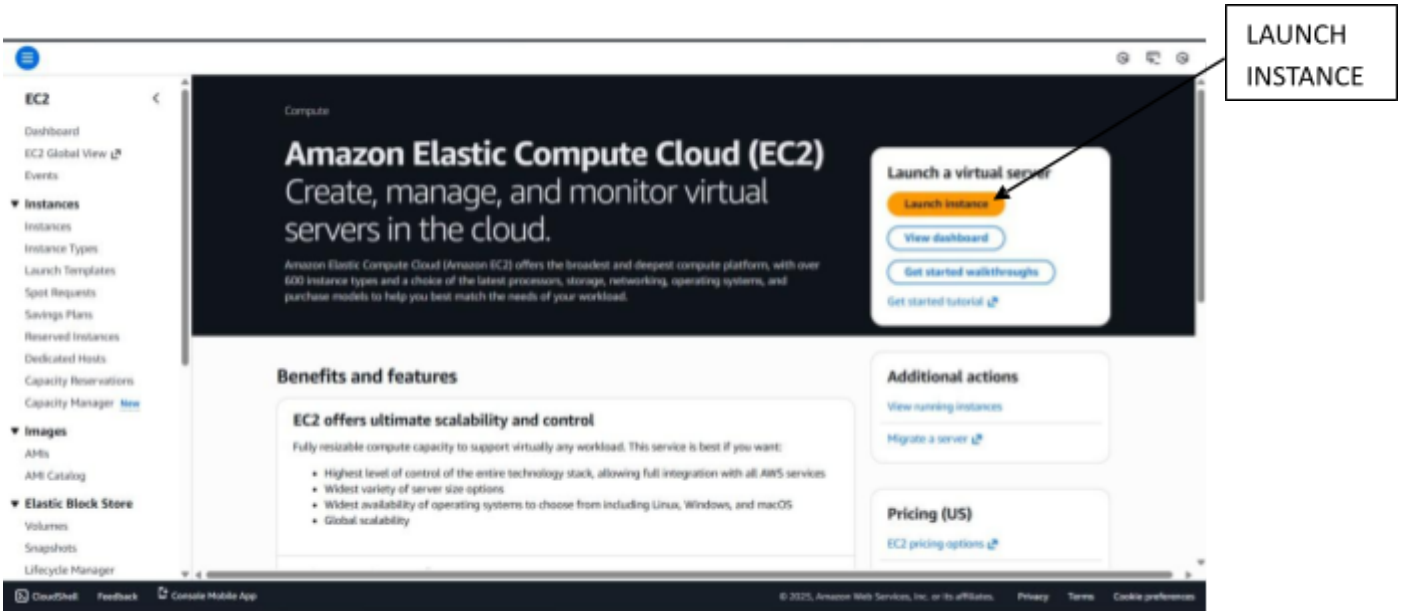


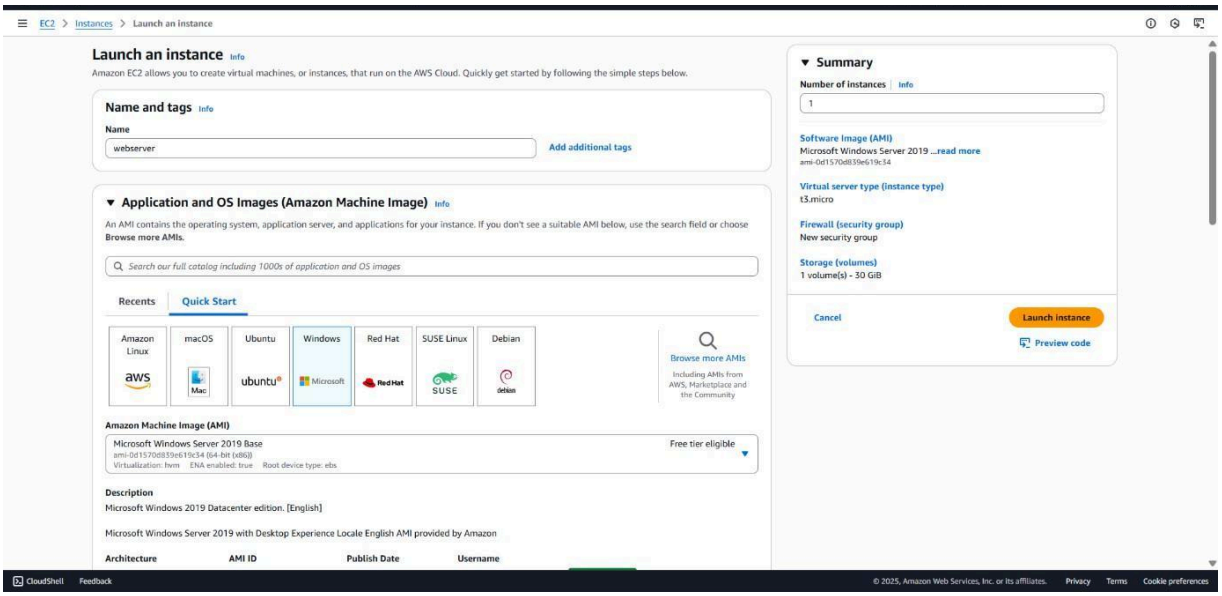
AND IF YOU AREN'T ABLE TO CREATE VPC SO YOU CAN CREATE A DEFAULT VPC AGAIN YOU CAN SEE IT HERE



