

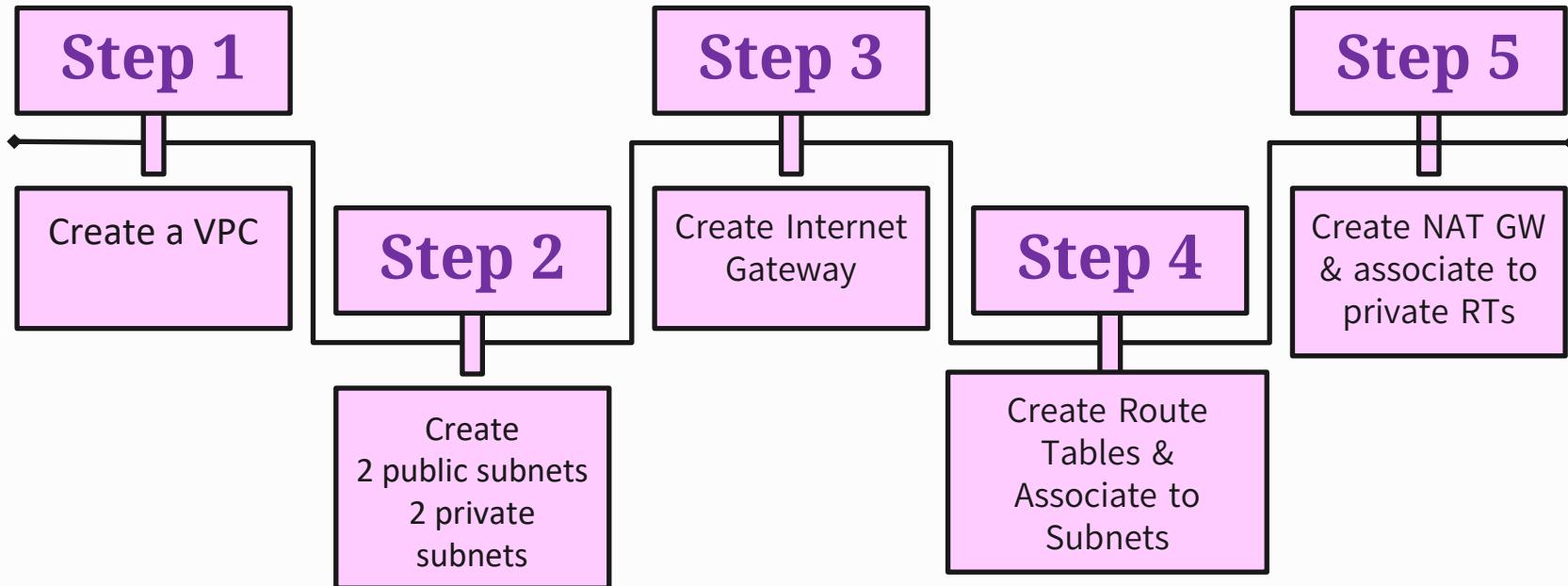
Highly Available Web Server

By: Salma Salah

Task Statement

Automate the creation of a highly available website that will load balance traffic across multiple web servers this website can scale from two to four load balanced instances based upon demand. Need to Install a web server by using AWS System Manager Run Command

First Part



Step 1

Create a VPC & Give Name (SSM-GBG) and choose IPV4 CIDR

The screenshot shows the AWS VPC dashboard. On the left, a sidebar lists various VPC components: Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. The main area displays 'Resources by Region' for the US East 1 region, showing counts for VPCs (1), Subnets (6), Route Tables (1), Internet Gateways (1), and Egress-only Internet Gateways (0). It also includes sections for NAT Gateways (0), VPC Peering Connections (0), Network ACLs (1), Security Groups (1), and Customer Gateways (0). A 'Service Health' section indicates no issues. A 'Settings' section allows configuration of Zones and Console Experiments. An 'Additional Information' section provides links to VPC Documentation, All VPC Resources, Forums, and Report an Issue. The 'AWS Network Manager' section describes its features for managing and monitoring network connectivity.

The screenshot shows the 'Create VPC' wizard in progress. The first step, 'VPC settings', is displayed. It asks 'Resources to create' with two options: 'VPC only' (selected) and 'VPC and more'. A 'Name tag - optional' field contains 'SSM-GBG'. Under 'IPv4 CIDR block', it says 'IPv4 CIDR manual input' (selected) and shows the value '10.0.0.0/16'. A note states 'CIDR block size must be between /16 and /28'. The 'IPv6 CIDR block' section is collapsed. The top navigation bar shows the user is in the 'Your VPCs' section under 'VPC'.

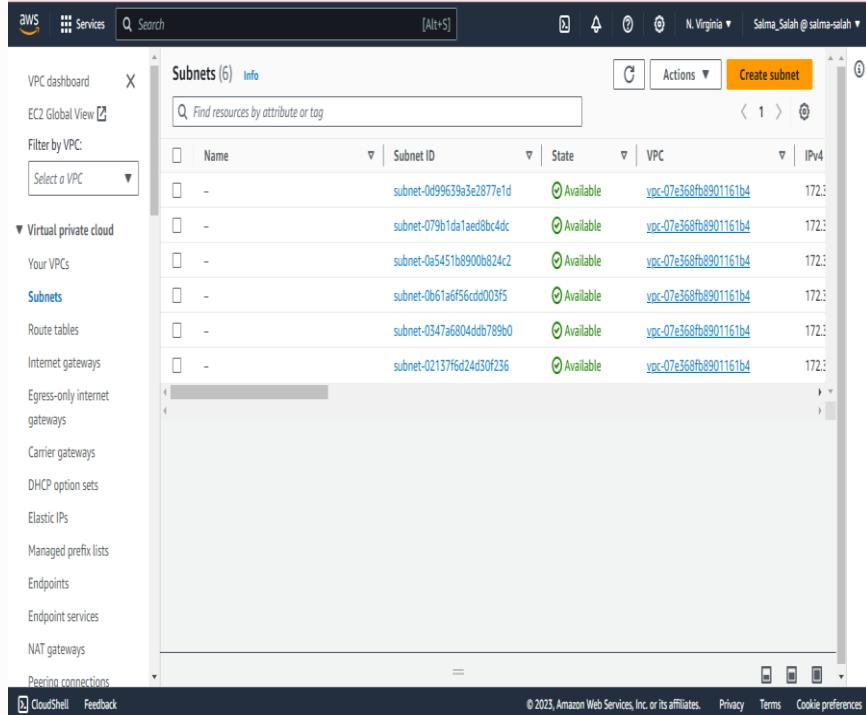
Step 1

Adding a tag for VPC

The screenshot shows the AWS VPC CIDR configuration page. At the top, there is a search bar and a navigation bar with the user 'Salma_Salah @ salma-salah'. Below the search bar, a CIDR block '10.0.0.0/16' is entered, with a note stating 'CIDR block size must be between /16 and /28.' Under 'IPv6 CIDR block', the option 'No IPv6 CIDR block' is selected. In the 'Tenancy' section, 'Default' is chosen. The 'Tags' section is expanded, showing two tags: 'Name' with value 'SSM-GBG' and 'CIDR' with value '10.0.0.0/16'. A tooltip 'Use 10.0.0.0/16' is visible next to the CIDR tag. An 'Add tag' button is present. At the bottom, it says 'You can add 48 more tags'. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

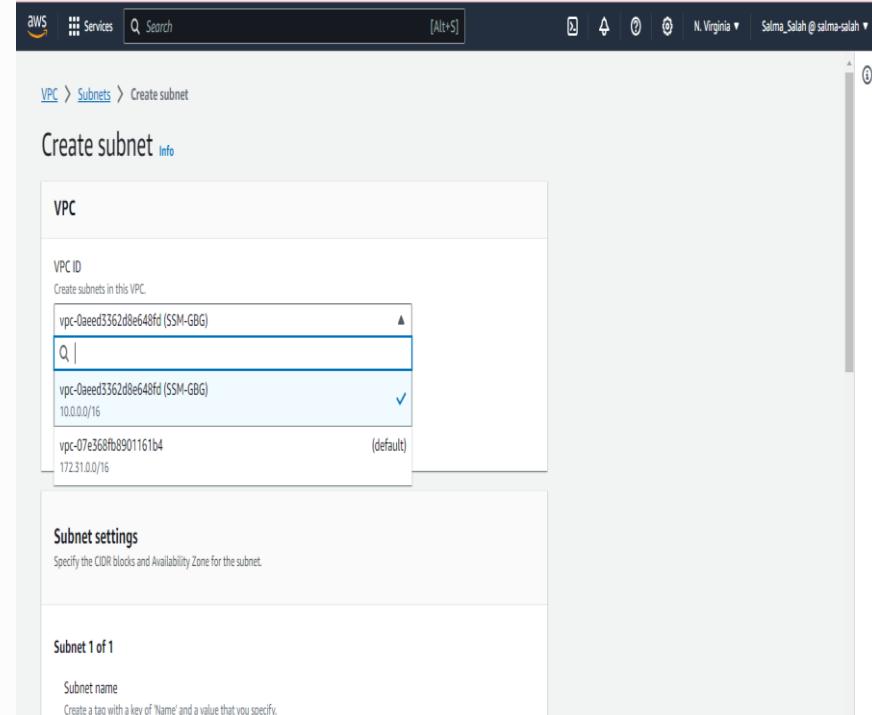
Step 2

Create 4 subnets



The screenshot shows the AWS VPC dashboard with the Subnets section selected. A table lists six available subnets:

Name	Subnet ID	State	VPC	IPv4
-	subnet-0d99639a3e2877e1d	Available	vpc-07e368fb8901161b4	172.31.0.0/16
-	subnet-079b1da1aed8bc4dc	Available	vpc-07e368fb8901161b4	172.31.1.0/16
-	subnet-0a5451b8900b824c2	Available	vpc-07e368fb8901161b4	172.31.2.0/16
-	subnet-0b61a6f56ccdd03f5	Available	vpc-07e368fb8901161b4	172.31.3.0/16
-	subnet-0347a6804ddb789b0	Available	vpc-07e368fb8901161b4	10.0.0.0/16



The screenshot shows the 'Create subnet' wizard in the AWS VPC console. The 'VPC' step is selected, showing the dropdown menu for choosing a VPC. The 'vpc-07e368fb8901161b4' VPC is highlighted.

VPC

VPC ID
Create subnets in this VPC.

vpc-0aeed3362d8e648fd (SSM-GBG)
vpc-0aeed3362d8e648fd (SSM-GBG)
10.0.0.0/16
vpc-07e368fb8901161b4 (default)
172.31.0.0/16

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.

In Each Subnet specify

- Name
- Availability Zone
- Subnet CIDR

Subnet 1 of 1

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

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.

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

IPv4 subnet CIDR block
 256 IPs
< > ^ v

▼ Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="Public-SSM-1"/>
<input type="text" value="CIDR"/>	<input type="text" value="10.0.10.0/24"/>

[CloudShell](#) [Feedback](#)

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

No preference

Subnet CIDR block
US East (N. Virginia) / us-east-1a us-east-1
ID: us-east-1a Network border group: us-east-1

US East (N. Virginia) / us-east-1b us-east-1
ID: us-east-1b Network border group: us-east-1

US East (N. Virginia) / us-east-1c us-east-1
ID: us-east-1c Network border group: us-east-1

US East (N. Virginia) / us-east-1d us-east-1
ID: us-east-1d Network border group: us-east-1

US East (N. Virginia) / us-east-1a

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

IPv4 subnet CIDR block
 256 IPs
< > ^ v

▼ Tags - optional

Key	Value - optional
-----	------------------

[CloudShell](#) [Feedback](#)

Repeat for Subnet 2 & 3

AWS Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah

Subnet 2 of 2

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

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

IPv4 subnet CIDR block
 256 IPs
< > ^ v

Tags - optional

Key	Value - optional
<input type="text" value="Name"/> X	<input type="text" value="Public-SSM-2"/> X
<input type="text" value="CIDR"/> X	<input type="text" value="10.0.20.0/24"/> X

Add another

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah

Subnet 3 of 3

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

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

IPv4 subnet CIDR block
 256 IPs
< > ^ v

Tags - optional

Key	Value - optional
<input type="text" value="Name"/> X	<input type="text" value="Private-SSM-1"/> X
<input type="text" value="CIDR"/> X	<input type="text" value="10.0.30.0/24"/> X

Add another

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Repeat for Subnet 4
- Check the 4 subnets

Subnet 4 of 4

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

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.