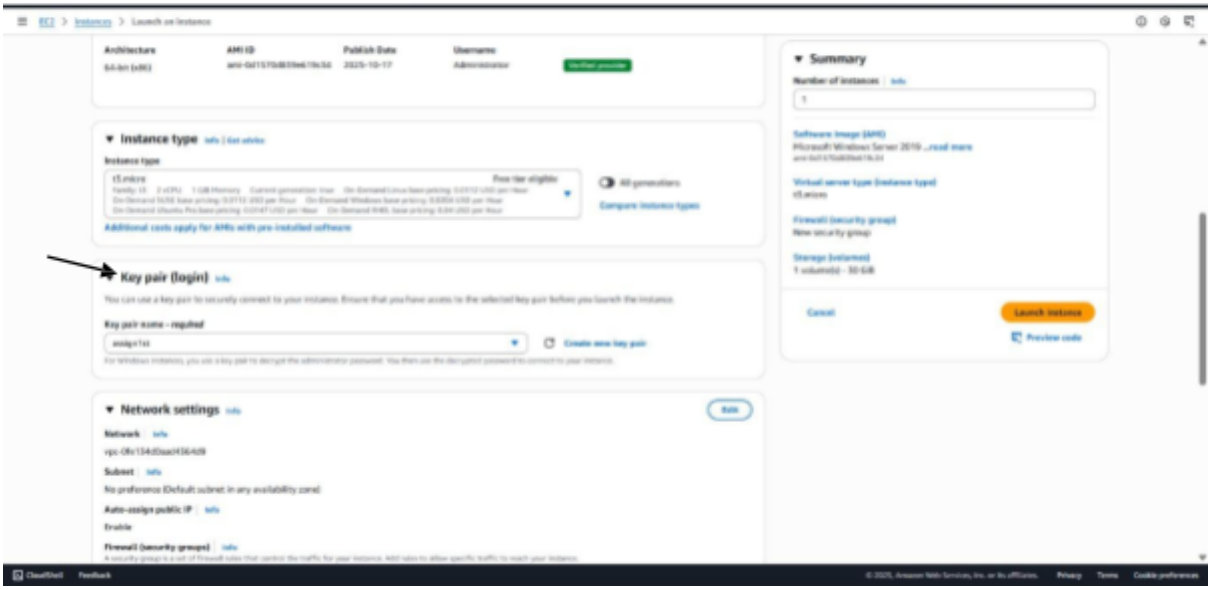
STEP 4 ,5 & 6

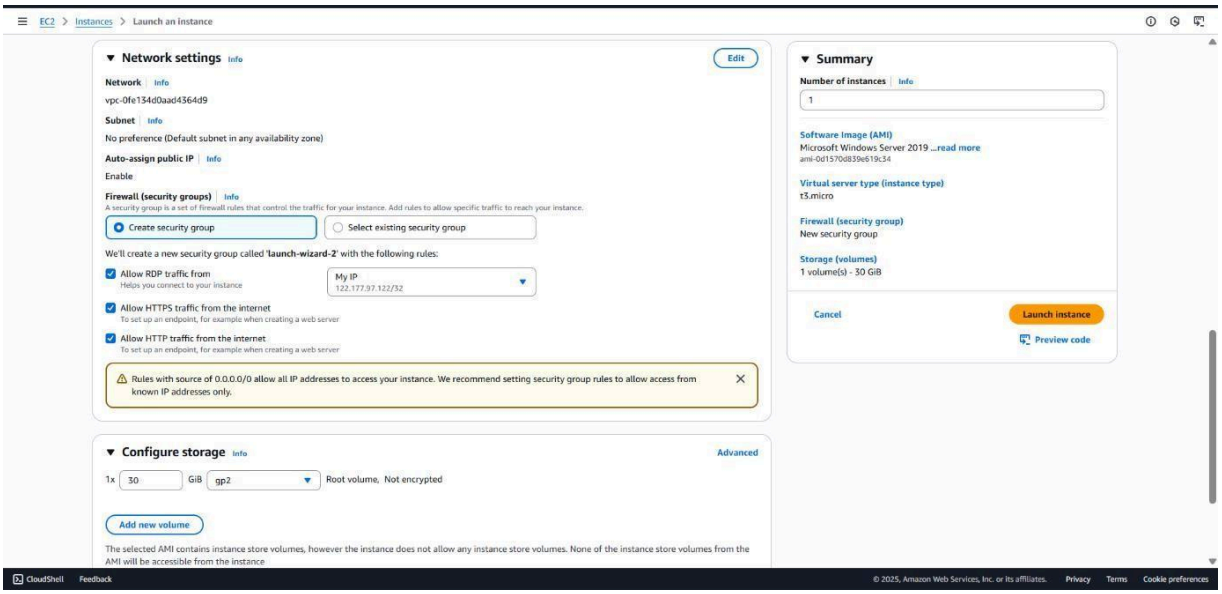
IN THIS WE WILL CREATE A EC2 INSTANCE TO RUN OUR WEBSITE AND ALSO WE PERFORM RDP WITH ACCESS KEY PAIR AND BY FLEET MANAGER