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

IPv4 subnet CIDR block
 256 IPs
< > ^ v

Tags - optional

Key	Value - optional
<input type="text" value="Name"/> X	<input type="text" value="Private-SSM-2"/> X
<input type="text" value="CIDR"/> X	<input type="text" value="10.40.0/24"/> X

[CloudShell](#) [Feedback](#)

You have successfully created 4 subnets: subnet-0c6e65fc987ba66eb, subnet-01ef1899670700a4d, subnet-0c4ebcca44b86cd45, subnet-0cbd7e815628f5f8

Subnets (4) [Info](#)

Subnet ID : [subnet-0c6e65fc987ba66eb](#) | [subnet-01ef1899670700a4d](#) | [subnet-0c4ebcca44b86cd45](#)

[Actions](#) [Create subnet](#)

Virtual private cloud

Your VPCs

Subnets

Show more (+1) Clear filters

Name	Subnet ID	State	IPv4 CIDR
Private-SSM-1	subnet-0c4ebcca44b86cd45	Available	vpc-0aeed3362d8e648fd SSM...
Public-SSM-2	subnet-01ef1899670700a4d	Available	vpc-0aeed3362d8e648fd SSM...
Public-SSM-1	subnet-0c6e65fc987ba66eb	Available	vpc-0aeed3362d8e640fd SSM...
Private-SSM-2	subnet-0cbd7e815628f5f8	Available	vpc-0aeed3362d8e648fd SSM...

[CloudShell](#) [Feedback](#)

Enable Auto Assign IPV4 IN

- Public Subnet 1

The screenshot shows the AWS VPC Subnets page. On the left, there's a sidebar with 'Virtual private cloud' navigation. Under 'Subnets', several subnets are listed:

Name	Subnet ID	State
Private-SSM-1	subnet-0c4ebcca44b86cd45	Available
Public-SSM-2	subnet-01ef1899670700a4d	Available
Public-SSM-1	subnet-0c6e65fc987ba66eb	Available
Private-SSM-2	subnet-0cdbd7e815628f5f8	Available

An 'Actions' menu is open over the 'Public-SSM-1' subnet, showing options like 'Edit subnet settings' (which is highlighted), 'Edit IPv6 CIDs', 'Edit network ACL association', 'Edit route table association', 'Edit CIDR reservations', 'Share subnet', 'Manage tags', and 'Delete subnet'. The 'Edit subnet settings' option is highlighted with a blue box.

The screenshot shows the 'Edit subnet settings' page for the 'Public-SSM-1' subnet. It has sections for 'Subnet' and 'Auto-assign IP settings'.

Subnet

Subnet ID	Name
subnet-0c6e65fc987ba66eb	Public-SSM-1

Auto-assign IP settings

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

Enable auto-assign public IPv4 address Info

Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info

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

Enable resource name DNS A record on launch Info

Enable Auto Assign IPV4 IN

- Public Subnet 2

The screenshot shows the AWS VPC dashboard with a green success message: "You have successfully changed subnet settings: Enable auto-assign public IPv4 address". The main table lists four subnets:

Name	Subnet ID	State	VPC
Private-SSM-1	subnet-0c4ebcca44b86cd45	Available	VPC
<input checked="" type="checkbox"/> Public-SSM-2	subnet-01ef1899670700a4d	Available	VPC
Public-SSM-1	subnet-0c6e65fc987ba66eb	Available	VPC
Private-SSM-2	subnet-0cbd07e815628f5f8	Available	VPC

A context menu is open over the "Public-SSM-2" row, with "Edit subnet settings" highlighted.

The screenshot shows the "Edit subnet settings" page for the subnet with ID "subnet-01ef1899670700a4d".

Subnet

Subnet ID	Name
subnet-01ef1899670700a4d	Public-SSM-2

Auto-assign IP settings

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

Enable auto-assign public IPv4 address Info

Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings

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

Enable resource name DNS A record on launch Info

Step 3

- Create Internet GateWay
- Attach IGW to VPC

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with options like 'Virtual private cloud', 'Your VPCs', 'Subnets', 'Route tables', 'Internet gateways' (which is selected), 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', 'Elastic IPs', 'Managed prefix lists', 'Endpoints', 'Endpoint services', 'NAT gateways', and 'Peering connections'. The main area is titled 'Internet gateways (1)' and shows a table with one row. The columns are 'Name', 'Internet gateway ID', 'State', and 'VPC ID'. The single entry is 'igw-0c347142903731a40' with state 'Attached' and VPC ID 'vpc-07e368fb8901161b4'. Below the table, it says 'Select an internet gateway above'.

This screenshot shows the 'Create internet gateway' wizard. The first step, 'Internet gateway settings', is displayed. It has a 'Name tag' section where 'SSM-IGW' is entered into a text input field. Below it is a 'Tags - optional' section where a single tag 'Name: SSM-IGW' is listed. At the bottom right of this step, there are 'Cancel' and 'Create internet gateway' buttons.

Step 3

- Create Internet GateWay
- Attach IGW to VPC

The screenshot shows the AWS VPC dashboard. A green success message at the top states: "The following internet gateway was created: igw-00343bfdd143dcfa1 - SSM-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet." Below this, there is a breadcrumb navigation: VPC > Internet gateways > igw-00343bfdd143dcfa1. The main view displays the details of the newly created Internet Gateway, including its ID (igw-00343bfdd143dcfa1), state (Detached), and owner (821594720492). An "Actions" dropdown menu is open, with "Attach to VPC" highlighted. The "Tags" section shows a single tag named "SSM-IGW". At the bottom, there are links for CloudShell and Feedback.

The screenshot shows the "Attach to VPC" dialog box. It has a header "Attach to VPC (igw-00343bfdd143dcfa1)" with an "Info" link. The main area is titled "VPC" and contains the instruction: "Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below." Below this is a "Available VPCs" section with a search bar labeled "Select a VPC". A dropdown menu shows the option "vpc-0aeed3362d8e649fd - SSM-GBG". At the bottom right of the dialog is an orange "Attach internet gateway" button.

Step 4

- Create Internet GateWay
- Attach IGW to VPC

The screenshot shows the AWS VPC Route Tables page. The left sidebar is titled "Route tables" and lists various VPC components: VPC dashboard, EC2 Global View, Filter by VPC (with a dropdown menu), Virtual private cloud, Your VPCs, Subnets, Route tables (selected), Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. The main content area is titled "Route tables (2) Info" and contains a table with two rows:

Name	Route table ID	Explicit subnet associations	Edge associations	Main
-	rtb-0d0d13f6fd48cd13	-	-	Yes
-	rtb-043f9de6daad585c1	-	-	Yes

At the bottom of the page, there is a "Select a route table" dropdown menu.

The screenshot shows the "Create route table" dialog box. The top section is titled "Route table settings" and includes fields for "Name - optional" (set to "PUBLIC-RT-1") and "VPC" (set to "vpc-0aeed3362d8e648fd (SSM-GBG)"). Below this is a "Tags" section with a table for adding tags. A single tag is present: "Key" is "Name" and "Value - optional" is "PUBLIC-RT-1". There is also a note: "You can add 49 more tags." At the bottom right of the dialog is a "Create route table" button.

Public Route Table

- Edit Routes
- Attach Internet GateWay

The screenshot shows the AWS VPC dashboard. A green success message at the top states: "Route table rtb-03771448932b378ab | PUBLIC-RT-1 was created successfully." Below this, the "Route tables" section is selected. It displays a table with one row for the newly created route table. The table columns include: Route table ID (rtb-03771448932b378ab), Main (No), Explicit subnet associations (empty), Edge associations (empty), VPC (vpc-0aeed3362d8e648fd | SSM-GBG), and Owner ID (821594020462). At the bottom, there are tabs for "Routes" (selected), "Subnet associations", "Edge associations", "Route propagation", and "Tags".

The screenshot shows the "Edit routes" page for the route table rtb-03771448932b378ab. The table lists two routes:

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

Below the table, there is a "Remove" button for the second route. At the bottom right, there are "Cancel", "Preview", and "Save changes" buttons.

Public Route Table

- Edit Subnet Associations
- Associate to Public Subnets

The screenshot shows the AWS VPC dashboard with the 'Route tables' section selected. A specific route table, 'rtb-03771448932b378ab / PUBLIC-RT-1', is highlighted. On the right side, a context menu is open with the following options: Set main route table, **Edit subnet associations**, Edit edge associations, Edit route propagation, Edit routes, Manage tags, and Delete. Below the menu, the 'Available subnets' section lists four subnets: Private-SSM-1, Public-SSM-2, Public-SSM-1 (selected), and Private-SSM-2. At the bottom, there are tabs for 'Routes' (selected), Subnet associations, Edge associations, Route propagation, and Tags.

The screenshot shows the 'Edit subnet associations' dialog box. It displays the 'Available subnets (1/4)' section with a table of subnets and their details. The 'Selected subnets' section contains one entry: 'subnet-0c6e65fc987ba66eb / Public-SSM-1'. At the bottom right, there are 'Cancel' and 'Save associations' buttons.

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
Private-SSM-1	subnet-0c4ebccc44b86cd45	10.0.30.0/24	-	Main (rtb-0d0d13f6fd48cd13)
Public-SSM-2	subnet-01ef899670700ad4	10.0.20.0/24	-	Main (rtb-0d0d13f6fd48cd13)
<input checked="" type="checkbox"/> Public-SSM-1	subnet-0c6e65fc987ba66eb	10.0.10.0/24	-	Main (rtb-0d0d13f6fd48cd13)
<input type="checkbox"/> Private-SSM-2	subnet-0cb7de815628f5f8	10.0.40.0/24	-	Main (rtb-0d0d13f6fd48cd13)

Step 5

- Create First NAT GateWay
- Attach First NAT GW to first private subnet

The screenshot shows the AWS VPC service interface. On the left, a navigation pane lists various VPC components: Virtual private cloud, Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways (which is selected), and Peering connections. The main content area is titled "NAT gateways" and contains a table with columns: Name, NAT gateway ID, Connectivity type, State, State message, and Primary public IP. A search bar at the top of the table says "Filter NAT gateways". Below the table, a section titled "Select a NAT gateway" is visible.

The screenshot shows the "Create NAT gateway" wizard. The first step, "NAT gateway settings", is displayed. It includes fields for "Name - optional" (containing "SSM-VGW"), "Subnet" (set to "subnet-0c6e65fc987ba66eb (Public-SSM-1)"), and "Connectivity type" (with "Public" selected). Below these, an "Elastic IP allocation ID" field contains "eipalloc-08010ef23e0dd9105" and an "Allocate Elastic IP" button. At the bottom of the page, there are "Next Step" and "Cancel" buttons.

Step 5

- Create Second NAT GateWay
- Attach Second NAT GW to Second private subnet

The screenshot shows the AWS Management Console interface for creating a NAT gateway. The top navigation bar includes the AWS logo, 'Services' dropdown, a search bar, and account information ('N. Virginia' and 'Salma_Salah @ salma-salah'). The main content area is titled 'Create NAT gateway' with an 'Info' link. A descriptive text explains that it's a highly available, managed Network Address Translation (NAT) service. The 'NAT gateway settings' section contains the following fields:

- Name - optional:** A text input field containing 'SSM-NGW-2'. Below it is a note: 'The name can be up to 256 characters long.'
- Subnet:** A dropdown menu showing 'subnet-01ef1899670700a4d (Public-SSM-2)'.
- Connectivity type:** A radio button group where 'Public' is selected, and 'Private' is unselected.
- Elastic IP allocation ID:** A dropdown menu showing 'eipalloc-0388fcc07c427bab'.
- Allocate Elastic IP:** A button to the right of the dropdown menu.

At the bottom of the page are links for 'CloudShell', 'Feedback', and copyright information: '© 2023, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

Public Route Table

- Edit Subnet Associations
- Associate to Public Subnets

AWS Services Search [All v5] N. Virginia Sime_Sahai @ sime-sahai

Route tables 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.
Private-RT-1

VPC
The VPC to use for this route table.
vpc-0eefc556208e549f (SM-GG)

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
Q, Name	X Q, Private-RT-1 X Remove

Add new tag
You can add 49 more tags.

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [All v5] N. Virginia Sime_Sahai @ sime-sahai

Route tables rt-0123456789ab Edit routes

Edit routes

Destination	Status	Propagated
10.0.0.0/16	local	No
NAT Gateway	Active	No
Q, 0.0.0.0 X	-	Remove

Add route Cancel Preview Save changes

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [All v5] N. Virginia Sime_Sahai @ sime-sahai

Route tables rt-0123456789ab Edit subnet associations

Edit subnet associations
Change which subnets are associated with this route table.

Available subnets (1/4)

Name	Subnet ID	IPv4 CDR	IPv6 CDR	Route table ID
Private-SSM-1	subnet-04bca46b56d45	10.0.30.0/24	-	Main (rt-00f135ff48c7f5)
Public-SSM-2	subnet-21d109677070d46	10.0.20.0/24	-	rt-036116c022913451e4 (Public)
Public-SSM-1	subnet-05e5539356e5b	10.0.10.0/24	-	rt-03714493736736b (Public)
Private-SSM-2	subnet-0cb7a7e1152185b9	10.0.40.0/24	-	Main (rt-00f135ff48c7f5)

Selected subnets

subnet-04bca46b56d45 / Private-SSM-1 X
--

Cancel Save associations

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Public Route Table

- Edit Subnet Associations
- Associate to Public Subnets

The screenshot shows the 'Create route table' page in the AWS VPC service. It includes fields for 'Name - optional' (Private-RT-2), 'VPC' (selected VPC ID), and 'Tags' (Key: Name, Value: Private-RT-2). The page also features a 'Route table settings' section with a note about creating tags and a 'Tags' section for adding more.

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.
Private-RT-2

VPC
The VPC to use for this route table.
vpc-0aeed3362d8e648fd (SSM-GBG)

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
Q Name X Q Private-RT-2 X Remove
Add new tag
You can add 49 more tags.

The screenshot shows the 'Edit routes' page for a specific route table. It lists three routes: one to 'local' via a NAT Gateway, and two to 'nat-' via specific NAT gateway IDs. The page includes a 'Tags' section and buttons for 'Preview' and 'Save changes'.

VPC > Route tables > rtb-03f66b917bc3abd44 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q 0.0.0.0/0	NAT Gateway	-	No
Q nat-	nat-0277ba3c1064e63 (SSM-NGW-1) nat-05611759e65ca6e0c (SSM-NGW-2)		

Add route

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

Revies Route Tables

The screenshot shows the AWS VPC Route Tables page. The left sidebar is collapsed, and the main content area displays a table of route tables.

Route tables (6) Info

Name	Rout...	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-0d0...	-	-	Yes	vpc
-	rtb-043...	-	-	Yes	vpc
PUBLIC-RT-1	rtb-037...	subnet-0c6e65fc987ba66eb / Public-SSM-1	-	No	vpc
PUBLIC-RT-2	rtb-066...	subnet-01ef1899670700a4d / Public-SSM-2	-	No	vpc
Private-RT-1	rtb-01d...	subnet-0c4ebcca44b86cd45 / Private-SSM-1	-	No	vpc
Private-RT-2	rtb-03f...	subnet-0cdbd7e815628f5f8 / Private-SSM-2	-	No	vpc

Select a route table

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Check VPC

AWS Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah

VPC dashboard EC2 Global View Filter by VPC: Select a VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways Carrier gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections

Your VPCs (1/2) Info Actions Create VPC

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
SSM-GBG	vpc-0aeed3362d8e648fd	Available	10.0.0.0/16	-

Resource map Info

VPC Show details Subnets (4) Route tables (5)

Subnets within this VPC: us-east-1a (Public-SSM-1, Private-SSM-1), us-east-1b (Public-SSM-2, Private-SSM-2). Route tables: PUBLIC-RT-1 (rtb-0d0d13f6fd48cd13), Private-RT-1, Private-RT-2, PUBLIC-RT-2.

```
graph LR; VPC[SSM-GBG] --- Subnets[Subnets (4)]; VPC --- RT[Route tables (5)]; Subnets --- usEast1a[us-east-1a]; Subnets --- usEast1b[us-east-1b]; RT --- PUBLICRT1[PUBLIC-RT-1]; RT --- RT1[Private-RT-1]; RT --- RT2[Private-RT-2]; RT --- PUBLICRT2[PUBLIC-RT-2];
```

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences CloudShell Feedback

AWS Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah

VPC dashboard EC2 Global View Filter by VPC: Select a VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways Carrier gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections

Your VPCs (1/2) Info Actions Create VPC

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
SSM-GBG	vpc-0aeed3362d8e648fd	Available	10.0.0.0/16	-

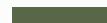
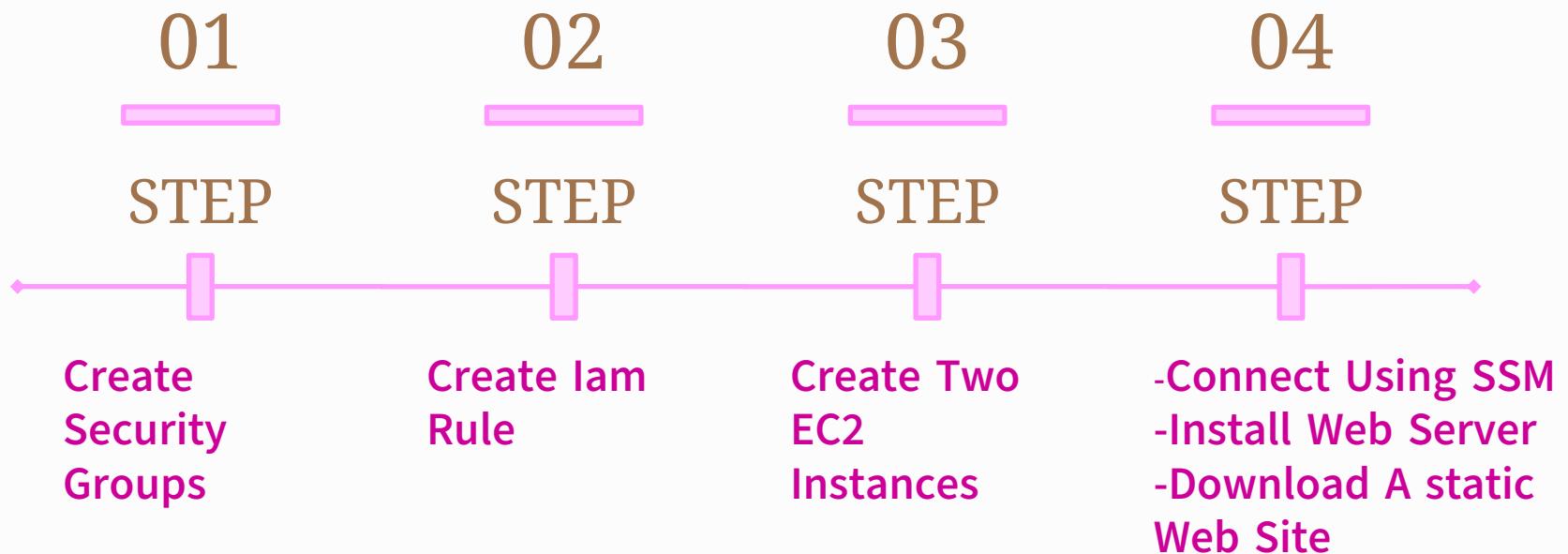
Subnets (4) Route tables (5) Network connections (3)

Subnets within this VPC: us-east-1a (Public-SSM-1, Private-SSM-1), us-east-1b (Public-SSM-2, Private-SSM-2). Route tables: PUBLIC-RT-1 (rtb-0d0d13f6fd48cd13), Private-RT-1, Private-RT-2, PUBLIC-RT-2. Network connections: SSM-IGW, SSM-NGW-1, SSM-NGW-2.

```
graph LR; VPC[SSM-GBG] --- Subnets[Subnets (4)]; VPC --- RT[Route tables (5)]; VPC --- NC[Network connections (3)]; Subnets --- usEast1a[us-east-1a]; Subnets --- usEast1b[us-east-1b]; RT --- PUBLICRT1[PUBLIC-RT-1]; RT --- RT1[Private-RT-1]; RT --- RT2[Private-RT-2]; RT --- PUBLICRT2[PUBLIC-RT-2]; NC --- SSMIGW[SSM-IGW]; NC --- SSMNGW1[SSM-NGW-1]; NC --- SSMNGW2[SSM-NGW-2];
```

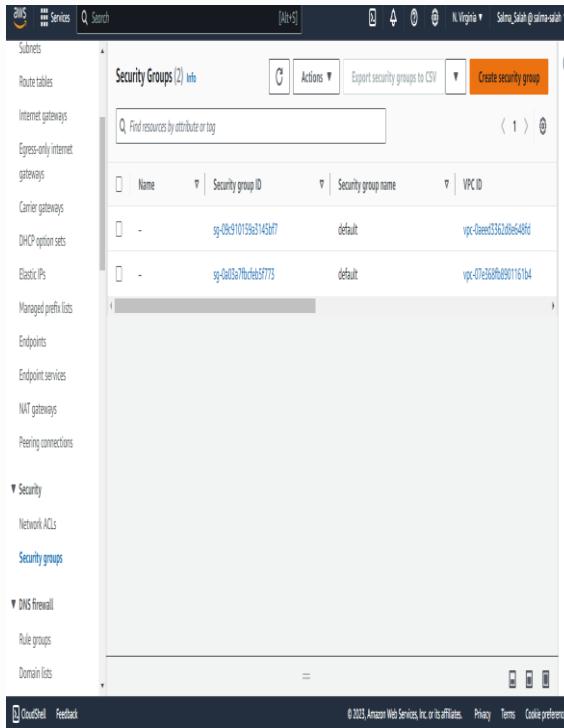
© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences CloudShell Feedback

Second Part

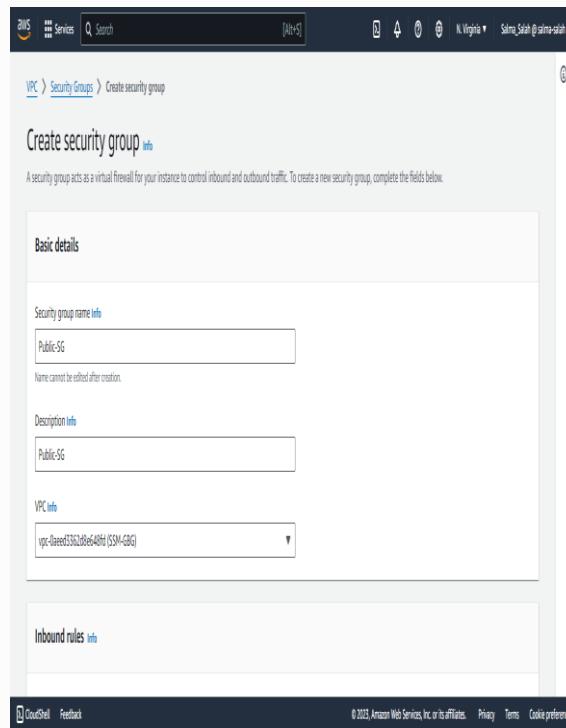


Step 1

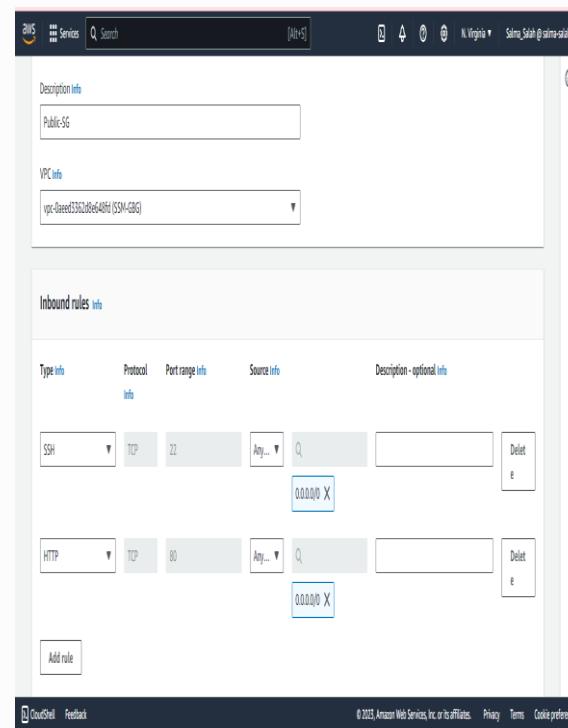
Create Security Groups for Public



The screenshot shows the AWS VPC Security Groups list. The left sidebar is collapsed. The main area displays two security groups: 'sg-0bc91015b57451d7' and 'sg-0ef2a7f0ed3f7713'. Both are associated with the 'default' VPC and have the 'public' security group name. A search bar at the top is empty, and there are buttons for 'Actions', 'Export security groups to CSV', and 'Create security group'.



The screenshot shows the 'Create security group' wizard. The first step, 'Basic details', is completed. The security group name is set to 'Public-SG'. The VPC dropdown is set to 'vpc-0aeeec5362a8e640ff (SSM-SG)'. The second step, 'Inbound rules', is shown below. It contains two rules: one for SSH (TCP port 22) and one for HTTP (TCP port 80). Both rules have 'Any' as the source and '0.0.0.0/0' as the destination. The 'Delete rule' button is visible for each row.



The screenshot shows the 'Edit security group' page for 'Public-SG'. The 'Description info' field is populated with 'Public-SG'. The 'VPC info' dropdown is set to 'vpc-0aeeec5362a8e640ff (SSM-SG)'. The 'Inbound rules' section is expanded, showing the two rules defined in the previous step. The 'Delete rule' button is visible for each row. The bottom of the screen shows the AWS footer.