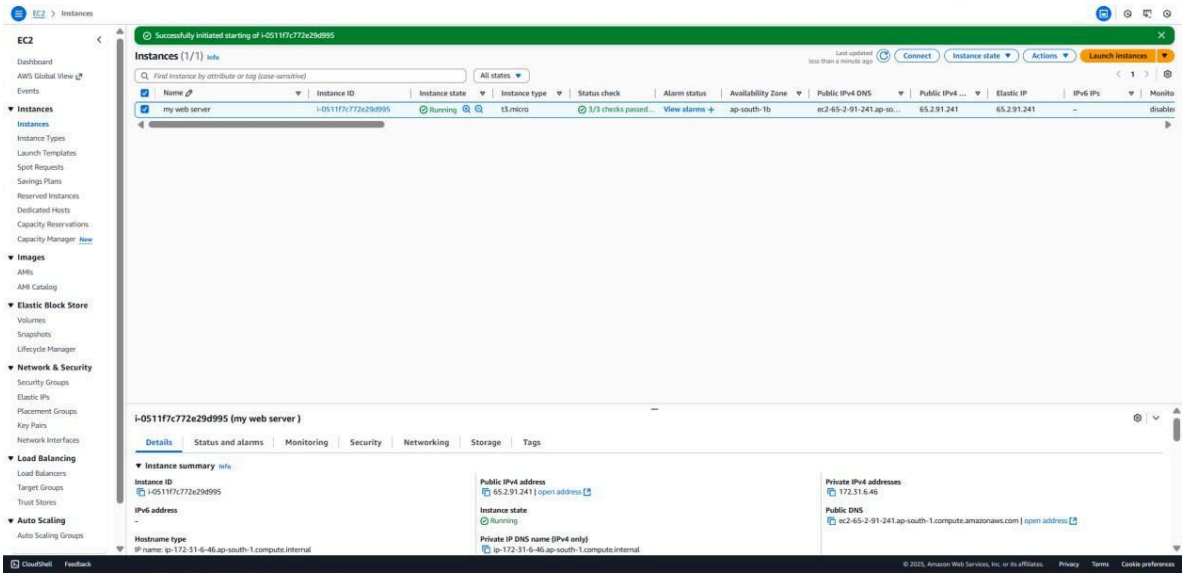


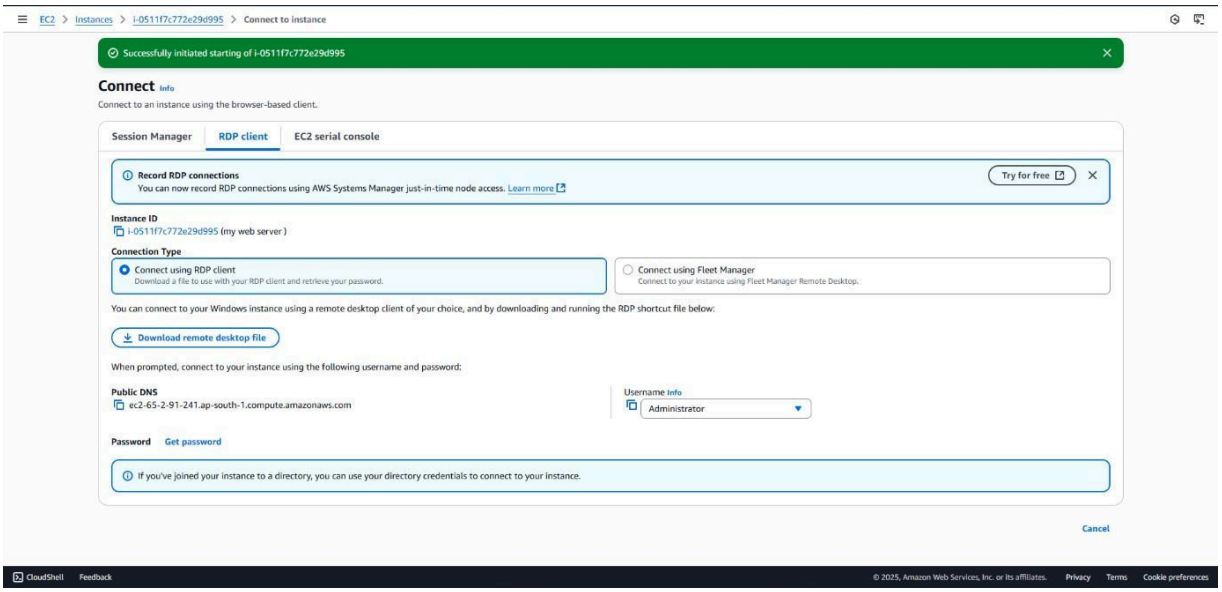


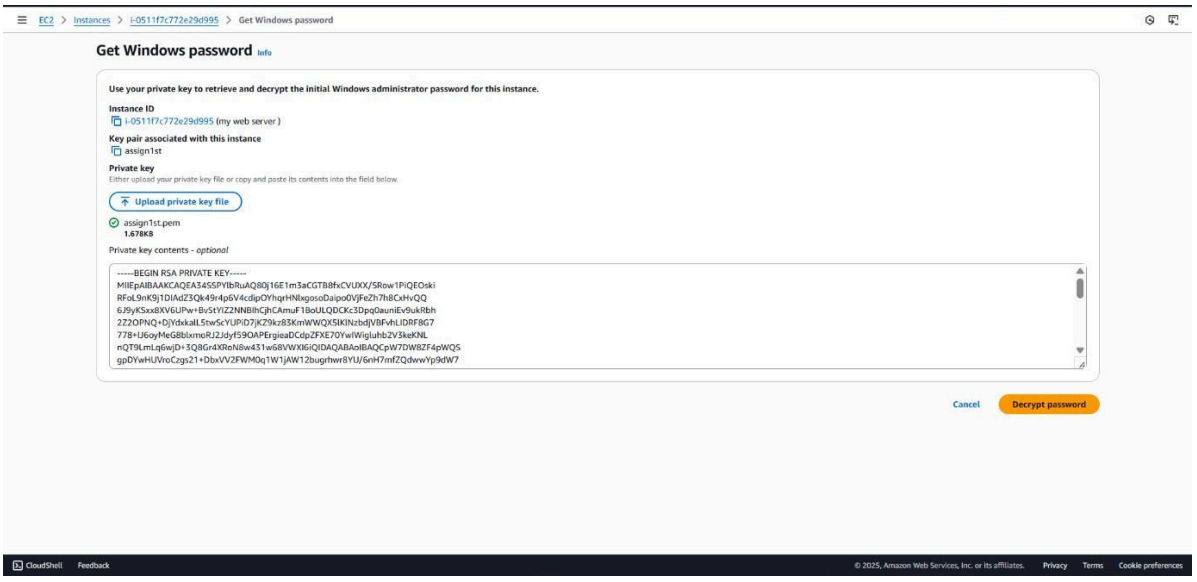
CREATE NEW KEY PAIR

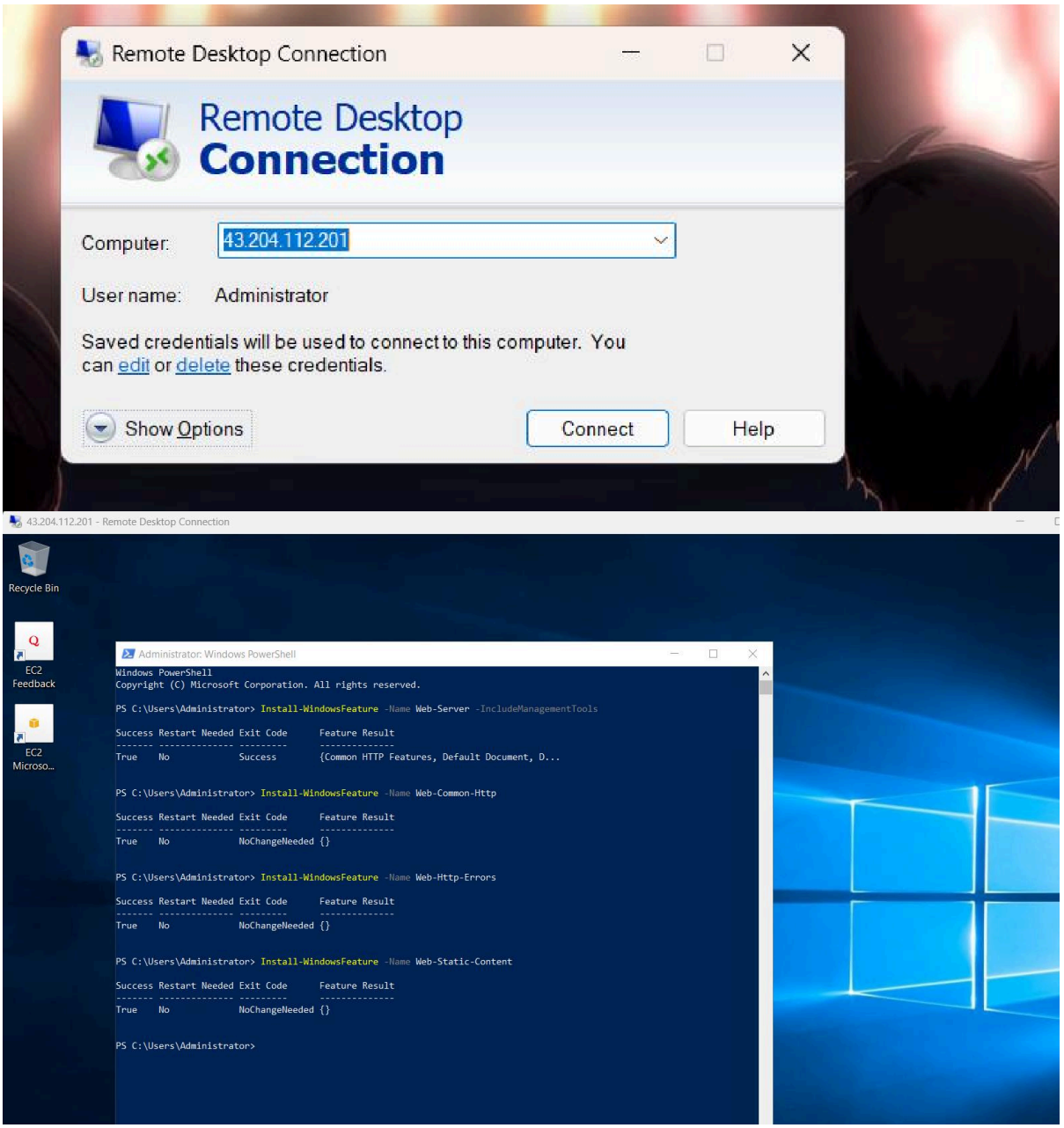


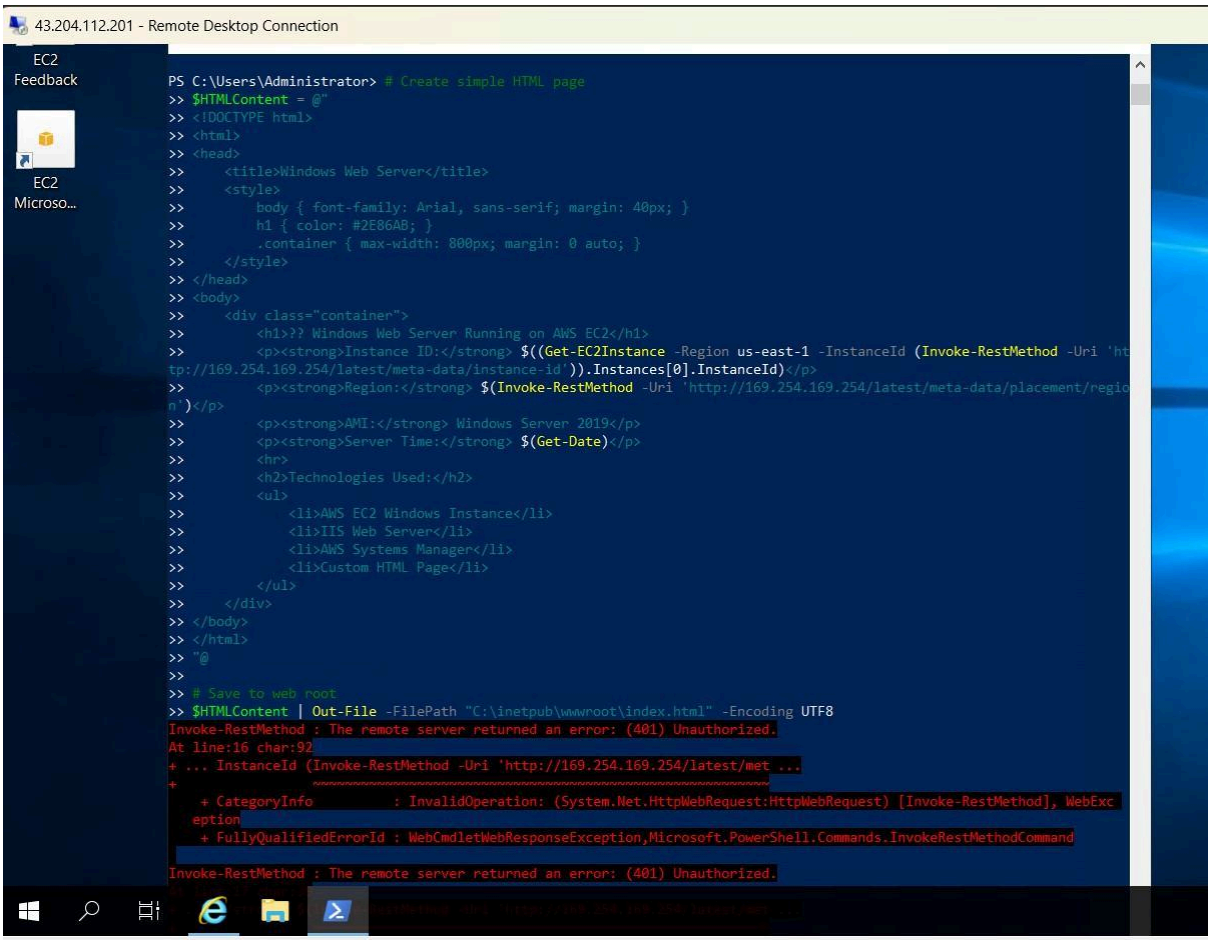

EC2 > Instances > Launch an instance
Network settings Info
Edit
Network Info
vpc-0fe134d0aad4364d9
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic 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-2' with the following rules:
Allow RDP traffic from
Helps you connect to your instance
My IP
122.177.97.122/32
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.
Summary
Number of instances Info
1
Software Image (AMI)
Microsoft Windows Server 2019 ...read more
ami-0d1570d839e619c54
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 30 GiB
Cancel
Launch instance
Preview code
Configure storage Info
Advanced
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