Create Security Groups for Private

The screenshot shows the AWS VPC Create security group interface. In the 'Basic details' section, the security group name is set to 'Private-SG-1'. The 'Description' field contains 'Private-SG-1'. Under 'VPC Info', the selected VPC is 'vpc-0aeed3362d8e648fd (SSM-GBG)'. In the 'Inbound rules' section, there are two rules: one for SSH (Protocol TCP, Port range 22, Source Any..., 0.0.0.0/0) and one for HTTP (Protocol TCP, Port range 80, Source Any..., 0.0.0.0/0). Both rules have a delete button next to them.

VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
Private-SG-1

Name cannot be edited after creation.

Description Info
Private-SG-1

VPC Info
vpc-0aeed3362d8e648fd (SSM-GBG)

Inbound rules Info

Type <small>Info</small>	Protocol	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
SSH	TCP	22	Any... ▾	0.0.0.0/0 X
HTTP	TCP	80	Any... ▾	0.0.0.0/0 X

Add rule

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS VPC Create security group interface. In the 'Basic details' section, the security group name is set to 'Private-SG-1'. The 'Description' field contains 'vpc-0aeed3362d8e648fd (SSM-GBG)'. In the 'Inbound rules' section, there are two rules: one for SSH (Protocol TCP, Port range 22, Source Any..., 0.0.0.0/0) and one for HTTP (Protocol TCP, Port range 80, Source Any..., 0.0.0.0/0). Both rules have a delete button next to them.

VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Private-SG-1

VPC Info
vpc-0aeed3362d8e648fd (SSM-GBG)

Inbound rules Info

Type <small>Info</small>	Protocol	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
SSH	TCP	22	Any... ▾	0.0.0.0/0 X
HTTP	TCP	80	Any... ▾	0.0.0.0/0 X

Add rule

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create Security Groups for second Private

The screenshot shows the AWS VPC Security Groups creation interface. At the top, there's a navigation bar with the AWS logo, a search bar, and account information for N. Virginia and Salma_Salah. Below the navigation bar, the breadcrumb path is VPC > Security Groups > Create security group. The main title is "Create security group" with an "Info" link. A descriptive text explains that a security group acts as a virtual firewall for your instance to control inbound and outbound traffic. The form is divided into sections: "Basic details" and "Inbound rules".

Basic details

Security group name [Info](#)
Private-SG-2
Name cannot be edited after creation.

Description [Info](#)
Private-SG-2

VPC [Info](#)
vpc-0aeed3362d8e648fd (SSM-GBG)

Inbound rules [Info](#)

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 2

Create IAM Rule with That Allow to Connect to EC2 Instance Using System Manager

The screenshot shows the AWS EC2 Dashboard. At the top, there is a search bar with the placeholder "Search results for 'IAM'". The sidebar on the left contains several sections: EC2 Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, and Elastic Block Store. Under the "Instances" section, there is a "Services [10]" category which includes IAM, IAM Identity Center, Resource Access Manager, and AWS App Mesh.

The screenshot shows the AWS IAM Roles page. The left sidebar includes Identity and Access Management (IAM), Dashboard, User groups, Users, Roles (selected), Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, and Services. The main content area displays a table of existing roles:

Role name	Trusted entities	Last activity
AWSServiceRoleForAmazonElasticFileSystem	AWS Service elasticfilesystem	3 days ago
AWSServiceRoleForAutoScaling	AWS Service autoscaling	3 hours ago
AWSServiceRoleForBackup	AWS Service backup	15 hours ago
AWSServiceRoleForElasticLoadBalancing	AWS Service elasticloadbalancing	4 hours ago
AWSServiceRoleForSupport	AWS Service support	-
AWSServiceRoleForTrustedAdvisor	AWS Service trustedadvisor	-
RULE-SSH	AWS Service ec2	4 hours ago

The screenshot shows the "Create role" wizard, Step 1: Select trusted entity. It includes fields for "Name, review, and create" and "Add permissions". Below these are four options:

- AWS service: Allows entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- AWS account: Allows 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: Allows users federated with SAML 2.0 from a corporate directory to perform actions in this account.

At the bottom, there is a "Use case" section and a "Next Step" button.

- Choose EC2 as Use CASE
- Choose Permission
- Write Role Name

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](#)

© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

IAM > Roles > Create role

Add permissions

Select trusted entity

Permissions policies (1/88) info
Choose one or more policies to attach to your new role.

Name, review, and create

Filter by type

Policy name

AmazonSSMManagedInstanceCore AWS managed The policy for Amazon EC2 Role to enable AWS Sys...

AWSelasticBeanstalkRoleCore AWS managed AWS/ElasticBeanstalkRoleCore [Elastic Beanstalk op...

Set permissions boundary - optional

[Cancel](#) [Previous](#) **Next**

[CloudShell](#) [Feedback](#)

© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

IAM > Roles > Create role

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
GDG-SSM

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.

Step 1: Select trusted entities

Trust policy

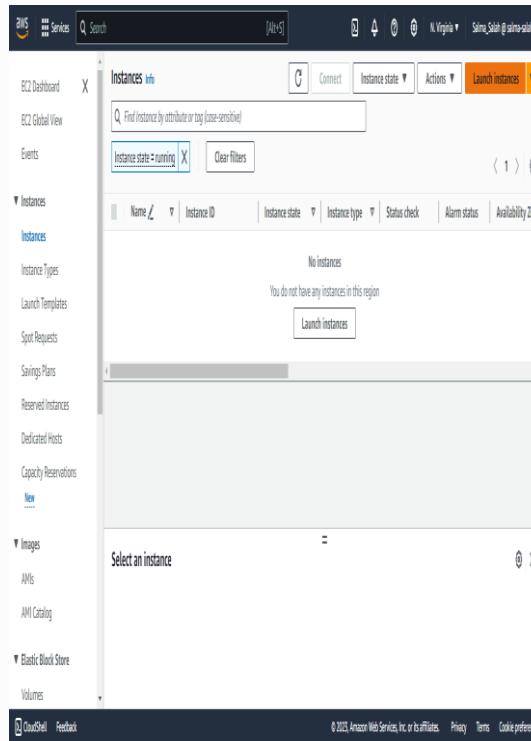
[Edit](#)

[CloudShell](#) [Feedback](#)

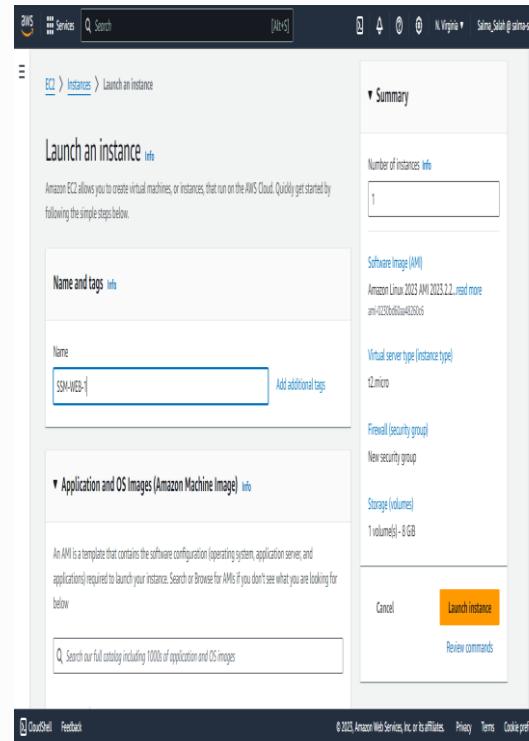
© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step 3

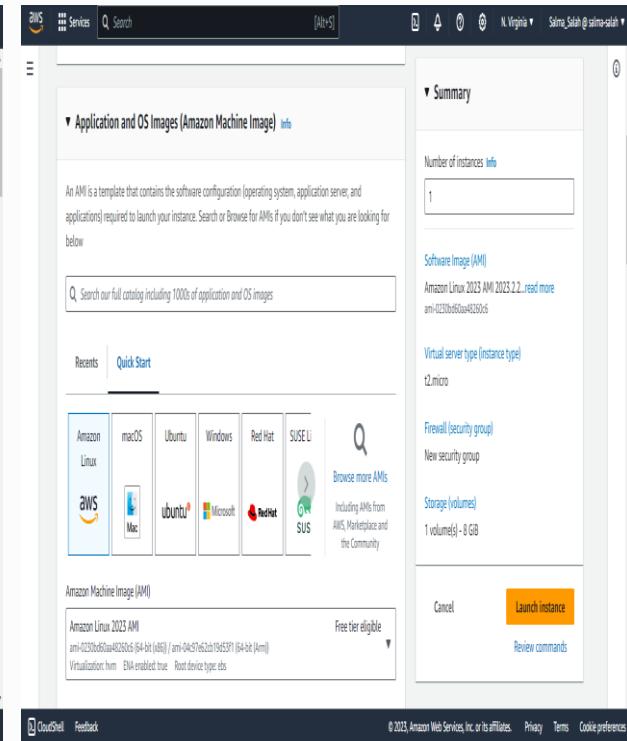
Create EC2 Instance in First Private Subnet



The screenshot shows the AWS EC2 Dashboard. The left sidebar includes links for EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), Elastic Block Store, and Volumes. The main pane displays the 'Instances' section with a search bar and filters for 'Instance state' (set to 'running') and 'Clear filters'. It shows a table with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Zone. A message states 'No instances' and 'You do not have any instances in this region'. A 'Launch instances' button is at the bottom.



The screenshot shows the 'Launch an instance' wizard. Step 1: 'Name and tags'. It shows a 'Name' field with 'SSM-WEB-1' and a 'Virtual server type (instance type)' dropdown set to 't2.micro'. Below are sections for 'Firewall (security group)', 'New security group', and 'Storage (volumes)'. A 'Launch instance' button is at the bottom.



The screenshot shows the 'Launch an instance' wizard. Step 2: 'Application and OS Images (Amazon Machine Image)'. It shows a search bar and a grid of OS images: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, AWS Lambda, and AWS Lambda (Mac). A message says 'Including AMIs from AWS Marketplace and the Community'. At the bottom, it shows 'Amazon Machine Image (AMI) Amazon Linux 2023 AMI ami-0230b65aa4c256c5 (64-bit (x86) / ami-04e297622b19455f) (64-bit (x64)) Virtualization: hvm ENA-enabled true Root device type: ebs'. A 'Launch instance' button is at the bottom.

- Create a New Key Pair
 - Insert in first Private Subnet
 - Choose Private SG

AWS Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah

Instance type Info

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 SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.0716 USD per Hour

On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

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

SSM-KEY

Create new key pair

Network settings

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.2.2...read more

ami-0230bd60aa48260c6

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel Launch instance

Review commands

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah

VPC - required Info
vpc-Qaeed35362d8e648fd (SSM-GBG)
10.0.0.16

Subnet Info
subnet-04ebccaa44b86cd45 Private-SSM-1
VPC: vpc-Qaeed35362d8e648fd Owner: 821594020462 Availability Zone: us-east-1a IP addresses available: 251 CIDR: 10.0.30.0/24

Create new subnet

Auto-assign public IP Info

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

Private-SG-1 sg-09c42a1c5d4223b4e X
VPC: vpc-Qaeed35362d8e648fd

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 2023.2.2...read more
ami-0230bd0a482606

Virtual server type (instance type)
t2.micro

Firewall (security group)
Private-SG-1

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

Cancel Launch instance Review commands

- Select IAM Role
- Launch Instance

The screenshot shows the AWS CloudFormation Launch Wizard interface. On the left, the 'Advanced details' section is expanded, containing fields for 'Domain join directory', 'IAM instance profile', and 'Instance auto-recovery'. The 'IAM instance profile' field has a dropdown menu open, showing 'Select' and 'GBG-SSM' (selected). Below this are three checkboxes for DNS requests. On the right, the 'Summary' section displays the configuration for launching one instance using the 'Amazon Linux 2023 AMI'. It includes fields for 'Software Image (AMI)', 'Virtual server type (instance type)', 'Firewall (security group)', and 'Storage (volumes)'. At the bottom right of the summary section is a prominent orange 'Launch instance' button.

0 x File systems Edit

Advanced details [Info](#)

Domain join directory [Info](#)

Select [Create new directory](#)

IAM instance profile [Info](#)

Select [Create new IAM profile](#)

GBG-SSM
arn:aws:iam:821594020462:instance-profile/GBG-SSM
[View hostname](#) [Info](#)

Enable IP name IPv4 (A record) DNS requests

Enable resource-based IPv4 (A record) DNS requests

Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery [Info](#)

Select

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.2... [read more](#)
ami-0230bd60aa48260c6

Virtual server type (instance type)

t2.micro

Firewall (security group)

Private-SG-1

Storage (volumes)

1 volume(s) - 8 GiB

Cancel [Launch instance](#) Review commands

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create EC2 Instance in Second Private Subnet

The image consists of three side-by-side screenshots of the AWS CloudFront interface, showing the process of launching an EC2 instance.

Screenshot 1: Launch an instance (Step 1)

This step shows the initial configuration:

- Name and tags:** Name is set to "SSM-WEBSITE-2".
- Software Image (AMI):** Amazon Linux 2023 AMI 2023.22 is selected.
- Virtual server type (instance type):** t2.micro
- Firewall (security group):** New security group
- Storage (volumes):** 1 volume(s) - 8 GB
- Buttons:** "Cancel" and "Launch instance"

Screenshot 2: Application and OS Images (Amazon Machine Image) (Step 2)

This step shows the selection of the AMI:

- Summary:** Number of instances: 1
- Software Image (AMI):** Search bar: "Search our full catalog including 1000s of application and OS images". Recent selection: Amazon Linux 2023 AMI 2023.22.
- Virtual server type (instance type):** t2.micro
- Firewall (security group):** New security group
- Storage (volumes):** 1 volume(s) - 8 GB
- Buttons:** "Cancel" and "Launch instance"

Screenshot 3: Instance type (Step 3)

This step shows the selection of the instance type:

- Summary:** Number of instances: 1
- Instance type:** t2.micro (Free tier eligible)
 - Family: t2
 - CPU: 1 vCPU
 - Memory: 1.6 GiB
 - Current generation: Yes
 - On-Demand Windows base pricing: \$0.076 USD per Hour
 - On-Demand SUSE base pricing: \$0.076 USD per Hour
 - On-Demand RHEL base pricing: \$0.076 USD per Hour
 - On-Demand Linux base pricing: \$0.076 USD per Hour
- Additional costs apply for AMIs with pre-installed software:**
- Buttons:** "Cancel" and "Launch instance"

Screenshot 4: Network settings (Step 4)

This step shows the selection of network settings:

- Summary:** Number of instances: 1
- Key pair (login):** Key pair name: "SSM-MEY" (Create new key pair button available)
- Buttons:** "Cancel" and "Launch instance"

- Insert in Second Private Subnet
- Choose Private SG
- Choose IAM Role

aws Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah ▾

▼ Network settings Info

VPC - required [Info](#)
vpc-0aeed3362d8e648fd (SSM-GBG)
10.0.0.0/16

Subnet info

subnet-0c0bd7815628f5f8 Private-SSM-2
VPC vpc-0eed3362d8e648fd Owner: 821594020462
Availability Zone: us-east-1b IP addresses available: 251 CIDR: 10.0.40.0/24

Auto-assign public IP Info

Disable

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
Private-SG-2 sg-07c4c637605f33d38 X
VPC vpc-0aeed3362d8e648fd

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 2023.2.2... [read more](#) ami-0230bd60aa48260c6

Virtual server type (instance type)
t2.micro

Firewall (security group)
Private-SG-2

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

Cancel **Launch instance** **Review commands**

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

aws Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah ▾

0x File systems

Edit

▼ Summary

Number of instances [Info](#)
1

Advanced details Info

Domain join directory [Info](#)
Select [Create new directory](#)

IAM instance profile [Info](#)
Select [Create new IAM profile](#)

Q |
Select
GBG-SSM
arn:aws:iam:821594020462:instance-profile/GBG-SSM
Instance hostname - mmo

Enable IP name IPv4 (A record) DNS requests
 Enable resource-based IPv4 (A record) DNS requests
 Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery [Info](#)
Select

Cancel **Launch instance** **Review commands**

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step 3

Connect to First EC2 Using Session Manager

The screenshot shows the AWS EC2 Instances page. There are two instances listed: SSM-WEB-2 and SSM-WEB-1. Both are running and belong to the t2.micro instance type. The context menu for SSM-WEB-1 is open, with the 'Actions' section expanded. The 'Connect' option is highlighted in blue.

Name	Instance ID	Instance state	Instance type	Status check
SSM-WEB-2	i-0c46db007fc80638	Running	t2.micro	-
SSM-WEB-1	i-018eff1a911c7f08c	Running	t2.micro	2/2 checked

The screenshot shows the 'Connect to instance' dialog for the instance i-018eff1a911c7f08c (SSM-WEB-1). The 'Session Manager' tab is selected. The dialog includes a list of 'Session Manager usage':

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

At the bottom right of the dialog are 'Cancel' and 'Connect' buttons.

Install Httpd

- Yum update -y
- Yum install httpd
- Systemctl enable -now httpd

Session ID: Salma_Salah-08f410f58f382b565 Instance ID: i-018eff1a911c7f08c

Terminate

```
sh-5.2$ sudo su
[root@ip-10-0-30-52 bin]# yum update -y
Last metadata expiration check: 0:20:07 ago on Sun Nov 19 22:53:32 2023.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-10-0-30-52 bin]# yum install httpd -y
Last metadata expiration check: 0:20:35 ago on Sun Nov 19 22:53:32 2023.
Dependencies resolved.
```

Package	Architecture	Version	Repository	Size
Installing:				
httpd	x86_64	2.4.58-1.amzn2023	amazonlinux	47 k
Installing dependencies:				
apr	x86_64	1.7.2-2.amzn2023.0.2	amazonlinux	129 k
apr-util	x86_64	1.6.3-1.amzn2023.0.1	amazonlinux	98 k
generic-logos-httpd	noarch	18.0.0-12.amzn2023.0.3	amazonlinux	19 k
httpd-core	x86_64	2.4.58-1.amzn2023	amazonlinux	1.4 M
httpd-filesystem	noarch	2.4.58-1.amzn2023	amazonlinux	14 k
httpd-tools	x86_64	2.4.58-1.amzn2023	amazonlinux	81 k
libbrotli	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	315 k
mailcap	noarch	2.1.49-3.amzn2023.0.3	amazonlinux	33 k
Installing weak dependencies:				
apr-util-openssl	x86_64	1.6.3-1.amzn2023.0.1	amazonlinux	17 k
mod_http2	x86_64	2.0.11-2.amzn2023	amazonlinux	150 k
mod_lua	x86_64	2.4.58-1.amzn2023	amazonlinux	61 k
Transaction Summary				
Install 12 Packages				
Total download size: 2.3 M				

Session ID: Salma_Salah-08f410f58f382b565 Instance ID: i-018eff1a911c7f08c

Terminate

```
Verifying      : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
Verifying      : httpd-filesystem-2.4.58-1.amzn2023.noarch
                                                               11/12
                                                               12/12

Installed:
  apr-1.7.2-2.amzn2023.0.2.x86_64          apr-util-1.6.3-1.amzn2023.0.1.x86_64        apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
  generic-logos-httd-18.0.0-12.amzn2023.0.3.noarch  httpd-2.4.58-1.amzn2023.x86_64        httpd-core-2.4.58-1.amzn2023.x86_64
  httpd-filesystem-2.4.58-1.amzn2023.noarch    httpd-tools-2.4.58-1.amzn2023.x86_64      libbrotli-1.0.9-4.amzn2023.0.2.x86_64
  mailcap-2.1.49-3.amzn2023.0.3.noarch       mod_http2-2.0.11-2.amzn2023.x86_64      mod_lua-2.4.58-1.amzn2023.x86_64

Complete!
[root@ip-10-0-30-52 bin]# systemctl enable -now httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ip-10-0-30-52 bin]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sun 2023-11-19 23:15:12 UTC; 15s ago
     Docs: man:httpd.service(8)
     Main PID: 25987 (httpd)
       Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
        Tasks: 17 (limit: 1114)
       Memory: 13.0M
         CPU: 7ms
        CGroup: /system.slice/httpd.service
           ├─25987 /usr/sbin/httpd -DFOREGROUND
           ├─25990 /usr/sbin/httpd -DFOREGROUND
           ├─25991 /usr/sbin/httpd -DFOREGROUND
           ├─25992 /usr/sbin/httpd -DFOREGROUND
           └─25993 /usr/sbin/httpd -DFOREGROUND

Nov 19 23:15:12 ip-10-0-30-52.ec2.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Nov 19 23:15:12 ip-10-0-30-52.ec2.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Nov 19 23:15:12 ip-10-0-30-52.ec2.internal httpd[25987]: Server configured, listening on: port 80
[root@ip-10-0-30-52 bin]#
```

Steps To Download a Static Website on EC2 using SSM

1. Make a new directory > mkdir gbg
2. Cd gbg
3. wget (link of static website)
4. Web site will be downloaded ad zip file > unzip(name)
5. See folders after unzip > ls
6. Cd gbg-main
7. Move files to /var/www/html/ > mv * /var/www/html/
8. Review move > Cd /var/www/html
9. ReStart httpd > systemctl restart httpd
10. You static website is ready :)

Downloading A Static Web Site Using wget

Session ID: Salma_Salah-0c6d3d6803f1852e Instance ID: i-00677ec104ce0957

Terminate

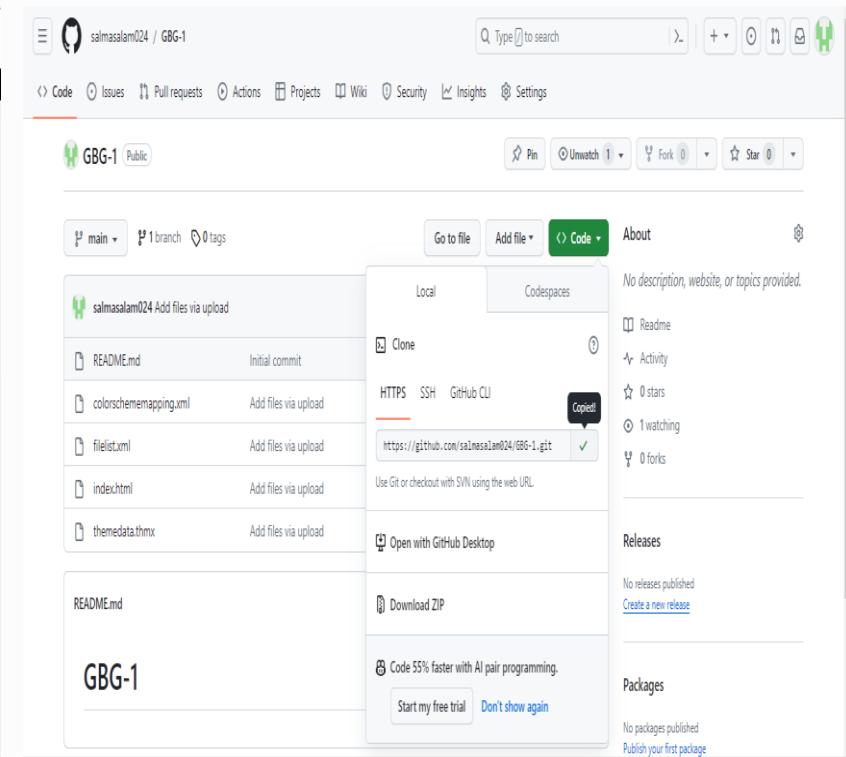
```
[root@ip-10-0-30-172 ~]# mkdir GBG
[root@ip-10-0-30-172 ~]# cd GBG
[root@ip-10-0-30-172 GBG]# wget https://github.com/salmasalam024/GBG-1.git
--2023-11-20 11:24:55-- https://github.com/salmasalam024/GBG-1.git
Resolving github.com (github.com)... 140.82.114.4
Connecting to github.com (github.com)|140.82.114.4|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/salmasalam024/GBG-1 [following]
--2023-11-20 11:24:55-- https://github.com/salmasalam024/GBG-1
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'GBG-1.git'

GBG-1.git                                [ =>                               ] 151.22K  --.-KB/s   in 0.01s

2023-11-20 11:24:55 (18.4 MB/s) - `GBG-1.git' saved [195810]

[root@ip-10-0-30-172 GBG]# wget https://github.com/salmasalam024/GBG-1/archive/refs/heads/master.zip
--2023-11-20 11:31:58-- https://github.com/salmasalam024/GBG-1/archive/refs/heads/master.zip
Resolving github.com (github.com)... 140.82.114.4
Connecting to github.com (github.com)|140.82.114.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/salmasalam024/GBG-1/zip/main [following]
--2023-11-20 11:31:58-- https://codeload.github.com/salmasalam024/GBG-1/zip/main
Resolving codeload.github.com (codeload.github.com)... 140.82.113.9
Connecting to codeload.github.com (codeload.github.com)|140.82.113.9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'master.zip'

master.zip                                [ =>                               ]  8.85K  --.-KB/s   in 0s
```