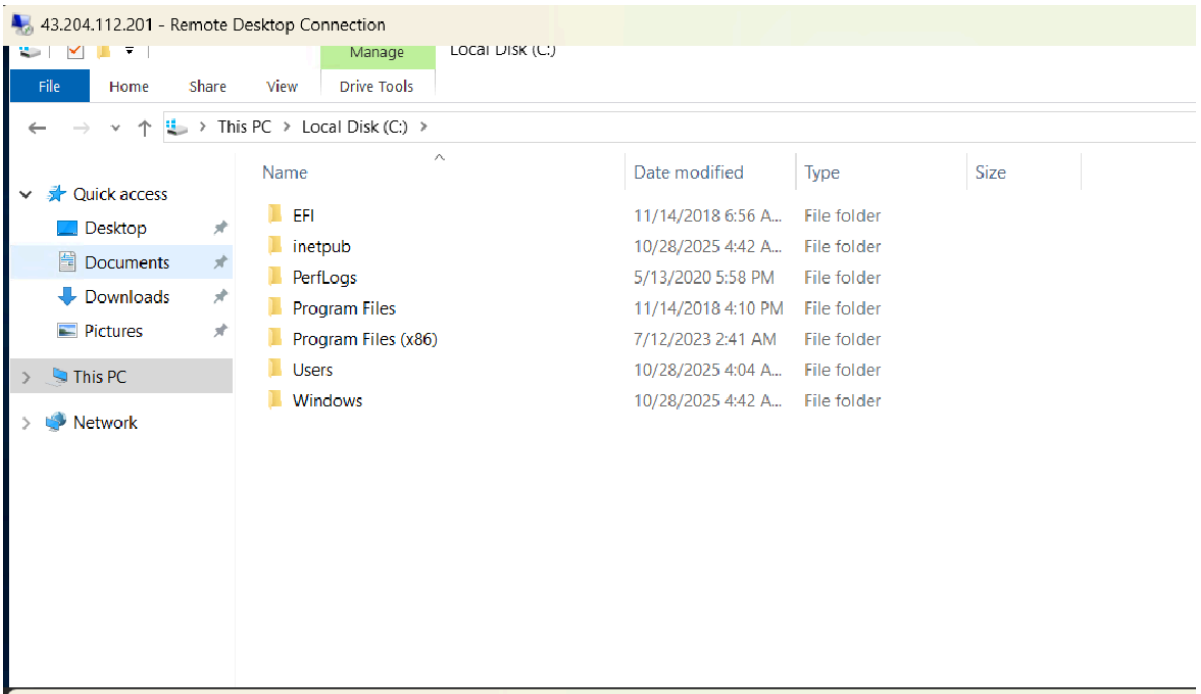

EC2 > Instances
Successfully initiated starting of i-0511f7c772e29d995
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
IPv6 IPs
my web server
i-0511f7c772e29d995
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
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

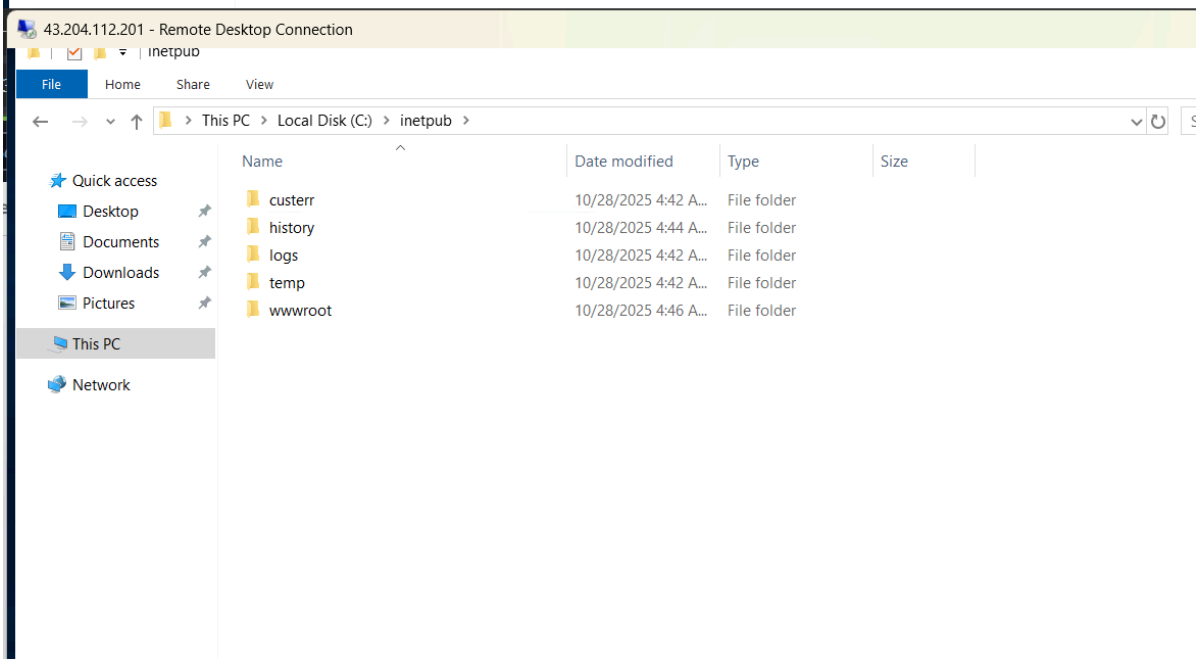

EC2 > Instances > i-0511f7c772e29d995 > Connect to instance
Successfully initiated starting of i-0511f7c772e29d995
Connect Info
Connect to an instance using the browser-based client.
Session Manager
RDP client
EC2 serial console
Record RDP connections
You can now record RDP connections using AWS Systems Manager just-in-time node access. Learn more
Try for free
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:
Download remote desktop file
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.
Cancel
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