Downloading A Static Web Site Using wget

Session ID: Salma_Salah-0c66d3d6803f1852e Instance ID: i-00677ec104cee0957

Terminate

```
2023-11-20 11:31:58 (52.6 MB/s) - 'master.zip' saved [9058]

[root@ip-10-0-30-172 GBG]# unzip master.zip
Archive: master.zip
f601e03f0a0f317856343906c227aeaa36ec7fef
  creating: GBG-1-main/
extracting: GBG-1-main/README.md
inflating: GBG-1-main/colorschememapping.xml
inflating: GBG-1-main/filelist.xml
inflating: GBG-1-main/index.html
inflating: GBG-1-main/themedata.thmx
[root@ip-10-0-30-172 GBG]# ls
GBG-1-main  GBG-1.git  master.zip
[root@ip-10-0-30-172 GBG]# cd GBG-1-main
[root@ip-10-0-30-172 GBG-1-main]# ls
README.md  colorschememapping.xml  filelist.xml  index.html  themedata.thmx
[root@ip-10-0-30-172 GBG-1-main]# mv * /var/www/html/
[root@ip-10-0-30-172 GBG-1-main]# cd /var/www/html
[root@ip-10-0-30-172 html]# ls
README.md  colorschememapping.xml  filelist.xml  index.html  themedata.thmx
[root@ip-10-0-30-172 html]# cd
[root@ip-10-0-30-172 ~]# systemctl restart httpd
Unknown command verb restart.
[root@ip-10-0-30-172 ~]# systemctl restart httpd
[root@ip-10-0-30-172 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Mon 2023-11-20 11:34:37 UTC; 10s ago
     Docs: man:httpd.service(8)
 Main PID: 54384 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
   Tasks: 177 (limit: 1114)
  Memory: 12.9M
```

Same Steps in Second EC2 As first

AWS Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah

EC2 Dashboard X

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

New

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Instances (1/2) Info Connect Instance state Actions Launch instances Connect View details Manage instance state Instance settings Networking Security Image and templates Monitor and troubleshoot

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status
SSM-WEB-2	i-0c46db007ffc80638	Running	t2.micro	0/2 ch
SSM-WEB-1	i-018eff1a911c7f08c	Running	t2.micro	0/2 ch

Instance: i-0c46db007ffc80638 (SSM-WEB-2)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0c46db007ffc80638 (SSM-WEB-2)	-	10.0.40.221

IPv6 address Instance state Public IPv4 DNS

Running -

Hostname type Private IP DNS name (IPv4 only)

IP name: ip-10-0-40-221.ec2.internal ip-10-0-40-221.ec2.internal

EC2 > Instances > i-0c46db007ffc80638 > Connect to instance

Connect to instance Info

Connect to your instance i-0c46db007ffc80638 (SSM-WEB-2) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 serial console

Session Manager usage:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- Sessions are secured using AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancel Connect

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Same Steps in Second EC2 As first

Session ID: Salma_Salah-09fa040866e6c4866 Instance ID: i-046db007fc80638

Terminate

```
sh-5.2$ sudo su
[root@ip-10-0-40-221 bin]# yum update -y
Last metadata expiration check: 0:12:41 ago on Sun Nov 19 23:10:04 2023.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-10-0-40-221 bin]# yum install httpd -y
Last metadata expiration check: 0:13:00 ago on Sun Nov 19 23:10:04 2023.
Dependencies resolved.

=====
Package           Architecture     Version      Repository    Size
=====
Installing:
httpd            x86_64          2.4.58-1.amzn2023   amazonlinux  47 k
Installing dependencies:
apr               x86_64          1.7.2-2.amzn2023.0.2  amazonlinux  129 k
apr-util          x86_64          1.6.3-1.amzn2023.0.1  amazonlinux  98 k
generic-logos-httd noarch         18.0.0-12.amzn2023.0.3  amazonlinux  19 k
httpd-core        x86_64          2.4.58-1.amzn2023   amazonlinux  1.4 M
httpd-filesystem noarch         2.4.58-1.amzn2023   amazonlinux  14 k
httpd-tools       x86_64          2.4.58-1.amzn2023   amazonlinux  81 k
libbrotli         x86_64          1.0.5-4.amzn2023.0.2  amazonlinux  315 k
mailcap           noarch         2.1.49-3.amzn2023.0.3  amazonlinux  33 k
Installing weak dependencies:
apr-util-openssl x86_64          1.6.3-1.amzn2023.0.1  amazonlinux  17 k
mod_http2         x86_64          2.0.11-2.amzn2023   amazonlinux  150 k
mod_lua           x86_64          2.4.58-1.amzn2023   amazonlinux  61 k

Transaction Summary

Install 12 Packages

Total download size: 2.3 M
```

Session ID: Salma_Salah-09fa040866e6c4866 Instance ID: i-046db007fc80638

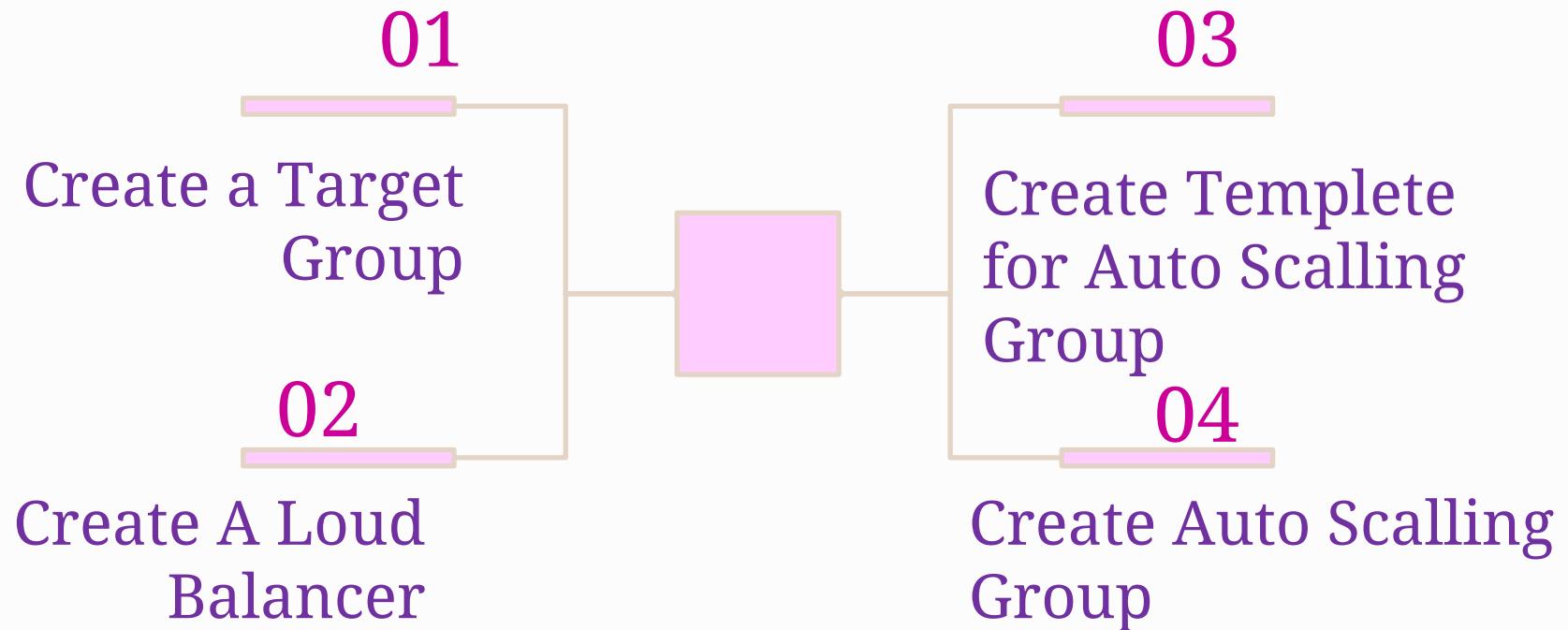
Terminate

```
mailcap-2.1.49-3.amzn2023.0.3.noarch          mod_http2-2.0.11-2.amzn2023.x86_64      mod_lua-2.4.58-1.amzn2023.x86_64

Complete!
[root@ip-10-0-40-221 bin]# systemctl enable --now httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ip-10-0-40-221 bin]# systemctl enable status httpd
Failed to enable unit: Unit file status.service does not exist.
[root@ip-10-0-40-221 bin]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sun 2023-11-19 23:24:04 UTC; 41s ago
     Docs: man:httdp.service(8)
 Main PID: 25741 (httdp)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 177 (limit: 1114)
   Memory: 13.1M
     CPU: 84ms
    Group: /system.slice/httpd.service
           ├─25741 /usr/sbin/httd -DFOREGROUND
           ├─25742 /usr/sbin/httd -DFOREGROUND
           ├─25743 /usr/sbin/httd -DFOREGROUND
           ├─25744 /usr/sbin/httd -DFOREGROUND
           └─25745 /usr/sbin/httd -DFOREGROUND

Nov 19 23:24:04 ip-10-0-40-221.ec2.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Nov 19 23:24:04 ip-10-0-40-221.ec2.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Nov 19 23:24:04 ip-10-0-40-221.ec2.internal httd[25741]: Server configured, listening on: port 80
```

Third Part



Step 1

Create a Target Group

The screenshot shows the 'Specify group details' step of the 'Create target group' wizard. The top navigation bar includes the AWS logo, 'Services', a search bar, and account information for 'N. Virginia' and 'Salma_Salah @ salma-salah'. The left sidebar has a tree view with 'EC2 > Target groups > Create target group' selected. The main content area is titled 'Specify group details' with the sub-section 'Basic configuration'. It states: 'Your load balancer routes requests to the targets in a target group and performs health checks on the targets.' Below this is a 'Basic configuration' section with the note: 'Settings in this section can't be changed after the target group is created.' Under 'Choose a target type', the 'Instances' option is selected, showing the following benefits:

- Supports load balancing to instances within a specific VPC
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

Other options shown are 'IP addresses' and 'Lambda function'. At the bottom, there are 'Step 1: Specify group details' and 'Step 2: Register targets' buttons.

The screenshot shows the 'Register targets' step of the 'Create target group' wizard. The top navigation bar includes the AWS logo, 'Services', a search bar, and account information for 'N. Virginia' and 'Salma_Salah @ salma-salah'. The left sidebar has a tree view with 'EC2 > Target groups > Create target group' selected. The main content area is titled 'Create target group' with the sub-section 'Target group name'. The 'Target group name' field contains 'SSM-TG'. A note below says: 'A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.' Under 'Protocol : Port', 'HTTP' is selected with port '80'. The 'IP address type' section shows 'IPv4' selected, with a note: 'Only targets with the indicated IP address type can be registered to this target group.' Below this, 'IPv6' is listed with a note: 'Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)' and a note: 'Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.' Under 'VPC', it says: 'Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.' A dropdown menu shows 'SSM-GBG' with the value 'vpc-0aeed3362d9e648fd' and 'IPv4: 10.0.0.0/16'. At the bottom, there are 'Step 1: Specify group details' and 'Step 2: Register targets' buttons.

Add Targets to the Target Group

- First EC2 in First Private Subnet
- Second EC2 in Second Private Subnet

The screenshot shows the 'Register targets' step in the AWS Lambda Step Functions interface. It displays a list of available instances:

Instance ID	Name	State	Security groups
i-0c46db007fc80638	SSM-WEB-2	Running	Private-SG-2
i-018eff1a911c7f08c	SSM-WEB-1	Running	Private-SG-1

Two instances are selected, indicated by a blue checkmark. Below the table, it says "2 selected". A port selection field shows "80" and a note "Ports for routing traffic to the selected instances." A "Filter instances" search bar is at the top.

The screenshot shows the 'Review targets' step in the AWS Lambda Step Functions interface. It displays a list of targets:

Remove	Health status	Instance ID	Name	Port	State	Security groups
X	Pending	i-0c46db007fc80638	SSM-WEB-2	80	Running	Private-SG-2
X	Pending	i-018eff1a911c7f08c	SSM-WEB-1	80	Running	Private-SG-1

Both targets are marked as "Pending". Below the table, it says "2 pending". A "Create target group" button is visible at the bottom right. The interface includes standard AWS navigation elements like CloudShell and Feedback.

Review Target Group

The screenshot shows the AWS EC2 Target Groups page for a target group named "SSM-TG".

Details:

- Target type: Instance
- Protocol: Port
- Protocol version: HTTP1
- VPC: [vpc-0aeed3362d8e648fd](#)
- IP address type: IPv4
- Load balancer: [SSM-LB](#)

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
2	2	0	0	0	0

Distribution of targets by Availability Zone (AZ):
Select values in this table to see corresponding filters applied to the Registered targets table below.

Navigation: EC2 > Target groups > SSM-TG

Actions: Actions ▾

Filters:

- Targets
- Monitoring
- Health checks
- Attributes
- Tags

Footer:

- CloudShell
- Feedback
- © 2023, Amazon Web Services, Inc. or its affiliates.
- Privacy
- Terms
- Cookie preferences

Step 2

Create Application Load Balancer

The screenshot shows three sequential steps in the AWS Management Console for creating an Application Load Balancer (ALB).