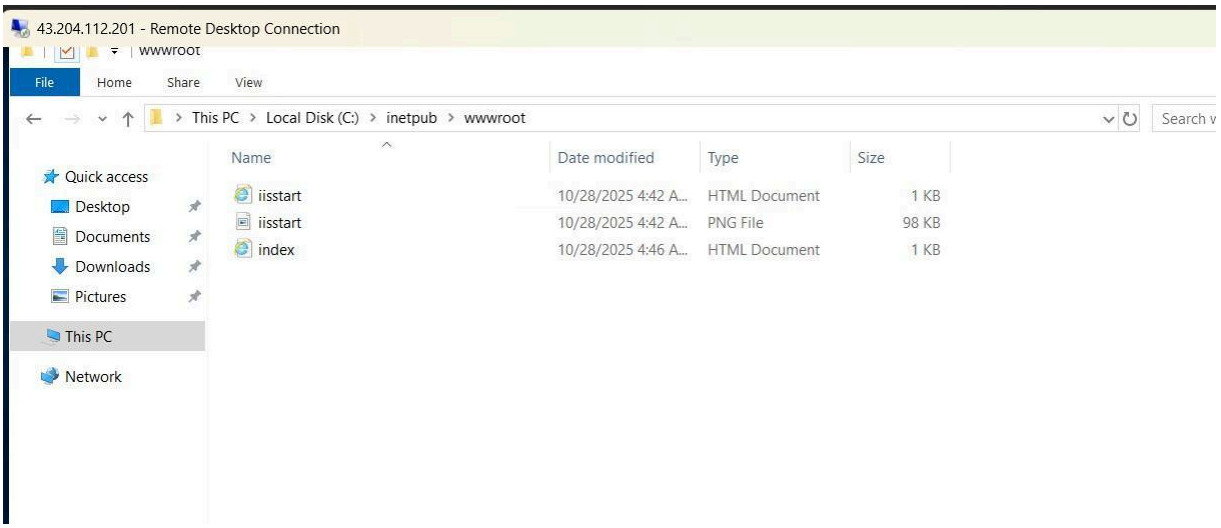

EC2 > Instances > i-0511f7c772e29d995 > Get Windows password
Get Windows password Info
Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.
Instance ID
i-0511f7c772e29d995 (my web server)
Key pair associated with this instance
assign1st
Private key
Either upload your private key file or copy and paste its contents into the field below.
Upload private key file
assign1st.pem
1.678KB
Private key contents - optional
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA345SPYlbRuAQ80j16E1m3aCGTB8fxCVUXX/SRow1PiQEOski
RFoL9nK9j1DIAdZ3Qk49r4p6V4cdipOYhqrHNlxgosoDaipo0VjFeZh7h8CxHvQQ
6J9yK5xx8lXVGUPw+Bv5tYiZ2NNBlhCjhCAmuF1BoULQDCKc3Dpq0auniEv5ukRbh
2Z2OPNQ+DjVdvkalL5rw5cYUPiD7jKZ9kz83KmWWQX5lKiNzbdjV8FvhLIDRF9G7
778+UGoyMeG8blxmoRJ2JdyI59OAPErgieaDCdpZFXE70YwIWiglubh2V3keKNL
nQT9LmLq6wjD+3Q8Gr4KRoN8w431w68VWXI6iQIDAQABAoIBAQCpW7DW8ZF4pWQS
gpDYwHUVroCzgs21+DbxVV2FWM0q1W1jAW12bugrhwr8YU/6nH7mfZQdwvYp9dW7
Cancel
Decrypt password
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

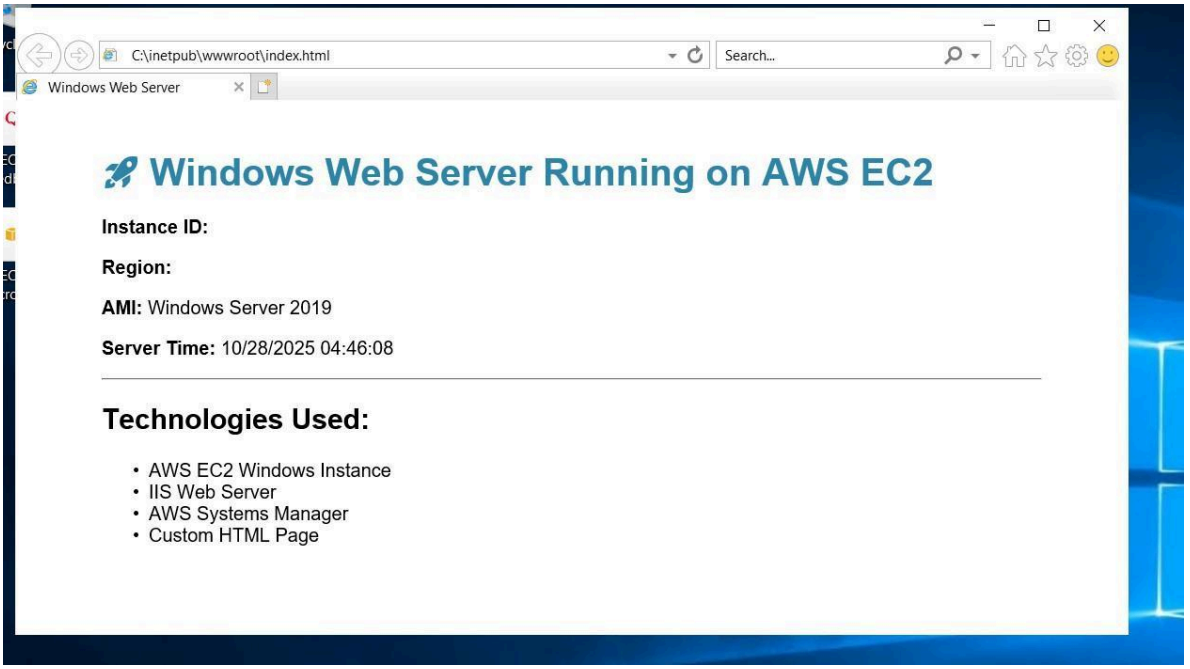

Remote Desktop Connection
Remote Desktop
Connection
Computer:
43.204.112.201
User name:
Administrator
Saved credentials will be used to connect to this computer. You can edit or delete these credentials.
Show Options
Connect
Help
43.204.112.201 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 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>

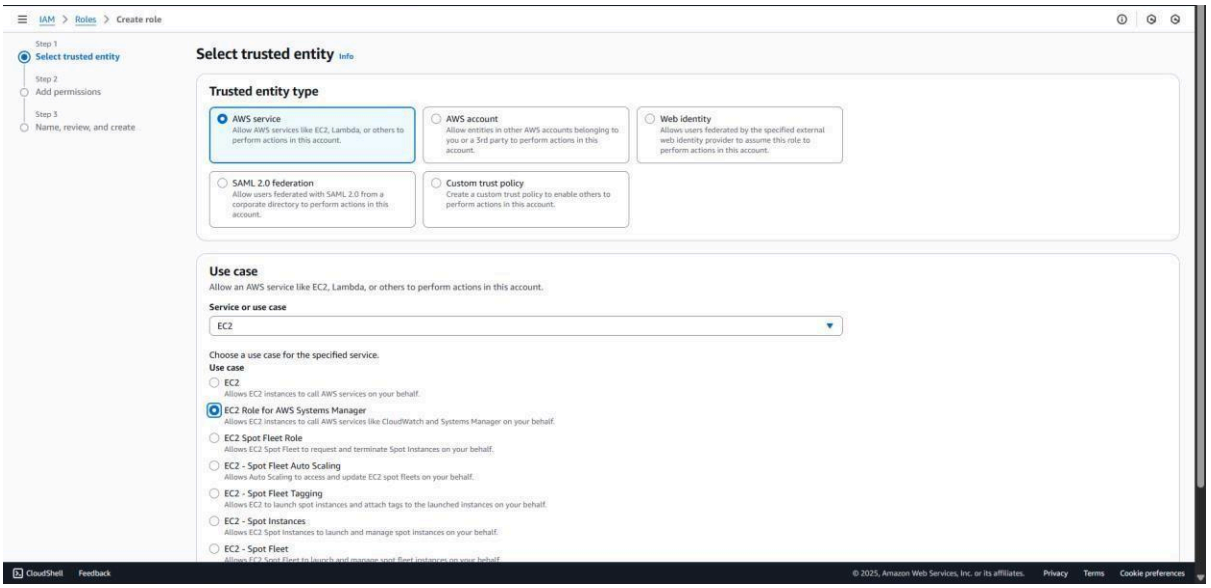

43.204.112.201 - Remote Desktop Connection
EC2 Feedback
EC2 Microso...
PS C:\Users\Administrator> # Create simple HTML page
>> $HTMLContent = @"
>> <!DOCTYPE html>
>> <html>
>> <head>
>> <title>Windows Web Server</title>
>> <style>
>> body { font-family: Arial, sans-serif; margin: 40px; }
>> h1 { color: #2E86AB; }
>> .container { max-width: 800px; margin: 0 auto; }
>> </style>
>> </head>
>> <body>
>>
>> <h1>?? Windows Web Server Running on AWS EC2</h1>
>> Instance ID: $((Get-EC2Instance -Region us-east-1 -InstanceId (Invoke-RestMethod -Uri 'http://169.254.169.254/latest/meta-data/instance-id')).Instances[0].InstanceId)
>> Region: $(Invoke-RestMethod -Uri 'http://169.254.169.254/latest/meta-data/placement/region')
>> AMI: Windows Server 2019
>> Server Time: $(Get-Date)
>> <hr>
>> <h2>Technologies Used:</h2>
>>
>> AWS EC2 Windows Instance
>> IIS Web Server
>> AWS Systems Manager
>> Custom HTML Page
>>
>>
>> </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], WebException
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeRestMethodCommand
Invoke-RestMethod : The remote server returned an error: (401) Unauthorized.