Step 1: Load balancers

The left pane shows the AWS Services navigation bar with "EC2" selected. The main content area displays the "Load balancers" section. It includes a search bar, a "Create load balancer" button, and a table with columns for Name, DNS name, State, VPC ID, and Availability Zones. A message states "No load balancers". Below the table, it says "Select a load balancer above." and "0 load balancers selected".

Step 2: Load balancer types

The middle pane shows the "Load balancer types" section. It compares three types:

- Application Load Balancer**: Handles HTTP and HTTPS traffic, routing requests to multiple targets.
- Network Load Balancer**: Handles TCP and UDP traffic, routing requests to multiple targets via a VPC.
- Gateway Load Balancer**: Handles SSL/TLS offloading, supporting GPRS/3G traffic.

Below each diagram is a brief description of its use case.

Step 3: Basic configuration

The right pane shows the "Basic configuration" step. It includes fields for "Load balancer name" (set to "SSM-ALB"), "Scheme" (set to "Internet-facing"), and "IP address type" (set to "IPv4"). It also includes a "Network settings" section.

Configuration of Application Load Balancer

- VPC
- Subnets
- SG
- Target Group

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC Info
Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.

SSM-GBG
vpc-0aee03362d8e648fd
IPv4: 10.0.0.16

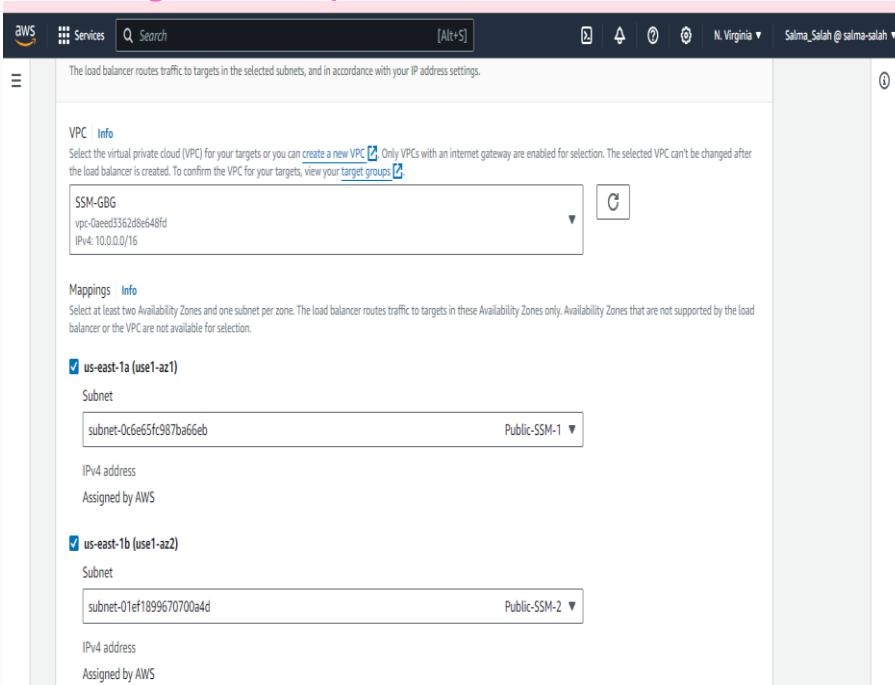
Mappings Info
Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

us-east-1a (use1-az1)
Subnet: subnet-0c6e65fc987ba66eb Public-SSM-1

IPv4 address: Assigned by AWS

us-east-1b (use1-az2)
Subnet: subnet-01ef1899670700a4d Public-SSM-2

IPv4 address: Assigned by AWS



Security groups [Info](#)
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups
Select up to 5 security groups

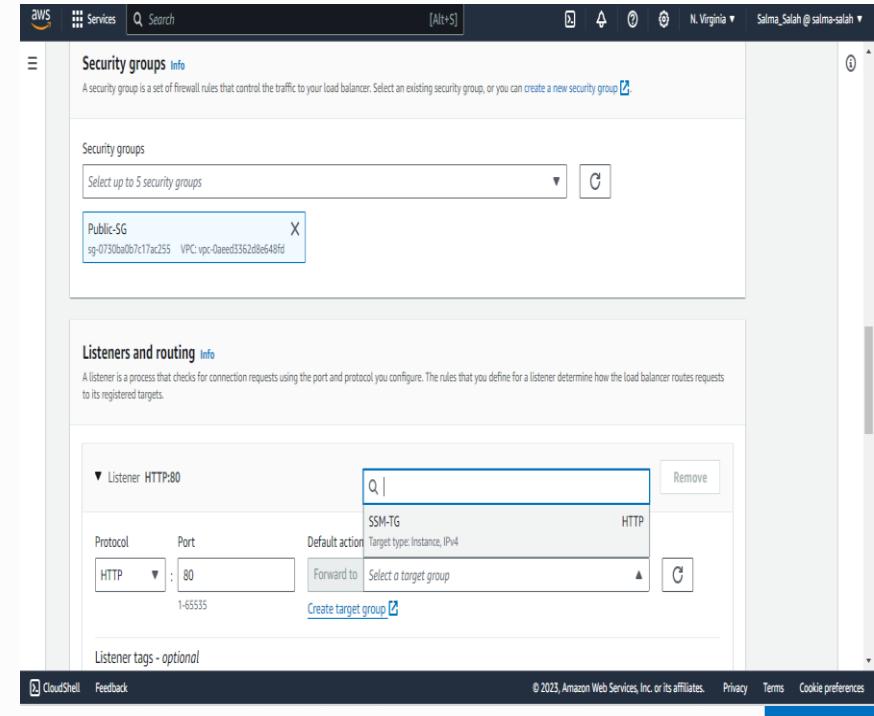
Public-SG
sg-0730ba0b7c17ac255 VPC: vpc-0aee03362d8e648fd

Listeners and routing [Info](#)
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

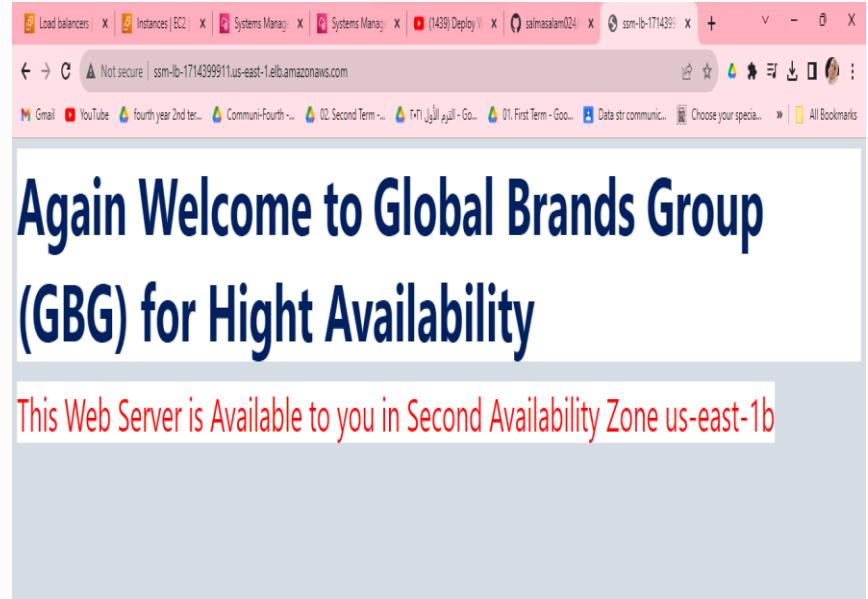
Listener HTTP:80
Protocol: HTTP Port: 80 Default action: SSM-TG Target type: Instance, IPv4
Forward to: Select a target group

1-65535 [Create target group](#)

Listener tags - optional



Access Two Private EC2s In the Target Group through Load Balancer



Step 3

Create Launch Template

- Set Name
- Choose OS

EC2 > Launch templates > Create launch template

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Launch template name - required
SSM-TEMP

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '(', ')', '@'.

Template version description
SSM-TEMP

Max 255 chars

Auto Scaling guidance [Info](#)
Select this if you intend to use this template with EC2 Auto Scaling

Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EC2 > Launch templates > Create launch template

Application and OS Images (Amazon Machine Image) - required [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 | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Linux | Browse more AMIs

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI
ami-0230bd60aa48260c6 [64-bit (x86)] / ami-04c97e62cb19d53f1 [64-bit (Arm)]
Virtualization: hvm ENA enabled: true Root device: ebs

Description

Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Add Security Group
- Add Key

Key pair name: SSM-KEY [Create new key pair](#)

Network settings [Info](#)

Subnet info: Don't include in launch template [Create new subnet](#)

When you specify a subnet, a network interface is automatically added to your template.

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.

Select existing security group [Create security group](#)

Security groups [Info](#)

Select security groups: Private-SG-1 [X](#)
VPC: vpc-0aeeed3362bfe648fd

[Compare security group rules](#)

[Advanced network configuration](#)

[Cancel](#) [Create launch template](#)

Instance type [Info](#) [Advanced](#)

Instance type: t2.micro [Free tier eligible](#)

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

All generations [Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

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: SSM-KEY [Create new key pair](#)

[Cancel](#) [Create launch template](#)

- Add IAM Role to be Able to Connect using SSM
- Add User Data so AutoScaled Instances Has httpd installed

The screenshot shows the 'Advanced details' section of the IAM Instance Profile creation wizard. It includes fields for IAM instance profile, User data - optional, Enable resource-based (IPv6 (AAAA record) DNS requests, Instance auto-recovery, Shutdown behavior, and Not applicable for EC2 Auto Scaling.

IAM instance profile: GBG-SSM
arn:aws:iam::821594020462:instance-profile/GBG-SSM

User data - optional: Don't include in launch template

Enable resource-based (IPv6 (AAAA record) DNS requests:

Instance auto-recovery: Don't include in launch template

Shutdown behavior: Not applicable for EC2 Auto Scaling

The screenshot shows the 'User data' section of the Launch Template creation wizard. It displays a code editor containing a shell script to install and start the Apache HTTP Server (httpd).

```
#!/bin/bash
sudo yum update -y
sudo yum install httpd -y
sudo systemctl disable --now firewalld
sudo systemctl enable --now httpd
EC2AZ=$[TOKEN= curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" & curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/placement/availability-zone]
```

User data - optional: Don't include in launch template

User data:

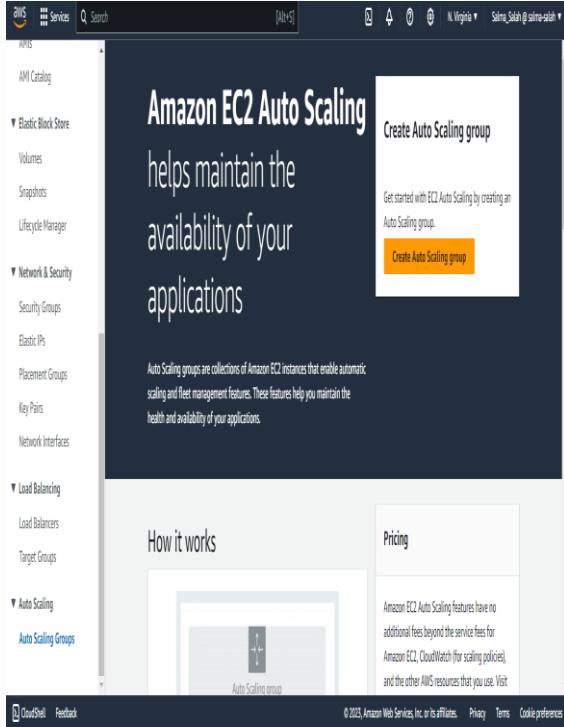
Choose file:

User data has already been base64 encoded:

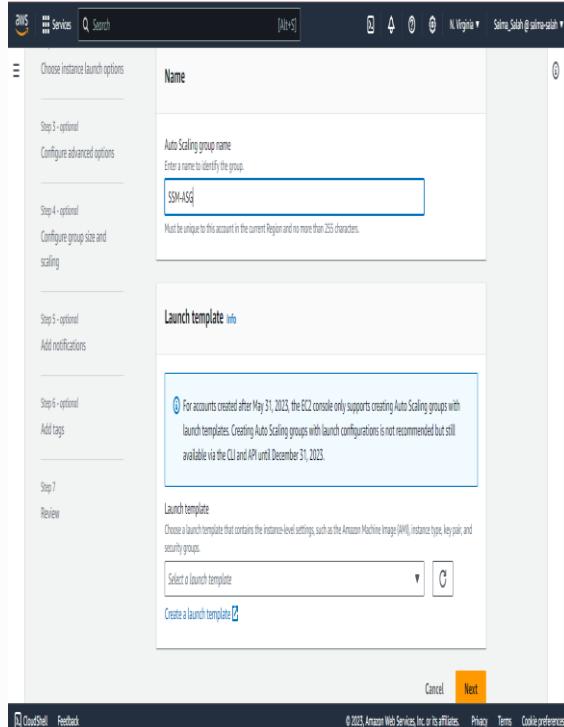
Part 4

Create AutoScaling Group

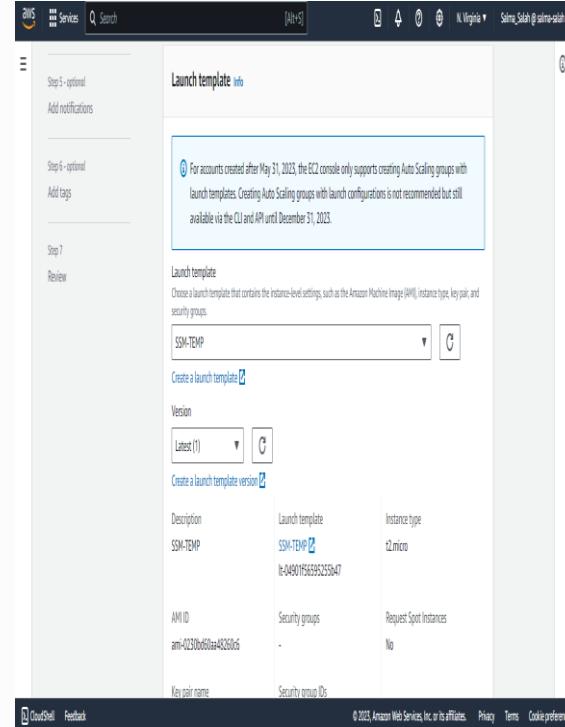
- Set Name
- Add Launch Template



The screenshot shows the Amazon EC2 Auto Scaling landing page. It features a large central banner with the text "Amazon EC2 Auto Scaling helps maintain the availability of your applications". Below the banner, there's a section titled "How it works" showing a diagram of an Auto Scaling group. Another section titled "Pricing" provides information about costs. On the left sidebar, there are links for 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, Auto Scaling, and Auto Scaling Groups.



This screenshot shows the "Create Auto Scaling group" wizard at Step 3: "Choose instance launch options". The "Name" field is populated with "SSM-ASG". The "Launch template" dropdown is set to "SSM-TEMP". A note states: "For accounts created after May 31, 2013, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2013." The "Next Step" button is visible at the bottom right.



This screenshot shows the "Create Auto Scaling group" wizard at Step 7: "Review". The "Launch template" dropdown is set to "SSM-TEMP". The "Version" dropdown is set to "Latest (1)". The "Description" is "SSM-TEMP", "Launch template" is "SSM-TEMP", and "Instance type" is "t2.micro". The "AMI ID" is "ami-01234567890abcdef", "Security groups" is "-", and "Request Spot Instances" is "No". The "Key pair name" is "Salma_Salih" and "Security group IDs" is "-". A note states: "For accounts created after May 31, 2013, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2013." The "Create" button is highlighted in orange at the bottom right.

Choose Availability Zones & Subnets in Which Auto Scaling is Used

- Private Subnet 1 in us-east-1a
- Private Subnet 2 in us-east-1b

The screenshot shows the AWS Auto Scaling configuration interface at Step 6 - optional. The main section is titled "Network" with an "Info" link. It contains a note about using multiple Availability Zones for better application balance. Below this, the "VPC" section is shown, where the user has selected "vpc-0aed3362d8e648fd (SSM-GBG)" and "10.0.0.0/16". There is also a "Create a VPC" button. The "Availability Zones and subnets" section follows, with a dropdown menu showing "Select Availability Zones and subnets". Two subnets are listed: "us-east-1a | subnet-0c4ebcca44b86cd45 (Private-SSM-1)" with IP range "10.0.30.0/24" and "us-east-1b | subnet-0cdbd7e815628f5f8 (Private-SSM-2)" with IP range "10.0.40.0/24". Both subnets have a delete "X" icon. A "Create a subnet" button is located at the bottom of this section. The top navigation bar includes the AWS logo, Services, Search, and user information (N. Virginia, Salma_Salah @ salma-salah). The bottom navigation bar includes CloudShell, Feedback, and links to Privacy, Terms, and Cookie preferences.

- Choose Load Balancer
- Set Desired Capacity
- Set Min Desired Capacity & Max Desired Capacity

AWS Services Search [Alt+S]

Step 3 - optional

Configure advanced options

Step 4 - optional

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer
Choose from your existing load balancers.

Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

Choose from your load balancer target groups
This option allows you to attach Application, Network, or Gateway Load Balancers.

Choose from Classic Load Balancers

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups ▾

SSM-TG | HTTP X

Application Load Balancer: SSM-LB

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S]

Choose instance launch options

Step 3 - optional

Configure advanced options

Step 4 - optional

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

Group size Info

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances) ▾

Desired capacity

Specify your group size.

2

Scaling Info

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity Max desired capacity

2 4

Equal or less than desired capacity Equal or greater than desired capacity

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Choose Auto Scaling to Start Based on the CPU Utilization IF CPU Utilization is > 80%

The screenshot shows the AWS CloudWatch Metrics console interface for creating a new scaling policy. The top navigation bar includes the AWS logo, Services, a search bar, and user information (N. Virginia, Salma_Salah @ salma-salah). The main section is titled "Automatic scaling - optional" and asks to choose a scaling policy. Two options are shown: "No scaling policies" (disabled) and "Target tracking scaling policy" (selected). The "Target tracking scaling policy" section describes how it uses CloudWatch metrics and target values to adjust capacity. Below this, fields are filled out: "Scaling policy name" is "Target Tracking Policy", "Metric type" is "Average CPU utilization", and "Target value" is "80". An "Instance warmup" field is set to "300 seconds". A checkbox for "Disable scale in to create only a scale-out policy" is unchecked.

Automatic scaling - optional

Choose whether to use a target tracking policy | [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling policy
Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

Target Tracking Policy

Metric type [Info](#)

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization

Target value

80

Instance warmup [Info](#)

300 seconds

Disable scale in to create only a scale-out policy

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Review Auto Scaling Group

AWS Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1: Choose launch template [Edit](#)

Step 2: Choose instance launch options [Edit](#)

Step 3 - optional [Configure advanced options](#)

Step 4 - optional [Configure group size and scaling](#)

Step 5 - optional [Add notifications](#)

Step 6 - optional [Add tags](#)

Step 7: Review [Edit](#)

Group details

Auto Scaling group name: SSM-ASG

Launch template

Launch template	Version	Description
SSM-TEMP	Latest	SSM-TEMP lt-04901f569525b047

Step 2: Choose instance launch options [Edit](#)

Network

VPC: vpc-0aeed3362d8e648fd

Availability Zone	Subnet	CIDR Range
us-east-1a	subnet-0c4ebcca44b86cd45	10.0.30.0/24
us-east-1b	subnet-0cbd7e815628f5fb	10.0.40.0/24

Instance type requirements

This Auto Scaling group will adhere to the launch template.

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S] N. Virginia Salma_Salah @ salma-salah

Step 6 - optional [Add tags](#)

Step 7: Review [Edit](#)

Step 2: Choose instance launch options

Network

VPC: vpc-0aeed3362d8e648fd

Availability Zone	Subnet	CIDR Range
us-east-1a	subnet-0c4ebcca44b86cd45	10.0.30.0/24
us-east-1b	subnet-0cbd7e815628f5fb	10.0.40.0/24

Instance type requirements

This Auto Scaling group will adhere to the launch template.

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Review Auto Scaling Group

Step 3: Configure advanced options

Load balancing

Load balancer 1

Name	Type	Target group
SSM-LB	Application/HTTP	SSM-TG

VPC Lattice integration options

VPC Lattice target groups

Health checks

Health check type	Health check grace period

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 4: Configure group size and scaling policies

Group size

Desired capacity	Desired capacity type
2	Units (number of instances)

Scaling

Minimum desired capacity	Maximum desired capacity
2	4

Target tracking policy

Policy type	Scaling policy name	Execute policy when
Target tracking scaling	Target Tracking Policy	As required to maintain Average CPU utilization at 80

Take the action

Instances need	Scale in
Add or remove capacity units as required	300 seconds to warm up before including in metric

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 5: Add notifications

Instance scale-in protection

Enable instance protection from scale in

Notifications

No notifications

Step 6: Add tags

Tags (0)

Key	Value	Tag new instances
		No tags

Cancel Previous Create Auto Scaling group

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Simulate Traffic using Stress to Test Auto Scaling in First EC2

The screenshot shows the AWS EC2 Instances page with a selected instance. A modal window titled "Connect to instance" is open, showing session manager usage instructions and a "Connect" button.

Session Manager usage:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Session ID: Salma_Salah-025b02cb04fb439cb Instance ID: i-018eff1a911c7f08c

```
sh-5.2$ sudo su
[root@ip-10-0-30-52 ~]# yum install stress
Last metadata expiration check: 1:22:04 ago on Sun Nov 19 22:53:32 2023.
Dependencies resolved.

Transaction Summary
=====
Install 1 Package

Total download size: 37 k
Installed size: 78 k
Is this ok [y/N]: y
Downloading Packages:
stress-1.0.4-28.amzn2023.0.2.x86_64.rpm          391 kB/s | 37 kB   00:00

Total                                         225 kB/s | 37 kB   00:00

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :
  Installing    : stress-1.0.4-28.amzn2023.0.2.x86_64
  Running scriptlet: stress-1.0.4-28.amzn2023.0.2.x86_64
  Verifying      : stress-1.0.4-28.amzn2023.0.2.x86_64
  Installed      : stress-1.0.4-28.amzn2023.0.2.x86_64

1/1
1/1
1/1
1/1
```

Simulate Traffic using Stress to Test Auto Scaling in Second EC2

The screenshot shows the AWS EC2 Session Manager interface. At the top, there's a navigation bar with the AWS logo, a search bar, and account information (N. Virginia, Salma_Salah @ salma-salah). Below the navigation bar, the URL is EC2 > Instances > i-0c46db007fc80638 > Connect to instance. The main content area is titled "Connect to instance" with a "Info" link. It says "Connect to your instance i-0c46db007fc80638 (SSM-WEB-2) using any of these options". There are four tabs: "EC2 Instance Connect", "Session Manager" (which is selected), "SSH client", and "EC2 serial console". A section titled "Session Manager usage:" lists the following bullet points:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

At the bottom, there are "Cancel" and "Connect" buttons. The footer includes links for Feedback, © 2023, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

The screenshot shows a terminal session on an Amazon Linux 2 instance. The session ID is Salma_Salah-0ed5fd6a10749a1e and the instance ID is i-0c46db007fc80638. The terminal output shows the following steps:

```
sh-5.2$ sudo su
[root@ip-10-0-40-221 ~]# yum install stress
Last metadata expiration check: 1:09:03 ago on Sun Nov 19 23:10:04 2023.
Dependencies resolved.

Transaction Summary
Install 1 Package

Total download size: 37 k
Installed size: 78 k
Is this ok [y/N]: y
Downloading Packages:
stress-1.0.4-28.amzn2023.0.2.x86_64.rpm          431 kB/s | 37 kB   00:00

Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing       : 1/1
  Installing     : stress-1.0.4-28.amzn2023.0.2.x86_64 1/1
  Running scriptlet: stress-1.0.4-28.amzn2023.0.2.x86_64 1/1
  Verifying       : stress-1.0.4-28.amzn2023.0.2.x86_64 1/1

Installed:
  stress-1.0.4-28.amzn2023.0.2.x86_64
```

The Two New EC2s From Auto Scaling

The screenshot shows the AWS EC2 Instances page with the following details:

Instances (4) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
i-00677ec104cee0957	i-00677ec104cee0957	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a
SSM-WEB-2	i-0c46db007ffc80638	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b
SSM-WEB-1	i-0f28f0a52b2a20674	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b
	i-018eff1a911c7f08c	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a

Select an instance

Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The left sidebar shows the navigation menu for EC2, including Instances, Images, and Elastic Block Store sections.

Access Two Private EC2s In the Target Group through Load Balancer



Access Auto Scalled Two Private EC2s through Load Balancer

The screenshot shows a web browser window with the URL `ssm-lb-1714399911.us-east-1.elb.amazonaws.com`. The page content is:

Welcome to Global Brands Group (GBG) for Auto Scaling

Even If Traffic is High we will host your Web Server

The screenshot shows a web browser window with the URL `ssm-lb-1714399911.us-east-1.elb.amazonaws.com`. The page content is:

Welcome to Global Brands Group (GBG) for Auto Scaling & High Availability

This is Second Auto Scaled Web Server In second Availability Zone us-east-1b