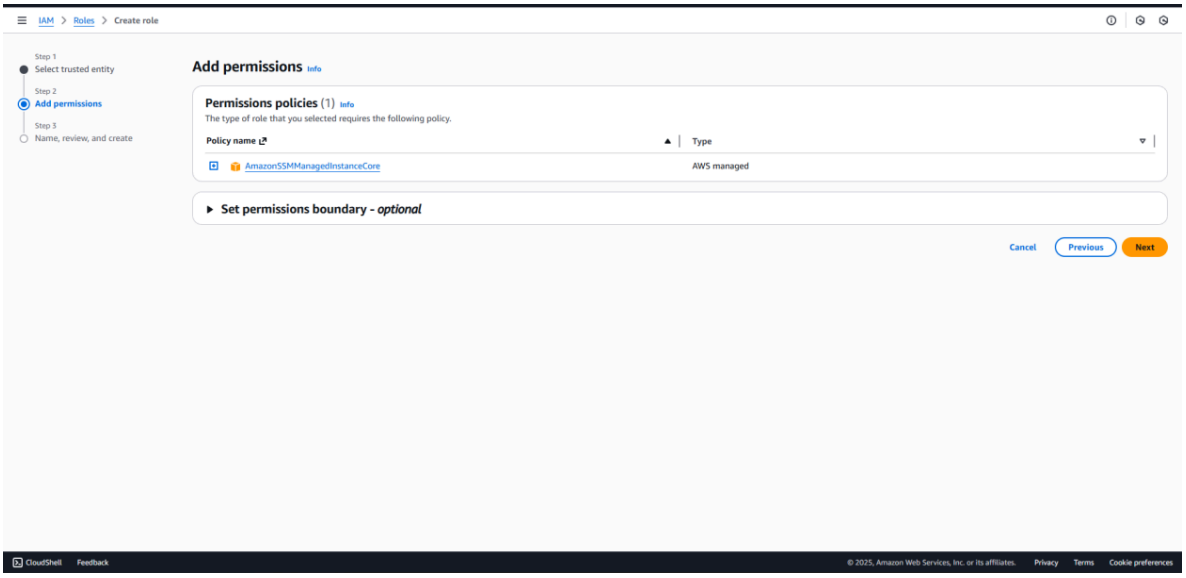

43.204.112.201 - Remote Desktop Connection
Manage
Local Disk (C:)
File
Home
Share
View
Drive Tools
This PC › Local Disk (C:) ›
Quick access
Desktop
Documents
Downloads
Pictures
This PC
Network
Name
Date modified
Type
Size
EFI 11/14/2018 6:56 A... File folder
inetpub 10/28/2025 4:42 A... File folder
PerfLogs 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

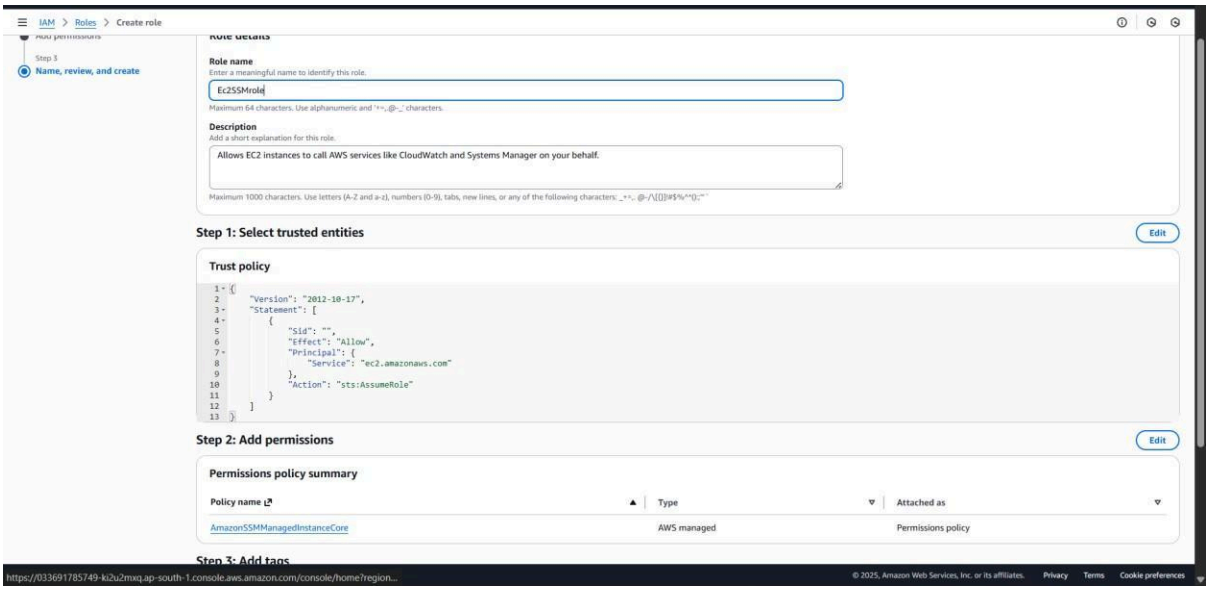

43.204.112.201 - Remote Desktop Connection
inetpub
File
Home
Share
View
This PC › Local Disk (C:) › inetpub ›
Quick access
Desktop
Documents
Downloads
Pictures
This PC
Network
Name
Date modified
Type
Size
custerr 10/28/2025 4:42 A... File folder
history 10/28/2025 4:44 A... File folder
logs 10/28/2025 4:42 A... File folder
temp 10/28/2025 4:42 A... File folder
wwwroot 10/28/2025 4:46 A... File folder

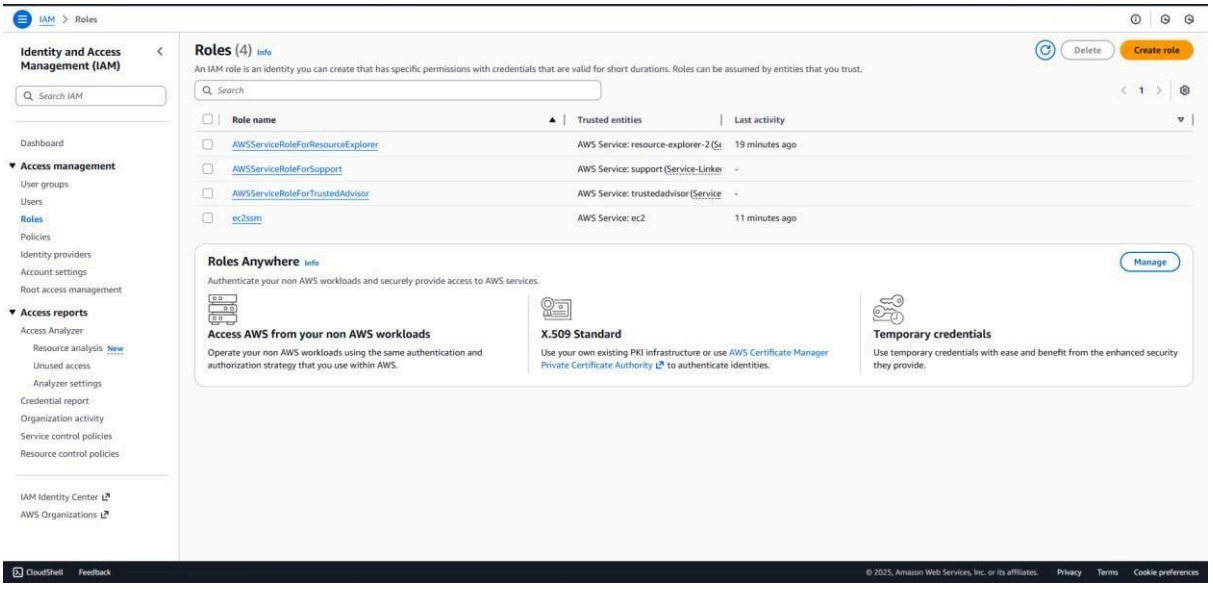

43.204.112.201 - Remote Desktop Connection
wwwroot
File
Home
Share
View
This PC > Local Disk (C:) > inetpub > wwwroot
Search w
Quick access
Desktop
Documents
Downloads
Pictures
This PC
Network
Name
Date modified
Type
Size
iisstart
10/28/2025 4:42 A...
HTML Document
1 KB
iisstart
10/28/2025 4:42 A...
PNG File
98 KB
index
10/28/2025 4:46 A...
HTML Document
1 KB

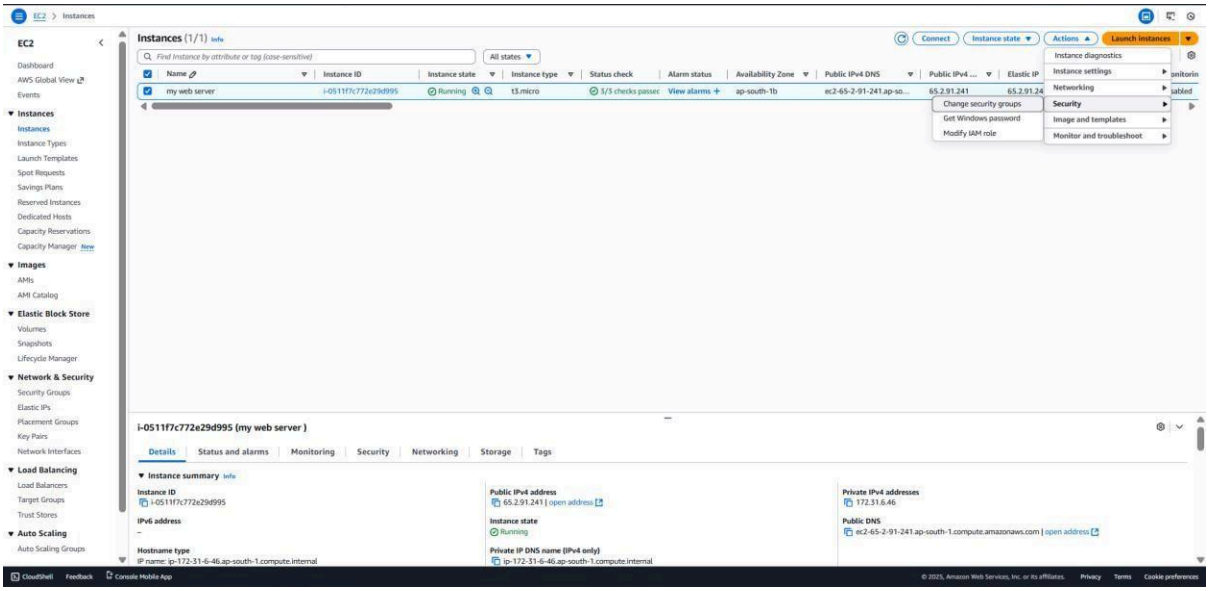

C:\inetpub\wwwroot\index.html
Search...
Windows Web Server
Windows Web Server Running on AWS EC2
Instance ID:
Region:
AMI: Windows Server 2019
Server Time: 10/28/2025 04:46:08
Technologies Used:
AWS EC2 Windows Instance
IIS Web Server
AWS Systems Manager
Custom HTML Page

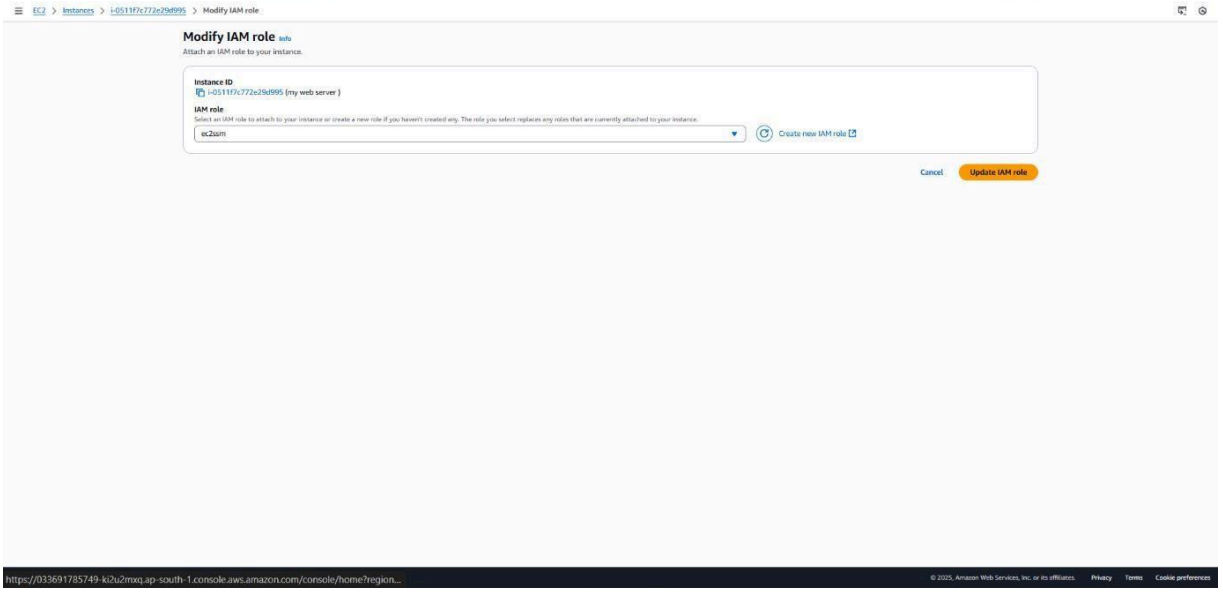

IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts 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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

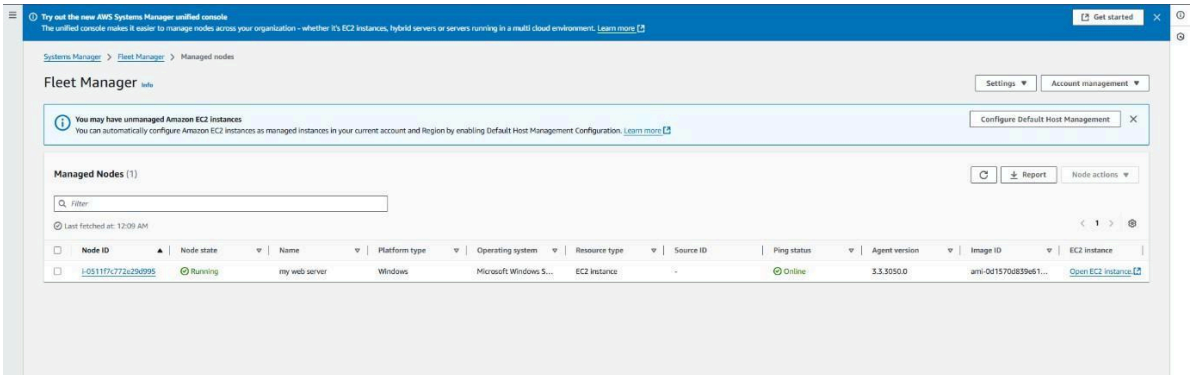

IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1) Info
The type of role that you selected requires the following policy.
Policy name
Type
AmazonSSMManagedInstanceCore
AWS managed
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

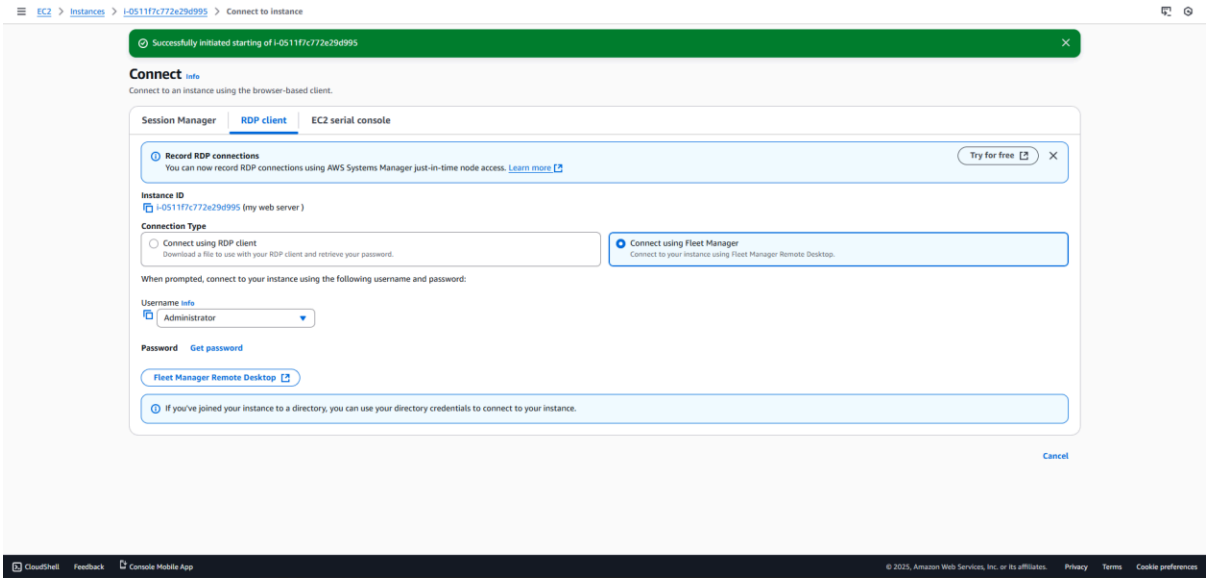

IAM > Roles > Create role
Step 3
Name, review, and create
Role name
Enter a meaningful name to identify this role.
Ec2SSMrole
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services like CloudWatch 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
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "",
"Effect": "Allow",
"Principal": {
"Service": "ec2.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
}
Step 2: Add permissions
Edit
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

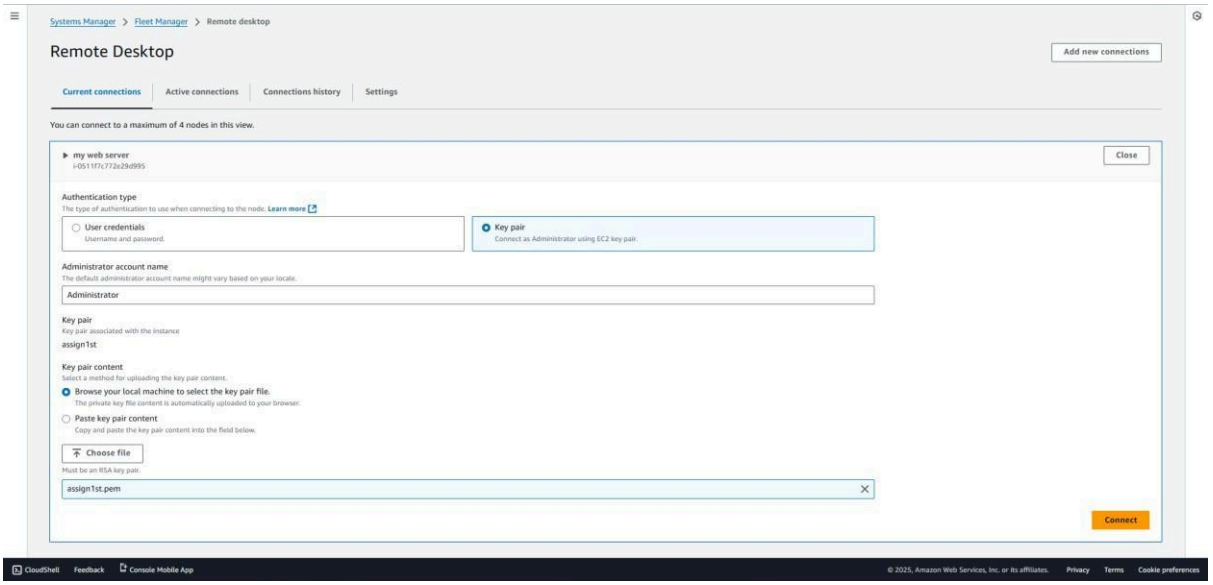

IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
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.
Delete
Create role
Search
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
Manage
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.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

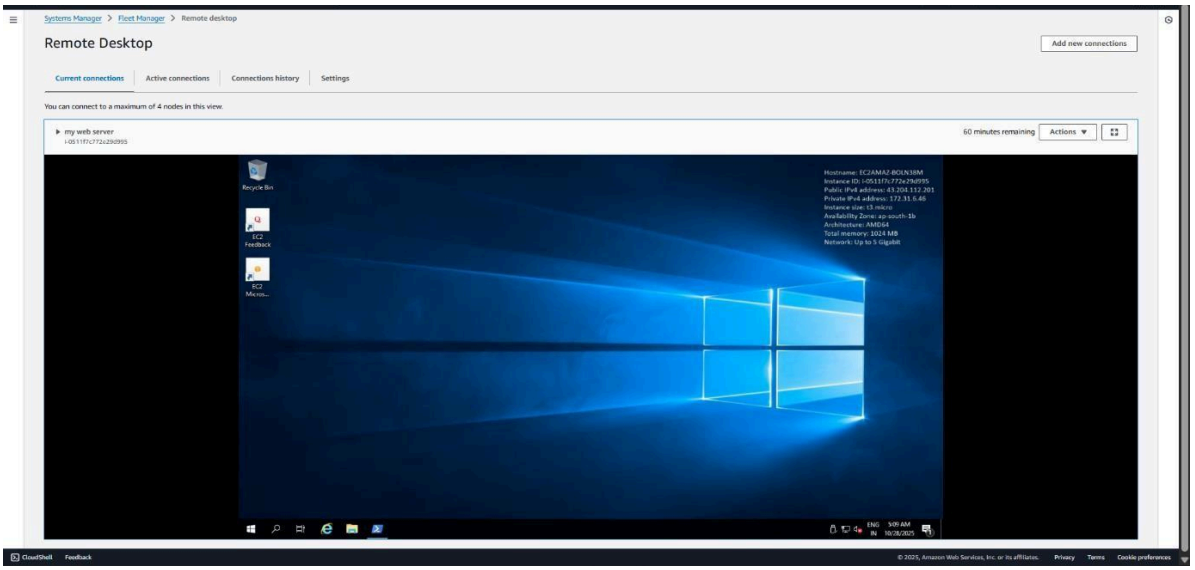

EC2 > Instances
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Instance diagnostics
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Change security groups
Get Windows password
Modify IAM role
my web server
i-0511f7c772e29d995
Running
t3.micro
ap-south-1b
i-0511f7c772e29d995 (my web server)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary
Public IPv4 address
65.2.91.241 | open address
Private IPv4 addresses
172.31.6.46
Public DNS
ec2-65-2-91-241.ap-south-1.compute.amazonaws.com | open address
Hostname type
IP name: ip-172-31-6-46.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-172-31-6-46.ap-south-1.compute.internal


EC2 > Instances > i-0511f7c772e29d995 > Modify IAM role
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
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


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
Get started
Systems Manager > Fleet Manager > Managed nodes
Fleet Manager Info
Settings
Account management
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
Configure Default Host Management
Managed Nodes (1)
Report
Node actions
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


EC2 > Instances > i-0511f7c772e29d995 > Connect to instance
Successfully initiated starting of i-0511f7c772e29d995
Connect Info
Connect to an instance using the browser-based client.
Session Manager
RDP client
EC2 serial console
Record RDP connections
You can now record RDP connections using AWS Systems Manager just-in-time node access. Learn more
Try for free
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
Fleet Manager Remote Desktop
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Systems Manager > Fleet Manager > Remote desktop
Remote Desktop
Add new connections
Current connections
Active connections
Connections history
Settings
You can connect to a maximum of 4 nodes in this view.
my web server
i-0511f7c772e29d995
Close
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.
Choose file
Must be an RSA key pair.
assign1st.pem
Connect
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Systems Manager > Fleet Manager > Remote desktop
Remote Desktop
Add new connections
Current connections
Active connections
Connections history
Settings
You can connect to a maximum of 4 nodes in this view.
my web server
60 minutes remaining
Actions
Recycle Bin
EC2 Feedback
Hostname: EC2AMAZ-BOLN38M
Instance ID: i-0511f7c772e29d995
Public IPv4 address: 43.204.152.201
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
ENG
IN
5:05 AM
10/28/2025
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences