

Intel® Endpoint Management Assistant (Intel® EMA)

Deployment Guide for Amazon Web Services (AWS)

Intel® EMA Version 1.7

February 2022

Legal Disclaimer

Copyright 2022 Intel Corporation.

This software and the related documents are Intel copyrighted materials, and your use of them is governed by the express license under which they were provided to you ("License"). Unless the License provides otherwise, you may not use, modify, copy, publish, distribute, disclose or transmit this software or the related documents without Intel's prior written permission.

This software and the related documents are provided as is, with no express or implied warranties, other than those that are expressly stated in the License.

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses. Check with your system manufacturer or retailer or learn more at <http://www.intel.com/technology/vpro>.

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Contents

1	Introduction	1
1.1	About Cloud Computing	1
1.2	Navigating in the AWS Management Console.....	1
1.2.1	Services.....	1
1.2.2	Resource Groups.....	2
1.2.3	Regions.....	2
1.3	Tags and Resource Groups	2
1.4	Before You Begin.....	2
2	High-level Architecture Diagrams.....	3
2.1	Single Server Deployment.....	3
2.2	Distributed Server Deployment	3
3	Select the Deployment Region	4
4	Network Deployment.....	5
4.1	Overview	5
4.2	Create a VPC.....	5
4.2.1	Navigate to the VPC Service	5
4.2.2	Create a VPC	6
4.2.3	Configure VPC Details	6
4.3	Create Subnets.....	6
4.3.1	Navigate to the Subnets screen	6
4.3.2	Create first private subnet.....	7
4.3.3	Create second private subnet.....	7
4.3.4	Create first public subnet	8
4.3.5	Create second public subnet.....	8
4.3.6	Review your subnets.....	9
4.4	Create an Internet Gateway for the public subnets	9
4.4.1	Create Internet Gateways	9
4.4.2	Attach Internet Gateway to the VPC.....	9
4.4.3	Enter attachment details.....	10
4.5	Create NAT Gateways for the private subnets	10
4.5.1	Navigate to NAT Gateways	10
4.5.2	Create first NAT Gateway.....	11
4.5.3	Create second NAT Gateway.....	12
4.6	Create and Configure Route Tables.....	12
4.6.1	Navigate to Route Tables.....	12
4.6.2	Create route table for public subnets.....	13
4.6.3	Create route table for first private subnet	13
4.6.4	Create route table for second private subnet	13
4.6.5	Review the route table list.....	14
4.6.6	Edit routes for the first private subnet route table.....	14
4.6.7	Edit subnet associations for the first private subnet route table	15
4.6.8	Edit routes for the second private subnet route table.....	15
4.6.9	Edit subnet associations for the second private subnet route table	16
4.6.10	Edit routes for the public subnet route table	17
4.6.11	Edit subnet associations for the public subnet route table	17
4.7	Security Groups	18
4.7.1	Create a Security Group for the VM(s).....	18
4.7.2	Update Security Group to Allow Traffic Between Intel EMA VMs (Distributed Server Only)	20
4.7.3	Create a Security Group for the Database	21
5	Virtual Machine Deployment	23

5.1	Overview	23
5.2	Create Virtual Machine(s).....	23
5.2.1	Navigate to the EC2 Service.....	23
5.2.2	Launch an EC2 Instance	24
5.2.3	Choose an Amazon Machine Image	24
5.2.4	Select the Machine Type.....	24
5.2.5	Configure Instance Details	25
5.2.6	Add Storage.....	25
5.2.7	Add Tags.....	25
5.2.8	Configure Security Group	26
5.2.9	Review Instance Launch	26
5.2.10	Select an EC2 Key Pair	26
5.3	Create a Second EC2 Instance (Distributed Server Only)	26
6	Configure AWS Systems Manager (Distributed Server Only)	27
6.1	Navigate to Systems Manager service	27
6.2	Start Quick Setup	27
6.3	Choose Permissions options	28
6.4	Choose Configurations options.....	28
6.5	Choose Targets	29
6.6	Verify Managed Instances List	29
6.7	Logging into your virtual machines via Session Manager.....	29
7	Relational Database Service (RDS) Deployment.....	30
7.1	Navigate to the RDS Service	30
7.2	Create Database Subnet Group.....	30
7.2.1	Subnet Group Details	31
7.3	Create a Database	31
7.3.1	Choose a Database Creation Method	32
7.3.2	Choose Engine Type and Edition.....	32
7.3.3	Choose Deployment Template	32
7.3.4	Configure Instance Name and Master User Credentials	33
7.3.5	Configure DB Instance Size.....	33
7.3.6	Configure Storage (Optional)	33
7.3.7	Configure Connectivity	34
7.3.8	Configure Connectivity - Additional Connectivity Configuration	34
7.3.9	Review and Create	35
7.4	Get Database Hostname.....	35
8	Load Balancer Deployment (Distributed Server Only)	36
8.1	Overview	36
8.2	Create Target Groups	36
8.2.1	Create Target Groups	36
8.2.2	Configure a Target Group for TCP/443.....	37
8.2.3	Create/Configure a Target for TCP/8084.....	38
8.2.4	Configure a Target for TCP/8080.....	38
8.2.5	Review Target Groups	39
8.2.6	Enable Stickiness for the TCP/443 Target Group.....	39
8.2.7	Enable Stickiness for the TCP/8084 Target Group.....	40
8.2.8	Note on Monitoring Target Group Health.....	40
8.3	Create a Network Load Balancer for web traffic.....	40
8.3.1	Create the Load Balancer.....	40
8.3.2	Choose Load Balancer Type	41
8.3.3	Configure Load Balancer.....	42
8.4	Create a Network Load Balancer for swarm traffic.....	43
8.4.1	Create the Load Balancer.....	43
8.4.2	Choose Load Balancer Type	44

8.4.3	Configure Load Balancer.....	45
8.4.4	Note the Load Balancer DNS Name.....	46
9	Appendix A - Notes on Active Directory Integration.....	48
10	Architecture Diagram with Active Directory Integration.....	49
10.1	Single Server Deployment.....	49
10.2	Distributed Server Deployment	49
10.3	Using AWS AD Connector to Extend Active Directory to the Cloud.....	49

1 Introduction

This document describes the procedure to deploy infrastructure to Amazon Web Services, a cloud computing platform, needed to support one or more instances of the Intel® Endpoint Management Assistant (Intel® EMA) server. It is intended for IT administrators with intermediate to advanced knowledge of IT infrastructure who may have limited knowledge about cloud computing.

There are several components needed for a complete cloud infrastructure environment, so we recommend that you read this guide carefully to understand how they are configured to work together. A description of each component is provided before the deployment procedure, with a link to the official cloud provider documentation for further information if needed.

1.1 About Cloud Computing

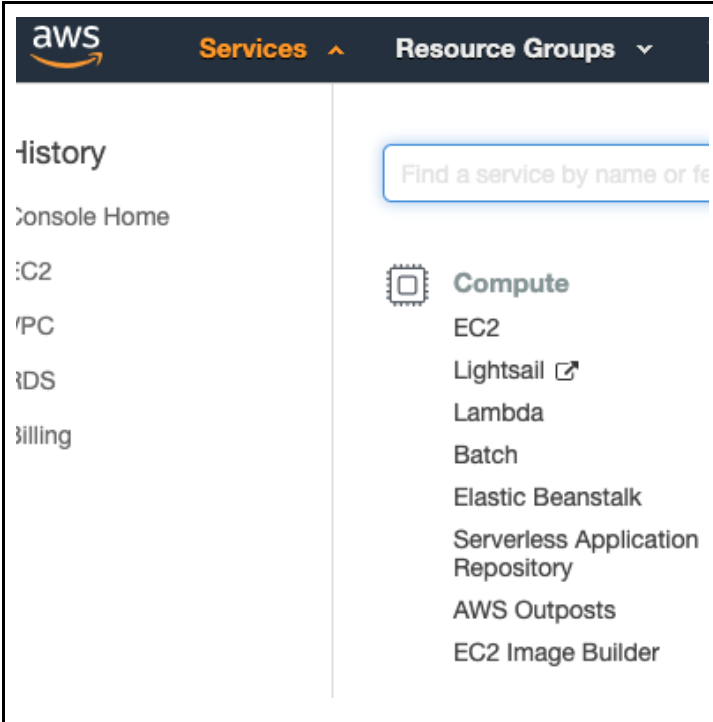
Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider. You can provision only what you need now and scale capacity to grow and shrink as business needs change.

Large cloud providers have data centers all around the world, allowing you to deploy resources geographically close to where your customers and end users are located.

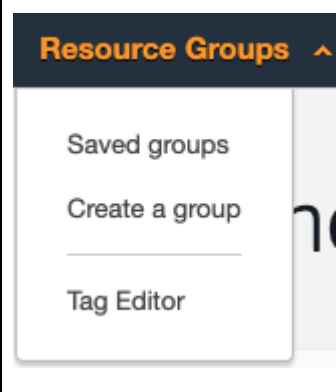
With fully-managed services like Amazon Relational Database Service, you can just focus on your data while the cloud provider manages all of the underlying hardware and software that provide the service. With virtual machines running in the cloud, you manage only the guest operating system and the software installed on it, while the cloud provider manages the underlying hardware and strives to provide you with the best reliability and availability.

1.2 Navigating in the AWS Management Console

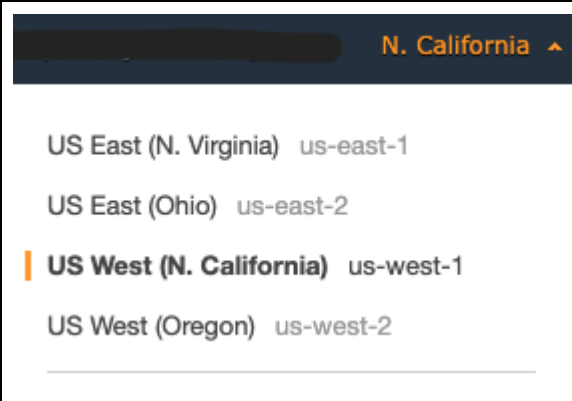
1.2.1 Services

	<p>After you have logged into the AWS Management Console at https://aws.amazon.com/console/ then you will see a Services menu in the top left corner of the screen.</p> <p>Clicking on this will open a list of all the services that AWS provides, organized by category like Compute, Storage, Database, and others.</p> <p>When deploying services in this guide, we will provide instructions directing you to this screen to select the appropriate service.</p>
------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.2.2 Resource Groups

	<p>Next to Services is the Resource Groups menu, where you can create or view resource groups that you have created.</p> <p>Normally you will see all resources deployed in the current region, regardless of who deployed it or which project it belongs to, so using resource groups can provide you with a filtered list of resources based on custom tags that you have attached to each resource.</p>
----------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.2.3 Regions

	<p>In the top right corner of the management console, you will see a menu where you must select the region where you want to deploy resources.</p> <p>You will only be able to see resources listed for the region that you have selected.</p>
-----------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Each AWS Region contains multiple distinct locations called Availability Zones, or AZs. Each Availability Zone is engineered to be isolated from failures in other Availability Zones.

1.3 Tags and Resource Groups

Tags are custom key-value pairs that you can assign to many different kinds of resources that you can deploy in AWS. It is a good practice to tag resources when they are created to enable you to more easily keep track of the resource owner, which project it belongs to, enable having a tag-based Resource Group, and enable tag-based billing reports.

We will not use tagging or create Resource Group in this guide since they are many different ways to do it and it would add a lot of extra steps, but you should be aware that it exists in case you want to implement a tagging and resource grouping strategy.

For more information about using tags, visit the following link:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

1.4 Before You Begin

If your organization already has a AWS account, then you should ask to have a cloud administrator grant you sufficient access to be able to create all of the resources listed in this guide.

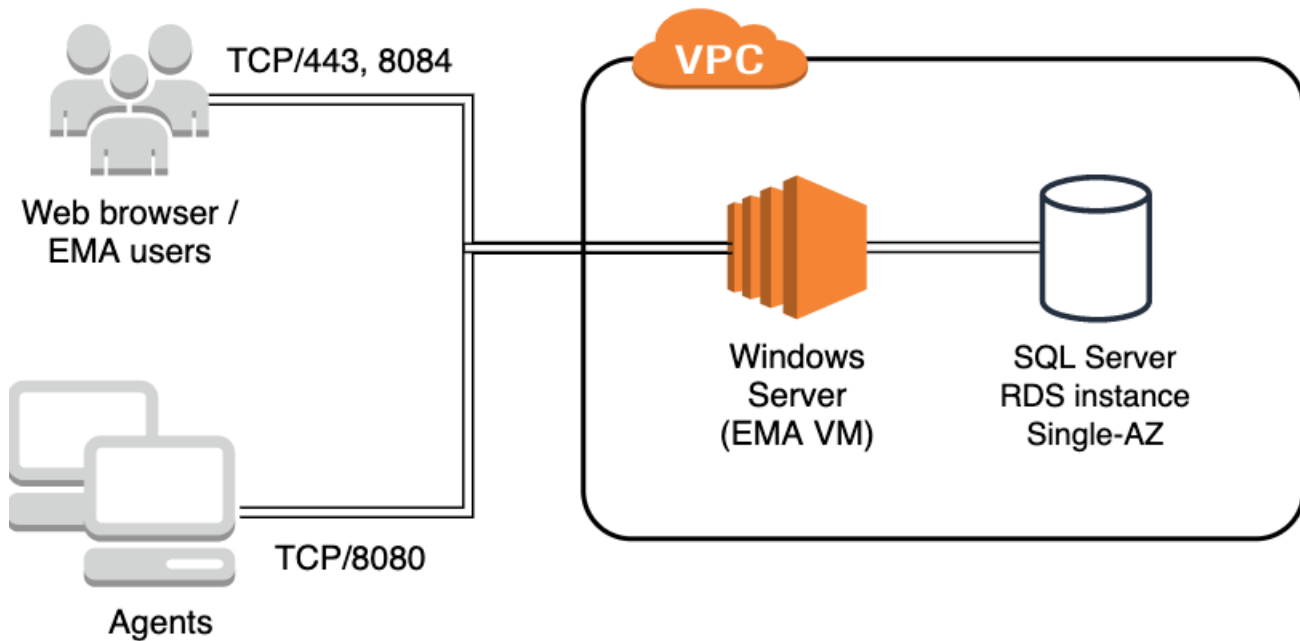
If your organization doesn't have a AWS account, or you want to evaluate it as an individual, then you can go to

<https://aws.amazon.com/console/> and click the **Create a Free Account** button.

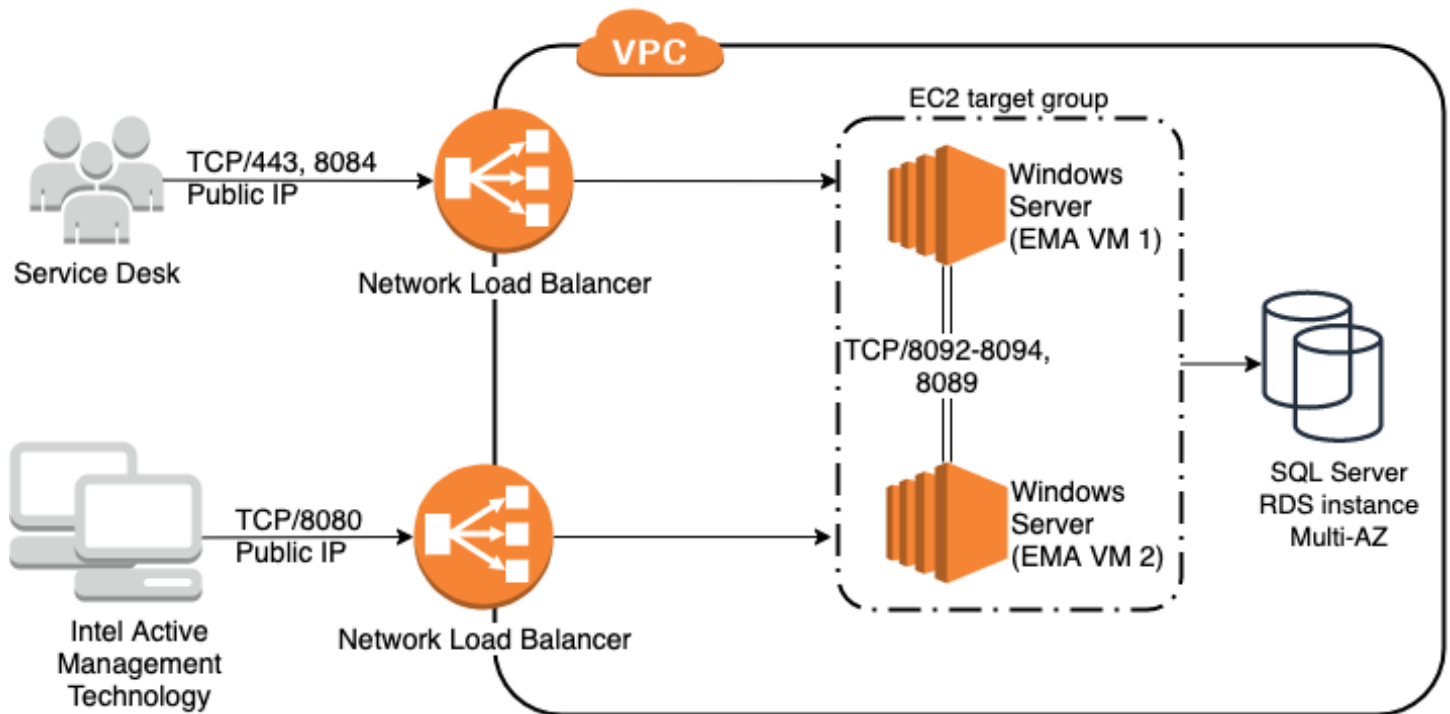
Check with your network administrator to ask if there is a preferred address space to use. You will want to avoid overlapping with your corporate network to prevent routing issues if you already have a VPN established to the cloud provider, or if you will in the future. You will also want to find out what the source IP address will be for traffic leaving your organization to reach the cloud so that you'll be able to allow only trusted networks to reach the Intel EMA virtual machine from the internet.

2 High-level Architecture Diagrams

2.1 Single Server Deployment



2.2 Distributed Server Deployment



3 Select the Deployment Region



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

US East (Ohio) us-east-2

US West (N. California) us-west-1

US West (Oregon) us-west-2

4 Network Deployment

4.1 Overview

In order for virtual machines to communicate with each other, with the cloud provider, or with the internet, we first need to configure a network environment. A Virtual Private Cloud (VPC) is the fundamental building block for your private network in AWS, and it closely resembles a traditional network except that it is virtualized within AWS. VPCs are logically isolated from each other.

When creating a VPC you will need to provide a custom private IP address space. AWS will assign resources a private IP address from this address space when needed. It is recommended that you avoid using an address space that overlaps with your organization's other network ranges in order to avoid routing conflicts if the networks become connected through a VPN. You should consult with your network engineering team to identify an available IP address block to use to avoid routing conflicts in case your company already has private IP connectivity to the cloud or will in the future.

After we create the VPC we'll also create our subnets. Subnets enable you to segment the VPC network by allocating a portion of the network's address space to each subnet. Our subnets will live in two separate Availability Zones (AZ) within our chosen Region so that we can provide higher availability for our database, and Intel EMA application. We will create both public and private subnets to use depending whether the resource needs direct internet access with a public IP address.

By default, the AWS firewall permits no inbound access to our resources, so part of the network deployment will include creating security groups to enable network communication to those resources.

To reduce the attack surface of our virtual machines, RDP will not be allowed in through the VPC firewall. Instead we will use the AWS Session Manager to enable remote management of the VMs. Also, for distributed server deployments, none of the virtual machines will have a public IP address.

For more information about VPCs, visit the following links:

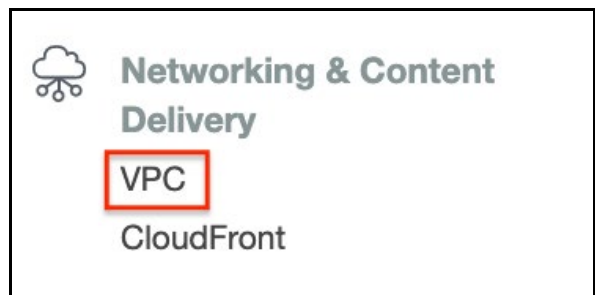
<https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-vpc.html>

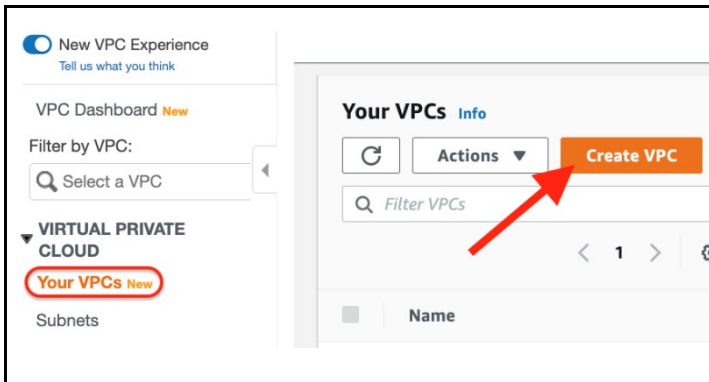
4.2 Create a VPC

The VPC Wizard could be used if you are only doing a single server deployment with one public subnet, but here we will create all of the networking components manually to give better visibility into what we need and because the wizard would not suffice for a distributed server deployment.

4.2.1 Navigate to the VPC Service

 <p>The screenshot shows the AWS Services menu. Under the 'Networking & Content Delivery' category, the 'VPC' service is highlighted with a red rectangular box. Other visible services include CloudFront.</p>	<p>From the Services menu, under Network & Content Delivery, select VPC.</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------

4.2.2 Create a VPC



From the VPC sidebar, select **Your VPCs**.

Click the **Create VPC** button.

4.2.3 Configure VPC Details

The screenshot shows the 'VPC settings' form. The 'Name tag - optional' field contains 'intel-ema-network'. The 'IPv4 CIDR block' section has 'IPv4 CIDR manual input' selected, with the value '10.250.0.0/24'. The 'IPv6 CIDR block' section has 'No IPv6 CIDR block' selected. The 'Tenancy' dropdown is set to 'Default'.

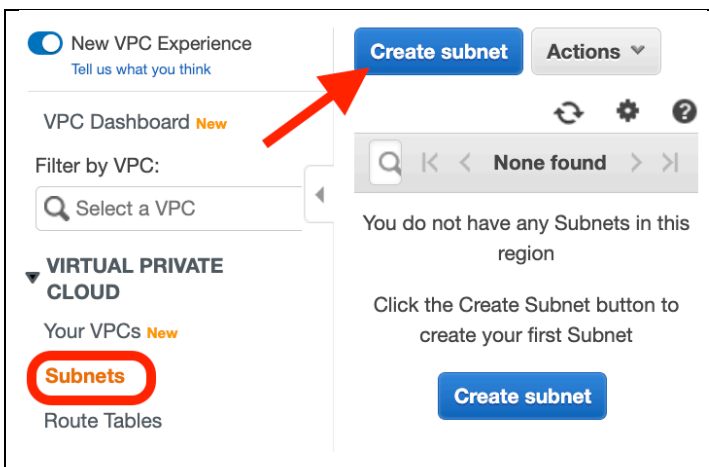
Enter the network details as follows

- **Name Tag:** Enter a unique name for the VPC.
Example: *intel-ema-network*
- **IPv4 CIDR block:** Choose an unused network large enough to contain your subnets.
Example: *10.250.0.0/24*

Click the **Create VPC** button

4.3 Create Subnets

4.3.1 Navigate to the Subnets screen



From the VPC sidebar, select **Subnets**.

4.3.2 Create first private subnet

<div><h3>Create subnet <small>Info</small></h3><div>VPC<div>VPC ID Create subnets in this VPC. vpc-03389964 (AWS) ▼</div><div>Associated VPC CIDRs IPv4 CIDRs 10.0.0.0/16</div></div><div>Subnet settings <small>Specify the CIDR blocks and Availability Zone for the subnet.</small><div>Subnet 1 of 2<div>Subnet name <small>Create a tag with a key of 'Name' and a value that you specify.</small> private-usw2a <small>The name can be up to 256 characters long.</small></div><div>Availability Zone <small>Info</small> <small>Choose the zone in which your subnet will reside, or let Amazon choose one for you.</small> US West (Oregon) / us-west-2a ▼</div><div>IPv4 CIDR block <small>Info</small> 10.250.0.0/24 ✕</div><div>▼ Tags - optional Key Name ✕ Value - optional private-usw2a ✕ Remove Add new tag <small>You can add 49 more tags.</small> Remove</div></div></div></div>	<p>Click the Create subnet button.</p> <p>Configure the subnet as follows:</p> <ul style="list-style-type: none">• VPC: Select the virtual network that you created previously.• Subnet name: Provide a unique subnet name. Example: <i>private-usw1a</i>• Availability Zone: In our design we want to use two distinct zones, so use your first chosen zone here. Example: <i>us-west-1a</i>• IPv4 CIDR block: Choose an unused IP block within your VPC address space. Example: <i>10.250.0.0/26</i> <p>Click the Create button.</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4.3.3 Create second private subnet

<div><h3>Subnet 2 of 2</h3><div>Subnet name <small>Create a tag with a key of 'Name' and a value that you specify.</small> private-usw1b <small>The name can be up to 256 characters long.</small></div><div>Availability Zone <small>Info</small> <small>Choose the zone in which your subnet will reside, or let Amazon choose one for you.</small> US West (Oregon) / us-west-2b ▼</div><div>IPv4 CIDR block <small>Info</small> 10.250.0.0/24 ✕</div><div>▼ Tags - optional Key Name ✕ Value - optional private-usw1b ✕ Remove Add new tag <small>You can add 49 more tags.</small> Remove Add new subnet</div></div>

4.3.4 Create first public subnet

<div><h3>Create subnet Info</h3><div><h4>VPC</h4><p>VPC ID Create subnets in this VPC.</p><p>vpc-03389964 (AWS) ▼</p><p>Associated VPC CIDRs</p><p>IPv4 CIDRs</p><p>10.0.0.0/16</p></div><div><h4>Subnet settings</h4><p>Specify the CIDR blocks and Availability Zone for the subnet.</p><div><h5>Subnet 1 of 2</h5><p>Subnet name Create a tag with a key of 'Name' and a value that you specify.</p><p>public-usw2a</p><p>The name can be up to 256 characters long.</p><p>Availability Zone Info Choose the zone in which your subnet will reside, or let Amazon choose one for you.</p><p>US West (Oregon) / us-west-2a ▼</p><p>IPv4 CIDR block Info</p><p>10.250.0.128/26 ✕</p><p>▼ Tags - optional</p><table><tr><td>Key</td><td>Value - optional</td><td></td></tr><tr><td>Q Name ✕</td><td>Q public-usw2a ✕</td><td>Remove</td></tr></table><p>Add new tag</p><p>You can add 49 more tags.</p><p>Remove</p></div></div></div>	Key	Value - optional		Q Name ✕	Q public-usw2a ✕	Remove	<p>Click the Create subnet button.</p> <p>Configure the subnet as follows:</p> <ul style="list-style-type: none">• VPC: Select the virtual network that you created previously.• Subnet name: Provide a unique subnet name. Example: <i>private-usw1a</i>• Availability Zone: In our design we want to use two distinct zones, so use your first chosen zone here. Example: <i>us-west-1a</i>• IPv4 CIDR block: Choose an unused IP block within your VPC address space. Example: <i>10.250.0.128/26</i> <p>Click the Create button.</p>
Key	Value - optional						
Q Name ✕	Q public-usw2a ✕	Remove					

4.3.5 Create second public subnet

<div><h3>Subnet 2 of 2</h3><p>Subnet name Create a tag with a key of 'Name' and a value that you specify.</p><p>public-usw1b</p><p>The name can be up to 256 characters long.</p><p>Availability Zone Info Choose the zone in which your subnet will reside, or let Amazon choose one for you.</p><p>US West (Oregon) / us-west-2b ▼</p><p>IPv4 CIDR block Info</p><p>10.250.0.196/26 ✕</p><p>▼ Tags - optional</p><table><tr><td>Key</td><td>Value - optional</td><td></td></tr><tr><td>Q Name ✕</td><td>Q public-usw1b ✕</td><td>Remove</td></tr></table><p>Add new tag</p><p>You can add 49 more tags.</p><p>Remove</p><p>Add new subnet</p></div>	Key	Value - optional		Q Name ✕	Q public-usw1b ✕	Remove	<p>Click the Create subnet button.</p> <p>Configure the subnet as follows:</p> <ul style="list-style-type: none">• Subnet name: Provide a unique subnet name. Example: <i>private-usw1a</i>• Availability Zone: In our design we want to use two distinct zones, so use your second chosen zone here. Example: <i>us-west-1b</i>• IPv4 CIDR block: Choose an unused IP block within your VPC address space. Example: <i>10.250.0.196/26</i> <p>Click the Create button</p>
Key	Value - optional						
Q Name ✕	Q public-usw1b ✕	Remove					

4.3.6 Review your subnets

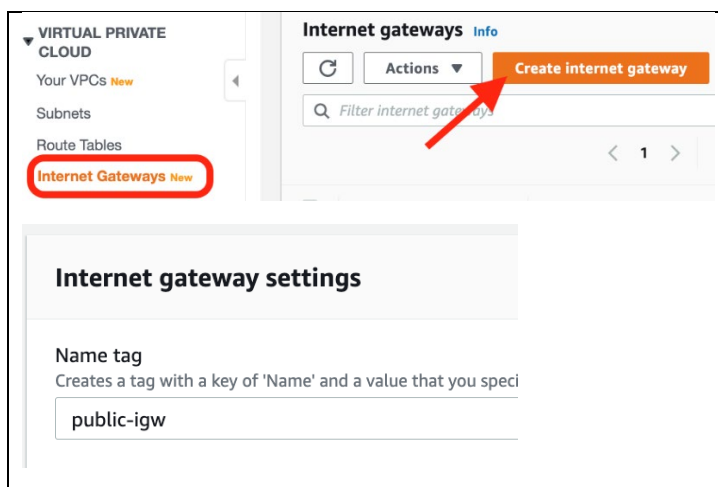
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	private-usw1a	subnet-0850a...	available	vpc-0550...	10.250.0.0/26
<input type="checkbox"/>	private-usw1b	subnet-016e1...	available	vpc-0550...	10.250.0.64/26
<input type="checkbox"/>	public-usw1a	subnet-07aff7...	available	vpc-0550...	10.250.0.128/...
<input type="checkbox"/>	public-usw1b	subnet-0110cd...	available	vpc-0550...	10.250.0.192/...

Review your subnet list. You should now have four subnets created.

4.4 Create an Internet Gateway for the public subnets

To route traffic from the public subnets to the Internet, we need to deploy an Internet Gateway and attach it to the VPC. We will configure routing for it in a later section.

4.4.1 Create Internet Gateways



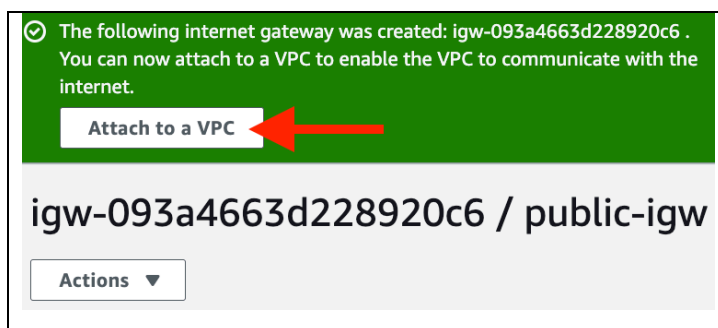
From the VPC sidebar, select Internet Gateways.

Click **Create Internet gateway**.

Enter a name tag. Example: *public-igw*

Click the **Create Internet gateway** button at the bottom of the screen to finish.

4.4.2 Attach Internet Gateway to the VPC



When the Internet Gateway has been created, you will be prompted to attach it to a VPC. Click the button as indicated. You can also do this from the Actions menu.

4.4.3 Enter attachment details

Attach to VPC (igw-05adc82a6f3c7c0e0) [Info](#)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

[▶ AWS Command Line Interface command](#)

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

Select the VPC that you previously created.

Click the **Attach internet gateway** button.

4.5 Create NAT Gateways for the private subnets

A NAT Gateway is a zonal resource that can be used by resources in that zone as an egress point for outbound internet traffic. The NAT Gateway will perform address translation and forward the traffic to the Internet Gateway in your VPC. We will create one for each of our two availability zones so that we do not lose connectivity if one of the zones goes down.

4.5.1 Navigate to NAT Gateways

VIRTUAL PRIVATE CLOUD

- Your VPCs [New](#)
- Subnets
- Route Tables
- Internet Gateways [New](#)
- Egress Only Internet Gateways [New](#)
- DHCP Options Sets [New](#)
- Elastic IPs [New](#)
- Managed Prefix Lists [New](#)
- Endpoints
- Endpoint Services
- NAT Gateways [New](#)**
- Peering Connections

NAT gateways [Info](#)

[Refresh](#) [Actions](#) [Create NAT gateway](#)

[<](#) [1](#) [>](#) [Settings](#)

Name	NAT gateway ID
------	----------------

From the VPC sidebar, select **NAT Gateways**.

4.5.2 Create first NAT Gateway

Create NAT gateway [Info](#)

Create a NAT gateway and assign it an Elastic IP address.

NAT gateway settings

Name - *optional*

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

The name can be up to 256 characters long.

Subnet

Select a public subnet in which to create the NAT gateway.

Elastic IP allocation ID [Info](#)

Assign an Elastic IP address to the NAT gateway.

Click the **Create NAT gateway** button.

Configure the NAT gateway settings as follows:

- **Name** (optional): Enter a unique name for the gateway
Example: *usw1a-nat-gw*
- **Subnet**: Choose the first public subnet
Example: *public-usw1a*
- **Elastic IP allocation ID**: Click the Allocate Elastic IP button to auto-fill this field.

Click the **Create NAT gateway** button to finish.

4.5.3 Create second NAT Gateway

Create NAT gateway Info

Create a NAT gateway and assign it an Elastic IP address.

NAT gateway settings

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

The name can be up to 256 characters long.

Subnet
Select a public subnet in which to create the NAT gateway.

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.

Allocate Elastic IP

Click the **Create NAT gateway** button.

Configure the NAT gateway settings as follows:

- **Name (optional):** Enter a unique name for the gateway
Example: *usw1b-nat-gw*
- **Subnet:** Choose the second public subnet
Example: *public-usw1b*
- **Elastic IP allocation ID:** Click the Allocate Elastic IP button to auto-fill this field.

Click the **Create NAT gateway** button to finish.

4.6 Create and Configure Route Tables

A Route Table is a set of rules, called routes, that are used to determine where network traffic is directed. The VPC already includes a default route table which is used for any subnets that are not explicitly associated with a route table. We will ignore this and instead create three new route tables, one of them associated with our public subnets, and two of them for our private subnets. We will add default routes to the NAT Gateways and the Internet Gateway.

4.6.1 Navigate to Route Tables

New VPC Experience
Tell us what you think

VPC Dashboard
EC2 Global View New

Filter by VPC:

VIRTUAL PRIVATE CLOUD

Your VPCs
Subnets
Route Tables

Route tables (11) Info

< 1 > ⚙

Select a route table

4.6.2 Create route table for public subnets

<div><h3>Create route table <small>Info</small></h3><p>A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.</p><div><h4>Route table settings</h4><p>Name - optional Create a tag with a key of 'Name' and a value that you specify.</p><input type="text" value="public-usw-routes"/><p>VPC The VPC to use for this route table.</p><input type="text" value="vpc-03389964 (AWS)"/></div></div>	<p>Click the Create route table button.</p> <p>Configure the route table as follows:</p> <ul style="list-style-type: none">• Name - optional: Enter a unique name for the route table Example: <i>public-usw-routes</i>• VPC: Select the virtual network that you created previously. <p>Click the Close button.</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4.6.3 Create route table for first private subnet

<div><h3>Route table settings</h3><p>Name - optional Create a tag with a key of 'Name' and a value that you specify.</p><input type="text" value="private-usw1a-routes"/><p>VPC The VPC to use for this route table.</p><input type="text" value="vpc-03389964 (AWS)"/></div>	<p>Click the Create route table button.</p> <p>Configure the route table as follows:</p> <ul style="list-style-type: none">• Name - optional: Enter a unique name for the route table Example: <i>private-usw1a-routes</i>• VPC: Select the virtual network that you created previously. <p>Click the Create button.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4.6.4 Create route table for second private subnet

<div><h3>Route table settings</h3><p>Name - optional Create a tag with a key of 'Name' and a value that you specify.</p><input type="text" value="private-usw1b-routes"/><p>VPC The VPC to use for this route table.</p><input type="text" value="vpc-03389964 (AWS)"/></div>	<p>Click the Create route table button.</p> <p>Configure the route table as follows:</p> <ul style="list-style-type: none">• Name - optional: Enter a unique name for the route table Example: <i>private-usw1b-routes</i>• VPC: Select the virtual network that you created previously. <p>Click the Create button.</p>	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

4.6.5 Review the route table list

<input type="checkbox"/>	Name	Route Table ID
<input type="checkbox"/>		rtb-01705bd4b29e283ee
<input checked="" type="checkbox"/>	private-usw1a-routes	rtb-034336669e17ced15
<input type="checkbox"/>	private-usw1b-routes	rtb-02a96e86856fc5cc0
<input type="checkbox"/>	public-usw-routes	rtb-055fb6f346f460d0a

Verify that your list of route tables has three new entries with the name tags that you chose for them.

4.6.6 Edit routes for the first private subnet route table

<input type="checkbox"/>	Name	Route Table ID
<input type="checkbox"/>		rtb-01705bd4b29e283ee
<input checked="" type="checkbox"/>	private-usw1a-routes	rtb-034336669e17ced15
<input type="checkbox"/>	private-usw1b-routes	rtb-02a96e86856fc5cc0
<input type="checkbox"/>	public-usw-routes	rtb-055fb6f346f460d0a

Route Table: rtb-034336669e17ced15

Summary **Routes** Subnet Associations

Edit routes

View All routes

Destination	Target
10.250.0.0/24	local

Edit routes

Destination	Target	Status
10.250.0.0/24	local	active
0.0.0.0/0	nat-002ed77f6a9ef0841	

Add route

nat-002ed77f6a9ef0841 usw1a-nat-gw

* Required Cancel Save routes

Select the route table for the first private subnet.
Example: *private-usw1a-routes*

Select the **Routes** tab underneath the listing.

Click the **Edit routes** button.

Click the **Add route** button and set these values:

- **Destination:** *0.0.0.0/0*
- **Target:** Select the NAT Gateway that you deployed to the first availability zone.
Example: *usw1a-nat-gw*

Click the **Save routes** button.

Click the **Close** button.

4.6.7 Edit subnet associations for the first private subnet route table

Route Table: rtb-034336669e17ced15

Summary Routes **Subnet Associations**

Edit subnet associations

None found

Subnet ID	IPv4 CIDR
You do not have any subnet associations.	

Edit subnet associations

Route table rtb-034336669e17ced15 (private-usw1a-routes)

Associated subnets subnet-0850a0c96d7a404da

Subnet ID	IPv4 CIDR
<input checked="" type="checkbox"/> subnet-0850a0c96d7a404da private-usw1a	10.250.0.0/26
<input type="checkbox"/> subnet-016e150f99130ef50 private-usw1b	10.250.0.64/26
<input type="checkbox"/> subnet-0110cd4da4ec72e62 public-usw1b	10.250.0.192/...
<input type="checkbox"/> subnet-07aff7a001005ed34 public-usw1a	10.250.0.128/...

* Required Cancel Save

Select the **Subnet Associations** tab.

Click the **Edit subnet associations** button.

Select the first private subnet to associate this route table with. If you followed the example names in this guide, then it will be easy to match the name of the route table with the subnet.

Click the **Save** button.

4.6.8 Edit routes for the second private subnet route table

Summary **Routes** Subnet Associations

Edit routes

View All routes

Destination	Target
10.250.0.0/24	local

Select the route table for the second private subnet.
Example: *private-usw1b-routes*

Select the **Routes** tab underneath the listing.

Click the **Edit routes** button.

Click the **Add route** button and set these values:

- Destination:** 0.0.0.0/0
- Target:** Select the NAT Gateway that you deployed to the second availability zone.
Example: *usw1b-nat-gw*

Click the **Save routes** button.

Click the **Close** button.

Edit routes

Destination	Target	Status
10.250.0.0/24	local	active
0.0.0.0/0	nat-06c46b8e4e4ed5c32	

Add route

nat-06c46b8e4e4ed5c32
usw1b-nat-gw

* Required

Cancel
Save routes

4.6.9 Edit subnet associations for the second private subnet route table

Summary

Routes

Subnet Associations

Edit subnet associations

None found

Subnet ID	IPv4 CIDR
You do not have any subnet associations.	

Edit subnet associations

Route table

rtb-02a96e86856fc5cc0

private-usw1b

routes

Associated subnets

subnet-016e150f99130ef50

Filter by attributes or search by keyword

Subnet ID	IPv4 CIDR
subnet-0850a0c96d7a404da private-usw1a	10.250.0.0/26
subnet-016e150f99130ef50 private-usw1b	10.250.0.64/26
subnet-0110cd4da4ec72e62 public-usw1b	10.250.0.192/...
subnet-07aff7a001005ed34 public-usw1a	10.250.0.128/...

Select the **Subnet Associations** tab.

Click the **Edit subnet associations** button.

Select the first second subnet to associate this route table with. If you followed the example names in this guide, then it will be easy to match the name of the route table with the subnet.

Click the **Save** button.

4.6.10 Edit routes for the public subnet route table

Summary

Routes

Subnet Associations

Edit routes

View

All routes

Destination

Target

10.250.0.0/24

local

Edit routes

Destination	Target	Status
10.250.0.0/24	local	active
0.0.0.0/0	igw-093a4663d228920c6	

Add route

igw-093a4663d228920c6

public-igw

* Required

Cancel

Save routes

Select the route table for the public subnets.
Example: *public-usw-routes*

Select the **Routes** tab underneath the listing.

Click the **Edit routes** button.

Click the **Add route** button and set these values:

- **Destination:** 0.0.0.0/0
- **Target:** Select the Internet Gateway that you deployed.
Example: *public-igw*

Click the **Save routes** button.

Click the **Close** button.

4.6.11 Edit subnet associations for the public subnet route table

Summary

Routes

Subnet Associations

Edit subnet associations

< < None found

Subnet ID

IPv4 CIDR

You do not have any subnet associations.

Route table

rtb-055fb6f346f460d0a (public-usw-routes)

Associated subnets

subnet-07aff7a001005ed34

subnet-0110cd4da4ec72e62

Filter by attributes or search by keyword

Subnet ID	IPv4 CIDR
subnet-0850a0c96d7a404da private-usw1a	10.250.0.0/26
subnet-016e150f99130ef50 private-usw1b	10.250.0.64/26
subnet-0110cd4da4ec72e62 public-usw1b	10.250.0.192/...
subnet-07aff7a001005ed34 public-usw1a	10.250.0.128/...

Select the **Subnet Associations** tab.

Click the **Edit subnet associations** button.

Select the both public subnets to associate this route table with.

Click the **Save** button.

4.7 Security Groups

A security group acts as a virtual firewall for your virtual machine instances to control incoming and outgoing traffic. When we create a VM later, we will be able to attach one or more security groups to it at that time. You can modify the rules for a security group at any time. New and modified rules are automatically applied to all instances that are associated with the security group.

When you create the security group rules, you will specify the source and destination. These can be expressed either as a list of IP networks, or as a security group ID. When you specify a security group as the source or destination for a rule, the rule affects all instances that are associated with the security group. We will use this feature for distributed server deployments to allow traffic between Intel EMA VMs without having to be overly broad and permitting all traffic within the private network, which follows the least-privilege security best practice.

In the procedures below, we will create a security group to control access to Intel EMA VMs and a separate group to control access to the database.

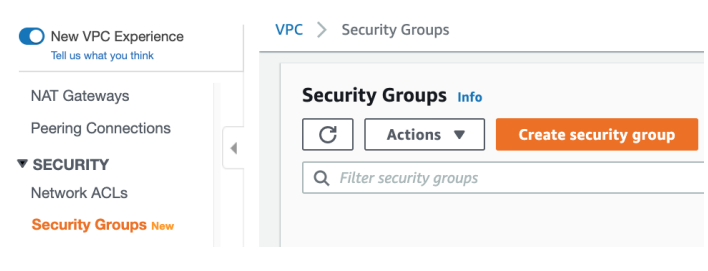
For more information about VPC Security Groups, visit the following link:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

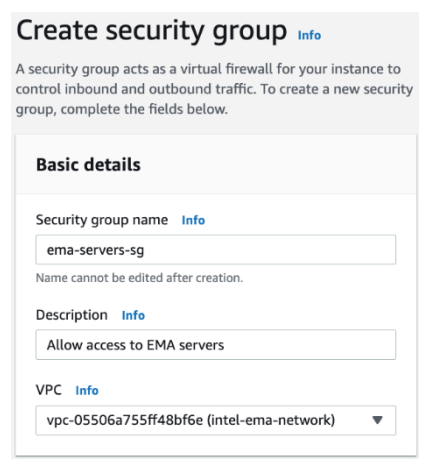
4.7.1 Create a Security Group for the VM(s)

Note: Some source addresses in the example images below are redacted because they would be specific to your own network environment and should not be copied verbatim. You should use your own trusted network(s) instead.

4.7.1.1 Create a Security Group

	<p>From the VPC section sidebar, select Security Groups.</p> <p>Click the Create security group button.</p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------

4.7.1.2 Configure Security Group Basic Details

	<p>Enter basic details for the security group that will allow access to the EMA server.</p> <ul style="list-style-type: none">• Security group name: Enter a unique name Example: <i>ema-server-sg</i>• Description (optional): Enter a description for the security group Example: <i>Allow access to EMA servers</i>• VPC: Select the VPC that you previously created.
------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4.7.1.3 Add an Inbound Rule for Web Traffic

Inbound rules [Info](#)

Inbound rule 1 [Delete](#)

Type [Info](#): HTTPS
Protocol [Info](#): TCP
Port range [Info](#): 443
Source type [Info](#): Custom
Source [Info](#): 10.250.0.0/24, [redacted]/32
Description - optional [Info](#): trusted networks for web
[Add rule](#)

Add an Inbound rule with the following settings.

- **Type:** *HTTPS*
- **Description:** *Trusted network(s) for web*
- **Source:** Enter the VPC CIDR block to allow health checks.
Example: *10.250.0.0/24*
You may also enter additional network(s) that should be allowed to access the EMA web UI, such as the public network that traffic from your service desk would originate from.

4.7.1.4 Add an Inbound Rule for Websocket Traffic

Inbound rule 2 [Delete](#)

Type [Info](#): Custom TCP
Protocol [Info](#): TCP
Port range [Info](#): 8084
Source type [Info](#): Custom
Source [Info](#): 10.250.0.0/24, [redacted]/32
Description - optional [Info](#): trusted networks for websocket
[Add rule](#)

Add an Inbound rule with the following settings.

- **Type:** *Custom TCP*
- **Port range:** *8084*
- **Description:** *Trusted network(s) for websocket*
- **Source:** Enter the VPC CIDR block to allow health checks.
Example: *10.250.0.0/24*
You may also enter additional network(s) that should be allowed to access the EMA web UI, such as the public network that traffic from your service desk would originate from.

4.7.1.5 Add an Inbound Rule for Swarm Traffic

Type [Info](#): Custom TCP
Protocol [Info](#): TCP
Port range [Info](#): 8080
Source type [Info](#): Custom
Source [Info](#): 0.0.0.0/0
Description - optional [Info](#): EMA agent traffic
[Add rule](#)

Add an Inbound rule with the following settings.

- **Type:** *Custom TCP*
- **Port range:** *8080*
- **Description:** *EMA agent traffic*
- **Source:** *0.0.0.0/0*

4.7.1.6 Create and Review

Details

Security group name

ema-servers-sg

Security group ID

sg-06acbdce6cea22f15

Description

Allow access to EMA servers

VPC ID

vpc-001161d1e7e50afb2

Owner

312506926764

Inbound rules count

4 Permission entries

Outbound rules count

1 Permission entry

Inbound rules

Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	8084	/32	Trusted network(s) for websocket
Custom TCP	TCP	8080	0.0.0.0/0	EMA agent traffic
RDP	TCP	3389	/32	Trusted network(s) for RDP
HTTPS	TCP	443	/32	Trusted network(s) for web

Click the **Create security group** button to save the rules.

Review the rule list for correctness.

Note: We have left Outbound rules with the default rule that allows all outbound traffic.

4.7.2 Update Security Group to Allow Traffic Between Intel EMA VMs (Distributed Server Only)

Now that we have created the ema-server-sg Security Group, click the **Edit inbound rules** button, and make the changes that follow below.

4.7.2.1 Add an Inbound Rule for Internal Traffic for Ports 8092-8094

Type **Info**

Custom TCP

Source type **Info**

Custom

Protocol **Info**

TCP

Source **Info**

sg-06acbdce6cea22f15

Port range **Info**

8092 - 8094

Description - optional **Info**

EMA internal

Add an Inbound rule with the following settings.

- **Type:** *Custom TCP*
- **Port range:** *8092-8094*
- **Description:** *EMA internal*
- **Source:** Click the empty text box and select the name of the security group that you created in the previous step.

4.7.2.2 Add an Inbound Rule for Internal Traffic for Port 8089

Type [Info](#)

Custom TCP ▼

Source type [Info](#)

Custom ▼

Protocol [Info](#)

TCP

Source [Info](#)

sg-06acbdce6cea22f15 ✕

Port range [Info](#)

8089

Description - optional [Info](#)

EMA admin port

Add an Inbound rule with the following settings.

- **Type:** *Custom TCP*
- **Port range:** *8089*
- **Description:** *EMA admin port*
- **Source:** Click the empty text box and select the name of the security group that you created in the previous step.

4.7.2.3 Save and Review the Final List for Correctness

Click the **Save rules** button. Review the rules for correctness.

Inbound rules					Edit inbound rules
Type	Protocol	Port range	Source	Description - optional	
Custom TCP	TCP	8084	10.250.0.0/24	trusted networks for websocket	
Custom TCP	TCP	8084	██████████/32	trusted networks for websocket	
Custom TCP	TCP	8080	0.0.0.0/0	EMA agent traffic	
Custom TCP	TCP	8089	sg-08d3222f040f45bdd (ema-servers-sg)	EMA admin port	
Custom TCP	TCP	8092 - 8094	sg-08d3222f040f45bdd (ema-servers-sg)	EMA internal	
HTTPS	TCP	443	10.250.0.0/24	trusted networks for web	
HTTPS	TCP	443	██████████/32	trusted networks for web	

4.7.3 Create a Security Group for the Database

4.7.3.1 Create a Security Group

New VPC Experience
Tell us what you think

NAT Gateways

Peering Connections

▼ SECURITY

Network ACLs

Security Groups **New**

VPC > Security Groups

Security Groups [Info](#)

From the **VPC** section sidebar, select **Security Groups**.

Click the **Create security group** button.

4.7.3.2 Configure Security Group Basic Details

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](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Enter basic details for the security group that will allow access to the EMA server.

- **Security group name:** Enter a unique name
Example: *ema-db-sg*
- **Description** (optional): Enter a description for the security group
Example: *Allow traffic from EMA server(s) to the database*
- **VPC:** Select the VPC that you previously created.

4.7.3.3 Add Inbound Rule for MSSQL

Inbound rules [Info](#)

Inbound rule 1

Type [Info](#)

Source type [Info](#)

Security Groups

ema-server-sg | sg-03661abff0a38ee50

Add an Inbound rule with the following settings.

- **Type:** *MSSQL*
- **Source:** Click the empty text box and select the security group for the EMA servers that you created previously.

4.7.3.4 Create and Review

Click the **Create security group** button. Review the rule list for correctness.

Inbound rules				Edit
Type	Protocol	Port range	Source	
MSSQL	TCP	1433	sg-08d3222f040f45bdd (ema-servers-sg)	

5 Virtual Machine Deployment

5.1 Overview

Amazon Elastic Compute Cloud (Amazon EC2) gives you the flexibility of compute virtualization without having to buy and maintain the physical hardware that runs it. However, you are still responsible for maintaining the guest operating system and the software that runs on it.

You will decide the amount of CPU, Memory, and Storage to allocate to the EC2 instance at the time of creation, but you can increase all of these at a later time or shrink the amount of CPU and Memory in order to optimize the VM for the workload to reduce costs.

EC2 secures logins for your instances using EC2 key pairs (AWS stores the public key, and you store the private key in a secure place). This can be created in advance or at the time of EC2 instance creation. You will need the private key in order to retrieve the automatically generated Administrator credentials for a Windows-based instance. You can have multiple key pairs in EC2, but you can only associate an instance with one and you cannot change this after the instance has been created.

Network access to your EC2 instances can be secured by attaching one or more Security Groups either when the instance is created or any time afterward. The Security Groups that we need were already configured in a previous section.

For distributed server deployments, there are additional steps included in the procedure below and in further sections which you can skip for single-server deployments. These include creating a second VM, associating the VMs with a Target Group, attaching the Target Group to the Load Balancer, and configuring the load balancer forwarding rules.

For more information about EC2 instances or key pairs, visit the following links:


<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html>

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-key-pairs.html>

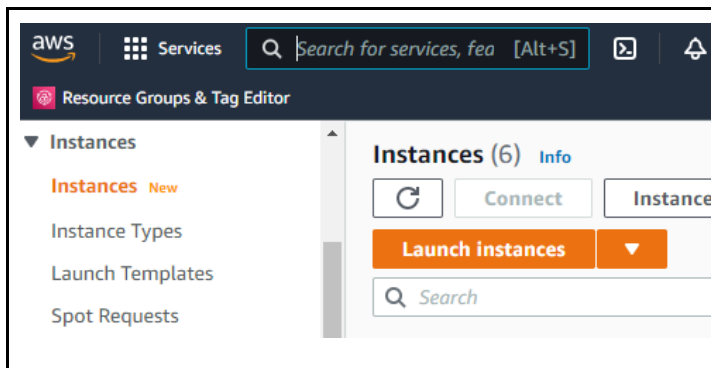
5.2 Create Virtual Machine(s)

Follow the procedure below to create an EC2 instance for the Intel EMA server using the latest Windows Server image and attach the security group that we previously created.

5.2.1 Navigate to the EC2 Service

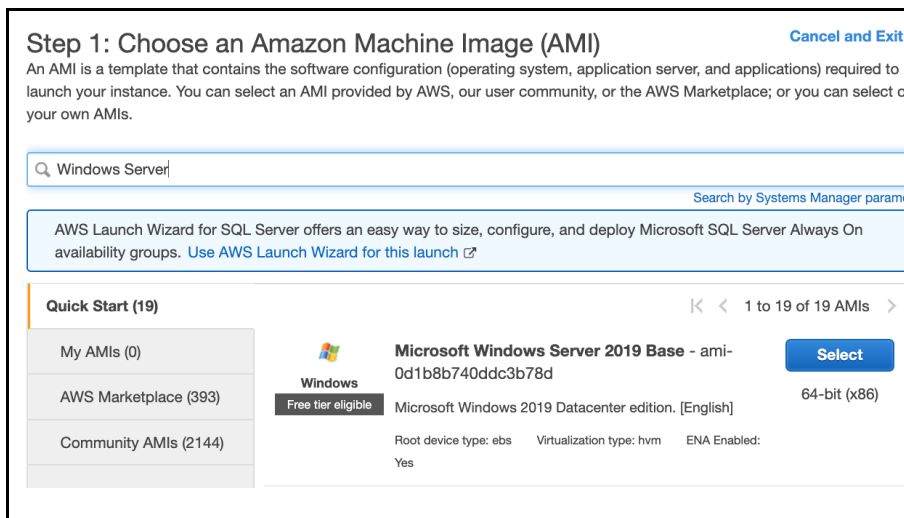
	From the Services menu, under the Compute section, select EC2
-------------------------------------------------------------------------------------	------------------------------------------------------------------------------------

5.2.2 Launch an EC2 Instance



Select **Instances** on the sidebar and click the **Launch Instance** button.

5.2.3 Choose an Amazon Machine Image

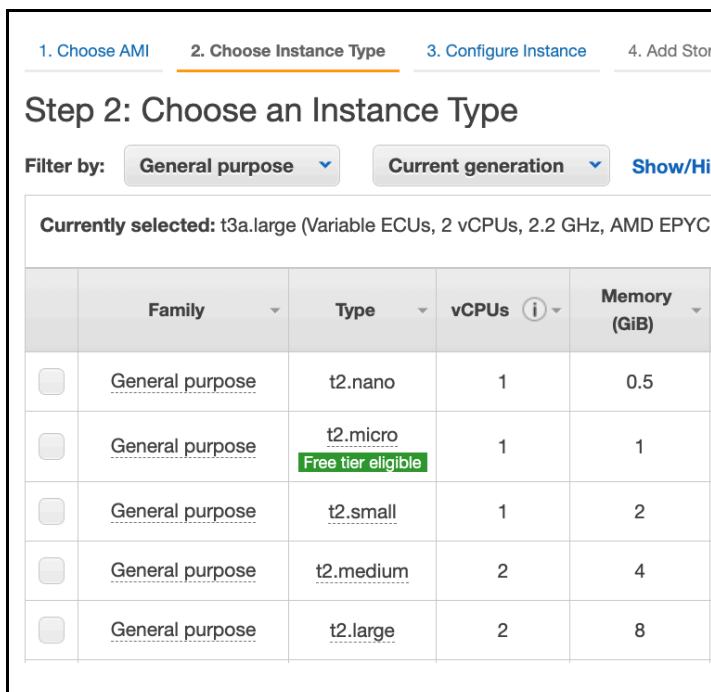


Search for the latest Microsoft Windows Server Base image supported by Intel EMA.

See the Intel® Endpoint Management Assistant Server Installation Guide for a list supported operating systems.

Click the **Select** button.

5.2.4 Select the Machine Type



Choose the machine type with the amount of CPU and Memory resources that you need. You can change this later when the instance is powered down, if needed.

See the Intel® Endpoint Management Assistant Server Installation Guide for system requirements.

Click the **Next: Configure Instance Details** button.

5.2.5 Configure Instance Details

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Cc

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or [create a new default VPC](#).

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, req the lower pricing, assign an access management role to the instance, and more.

Number of instances ⓘ1Launch into Auto Scal

Purchasing option ⓘ☐ Request Spot instances

Network ⓘvpc-05506a755ff48bf6e | intel-ema-network
No default VPC found. [Create a new default VPC](#).

Subnet ⓘsubnet-0850a0c96d7a404da | private-usw1a | us-we
59 IP Addresses available

Auto-assign Public IP ⓘDisable

Configure the instance details as follows:

- **Network:** Set to the VPC that you created previously.
Example: *intel-ema-network*
- **Subnet:** Choose one of the private subnets.
Example: *private-usw1a*
- **Auto-assign Public IP:** *Disable*

The rest of the instance details on this screen can be left at default.

Click the **Next: Add Storage** button.

5.2.6 Add Storage

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption
Root	/dev/sda1	snap-0cc417e3e52bda57e	30	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypte

Storage settings can be left at default unless you need more space. Refer to the Intel® Endpoint Management Assistant Server Installation Guide for system requirements.

Click the **Next: Add Tags** button.

5.2.7 Add Tags

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ
Name	ema-server-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add a tag with the key “Name” and a value of the server name that you want.

Add any additional custom tags that you may want to help organize your resources, as previously discussed in the Tags and Resource Groups section of the Introduction.

Click the **Next: Configure Security Group** button.

5.2.8 Configure Security Group

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below.

Assign a security group: ☐ Create a new security group
☒ Select an existing security group

Security Group ID	Name	Description
<input type="checkbox"/> sg-04c1e0cf58c3b592e	default	default VPC security group
<input type="checkbox"/> sg-017cfe786b8c9004a	ema-db-sg	Allow traffic from EMA server(s) to the database
<input checked="" type="checkbox"/> sg-06acbdce6cea22f15	ema-servers-sg	Allow access to EMA servers

Set the **Assign a security group** radio button to *Select an existing security group*.

Select the Security Group that you previously created for Intel EMA servers. Example: *ema-servers-sg*.

Click the **Next: Review and Launch** button.

You may receive a warning that you will not be able to connect to the instance since the security group doesn't have port 3389 (RDP) open. You can ignore that message and continue since we have another way to access the virtual machine.

5.2.9 Review Instance Launch

Review the instance details and then click the **Launch** button.

5.2.10 Select an EC2 Key Pair

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

ema-demo

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

You will be prompted to select an existing key pair or create a new key pair.

Choose the appropriate key pair from the list, or else use the option to create a new key pair and click the **Download Key Pair** button to save the private key file to your computer.

If you chose to use an existing key pair then you must have access to the private key file.

Click the **Launch Instances** button.

5.3 Create a Second EC2 Instance (Distributed Server Only)

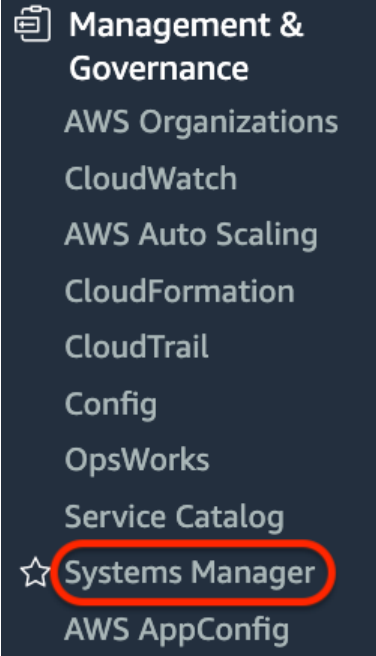
For distributed server deployments, repeat the previous procedure to create the second Intel EMA server, selecting a different subnet and giving it a different Name tag, such as *ema-server-2*.

6 Configure AWS Systems Manager (Distributed Server Only)

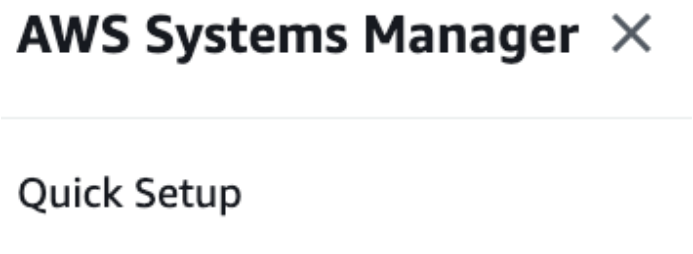
AWS Systems Manager is a service that gives you greater visibility and control of your infrastructure on AWS. We need to enable this to use the Session Manager component that will let us have remote access to our VMs which do not have a public IP address.

For further reading about Systems Manager, visit the following link: <https://aws.amazon.com/systems-manager/>

6.1 Navigate to Systems Manager service

 <p>Management & Governance</p> <ul style="list-style-type: none">AWS OrganizationsCloudWatchAWS Auto ScalingCloudFormationCloudTrailConfigOpsWorksService Catalog★ Systems ManagerAWS AppConfig	<p>From the Services menu, under the Management & Governance section, select Systems Manager.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------

6.2 Start Quick Setup

 <p>AWS Systems Manager X</p> <p>Quick Setup</p>	
-------------------------------------------------------------------------------------------------------------------------------------	--

6.3 Choose Permissions options

<div><h3>Quick Setup <small>Info</small></h3><p>Configure required security roles and commonly used Systems Manager capabilities.</p><div><h4>Permissions (Required)</h4><p>Use the following options to configure two roles that give Systems Manager permission to access your instances and run commands on them.</p></div><div><div><h4>Instance profile role</h4><div><div><h5>Use the default role <input checked="" type="radio"/></h5><p>Quick Setup creates a new instance profile that uses a secure IAM permissions policy. Quick Setup assigns the profile to the instances that you specify.</p></div><div><h5>Choose an existing role <input type="radio"/></h5><p>Uses an existing instance profile. The instance profile must contain the required permissions policy. Choose the instance profile from the following list.</p></div></div><div><h4>Assume role for Systems Manager</h4><div><div><h5>Use the default role <input checked="" type="radio"/></h5><p>Quick Setup creates a new assume role that enables Systems Manager to securely run commands on your instances.</p></div><div><h5>Choose an existing role <input type="radio"/></h5><p>Uses an existing service role. The role must contain the required permissions policy. Choose the role from the following list</p></div></div></div></div></div></div>	
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

6.4 Choose Configurations options

<div><h3>Configuration options</h3><p>Quick Setup configures the following Systems Manager components based on best practices. Select the check boxes for actions you want to schedule. Learn more</p><ul style="list-style-type: none"><input checked="" type="checkbox"/> Update Systems Manager (SSM) Agent every two weeks<input checked="" type="checkbox"/> Collect inventory from your instances every 30 minutes<input checked="" type="checkbox"/> Scan instances for missing patches daily<input type="checkbox"/> Install and configure the CloudWatch agent<input type="checkbox"/> Update the CloudWatch agent once every 30 days<p>If you run Quick Setup, Systems Manager Explorer is enabled.</p><p>Learn more about the metrics included in the CloudWatch agent's basic configuration and Amazon CloudWatch pricing.</p></div>	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

6.5 Choose Targets

Targets

Targets are the Amazon EC2 instances to manage with Systems Manager.

Target selection method

☒ Choose all instances in the current AWS account and Region

☐ Specify instance tags

☐ Choose instances manually

Cancel **Enable**

6.6 Verify Managed Instances List

AWS Systems Manager > Managed Instances

Managed Instances Settings

Managed instances View details Agent auto update Configure Inventory Actions

Search

Instance ID	Name	Ping status	Platform type	Platform name	Platform version	Agent version	IP address	Computer name	Association status
<input type="radio"/> i-0a6a82fc33afa0cf7	ema-server-2	Online	Windows	Microsoft Windows Server 2019 Datacenter	10.0.17763	3.0.222.0	10.250.0.82	EC2AMAZ-PM4CVE0.WORKGROUP	Pending
<input type="radio"/> i-06364ced48ee5bb96	ema-server-1	Online	Windows	Microsoft Windows Server 2019 Datacenter	10.0.17763	3.0.222.0	10.250.0.16	EC2AMAZ-BBHE25G.WORKGROUP	Success

From the Systems Manager sidebar, select Managed Instances.

It may take several minutes for your virtual machines to show up in this list after you first run the Quick Setup.

When your VMs have successfully registered with System Manager then you will see them listed here.

6.7 Logging into your virtual machines via Session Manager

Using the Session Manager through the AWS console will only let you connect to a Powershell session on the VM. In order to connect with RDP, we need to invoke session manager from a local command line, using the AWS Command Line Interface (CLI), and passing in an option to enable port forwarding.

Installing the AWS CLI is beyond the scope of this document. See: <https://aws.amazon.com/cli/> for further information.

When you have the CLI installed and configure and your VMs are showing up in AWS System Manager, then you can run a CLI command with this syntax:

```
aws ssm start-session --target <instanceId> --document-name AWS-StartPortForwardingSession --parameters "localPortNumber=55678,portNumber=3389"
```

Replace <instanceId> with the ID of the EC2 instance that you want to connect to. Example: i-06364ced48ee5bb96

If this command is successful, then you will be able to use a Remote Desktop client to connect to localhost at the localPortNumber that you specified. You can then log in using the credentials for that VM.

7 Relational Database Service (RDS) Deployment

AWS has a fully managed platform-as-a-service database engine called Amazon Relational Database Service (Amazon RDS), which makes it easy to set up, operate, and scale a relational database in the AWS Cloud. It provides cost-efficient, resizable capacity and manages common database administration tasks including backups, software patching, automatic failure detection, and recovery.

The basic building block of Amazon RDS is the DB instance. A DB instance is an isolated database environment in the AWS Cloud. Your DB instance can contain multiple user-created databases. You can access your DB instance by using the same tools and applications that you use with a standalone database instance. The computation and memory capacity of a DB instance is determined by its DB instance class. You can select the DB instance that best meets your needs. If your needs change over time, you can change DB instances.

Since our VPC was created with multiple subnets in different Availability Zones, we will be able to launch an RDS instance with an option called a Multi-AZ deployment. By choosing this option for our production deployment, your primary DB instance is automatically and synchronously replicated to a secondary standby DB instance in a different Availability Zone. This approach helps provide data redundancy and failover support, eliminate I/O freezes, and minimize latency spikes during system backups. We will create a Database Subnet Group which will inform RDS which Availability Zones to use for this purpose.


A Security Group that we previously created in this guide will be used to control access to the RDS instance and only allow our Intel EMA EC2 instance(s) to connect to it.

For more information about RDS, visit the following link:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

Follow this procedure to create a Relational Database Service (RDS) instance and attach the security group that was previously created to allow traffic in from the Intel EMA EC2 instance(s) to the database.

7.1 Navigate to the RDS Service

	From the Services menu, under Database , select RDS
-------------------------------------------------------------------------------------	--------------------------------------------------------------------------

7.2 Create Database Subnet Group

	From the RDS sidebar, select Subnet groups and then click the Create DB Subnet Group button.
-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------

7.2.1 Subnet Group Details

Create DB Subnet Group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name
You won't be able to modify the name after your subnet group has been created.

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Subnets selected (2)

Availability zone	Subnet ID	CIDR block
us-west-1a	subnet-0850a0c96d7a404da	10.250.0.0/26
us-west-1b	subnet-016e150f99130ef50	10.250.0.64/26

Enter the Subnet group details as follows.

- **Name:** Enter a unique name
Example: *ema-db-subnet-group*
- **Description** (optional)
Example: *Identifies subnets to use with the EMA DB instance*
- **VPC:** Select the VPC that you previously created.
- **Availability Zones:** Select both zones in which you created the subnets.
- **Subnets:** Choose both of the private subnets that were previously created.

Click the **Create** button.

7.3 Create a Database

Amazon RDS

[Dashboard](#)
[Databases](#)
[Query Editor](#)
[Performance Insights](#)

RDS > Databases

Databases







☒ Group resources

From the RDS sidebar, select Databases and then click the **Create database** button.

7.3.1 Choose a Database Creation Method

<div><h4>Create database</h4><div><h5>Choose a database creation method Info</h5><div><div><input checked="" type="radio"/> Standard Create You set all of the configuration options, including ones for availability, security, backups, and maintenance.</div><div><input type="radio"/> Easy Create Use recommended best-practice configurations. Some configuration options can be changed after the database is created.</div></div></div></div>	Select the Standard Create database creation method
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------

7.3.2 Choose Engine Type and Edition

<div><h4>Engine options</h4><div><h5>Engine type Info</h5><div><div><input type="radio"/> Amazon Aurora </div><div><input type="radio"/> MySQL </div><div><input type="radio"/> MariaDB </div><div><input type="radio"/> PostgreSQL </div><div><input type="radio"/> Oracle </div><div><input checked="" type="radio"/> Microsoft SQL Server </div></div><div><h5>Edition</h5><div><input type="radio"/> SQL Server Express Edition Affordable database management system that supports database sizes up to 10 GB.</div><div><input type="radio"/> SQL Server Web Edition In accordance with Microsoft's licensing policies, it can only be used to support public and Internet-accessible webpages, websites, web applications, and web services.</div><div><input checked="" type="radio"/> SQL Server Standard Edition Core data management and business intelligence capabilities for mission-critical applications and mixed workloads.</div><div><input type="radio"/> SQL Server Enterprise Edition Comprehensive high-end capabilities for mission-critical applications with demanding database workloads and business intelligence requirements.</div></div><div><h5>Version Info</h5><div>SQL Server 2017 14.00.3281.6.v1 ▼</div></div><div><h5>License</h5><div>license-included</div></div></div></div>	<p>Select the Microsoft SQL Server engine</p> <p>Select appropriate SQL server edition. For the purposes of this documentation we are assuming a production deployment using the SQL Server Standard Edition. SQL Server Express Edition could be used for development and testing to reduce costs.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.3.3 Choose Deployment Template

<div><h4>Templates</h4><p>Choose a sample template to meet your use case.</p><div><div><input checked="" type="radio"/> Production Use defaults for high availability and fast, consistent performance.</div><div><input type="radio"/> Dev/Test This instance is intended for development use outside of a production environment.</div></div></div>	Under Templates, select Production
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------

7.3.4 Configure Instance Name and Master User Credentials

<div><h4>Settings</h4><p>DB instance identifier Info Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.</p><input type="text" value="ema-db"/><p>The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.</p><p>▼ Credentials Settings</p><p>Master username Info Type a login ID for the master user of your DB instance.</p><input type="text" value="admin"/><p>1 to 16 alphanumeric characters. First character must be a letter</p><p><input type="checkbox"/> Auto generate a password Amazon RDS can generate a password for you, or you can specify your own password</p><p>Master password Info</p><input type="password" value="*****"/><p>Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), "(double quote) and @ (at sign).</p><p>Confirm password Info</p><input type="password" value="*****"/></div>	<p>Give the database a unique name Example: <i>ema-db</i></p> <p>Create a username and password</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------

7.3.5 Configure DB Instance Size

<div><h4>DB instance size</h4><p>DB instance class Info Choose a DB instance class that meets your processing power and is limited to those supported by the engine you selected above.</p><p><input checked="" type="radio"/> Standard classes (includes m classes)</p><p><input type="radio"/> Memory Optimized classes (includes r and x classes)</p><p><input type="radio"/> Burstable classes (includes t classes)</p><div><input type="text" value="db.m5.large"/><p>2 vCPUs 8 GiB RAM EBS: 3500 Mbps</p></div><p><input type="radio"/> Include previous generation classes</p></div>	<p>Set the DB instance class to provide adequate resources. Suggested: <i>db.m5.large</i></p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------

7.3.6 Configure Storage (Optional)

You can increase the default amount of storage that is allocated, if you wish. We will leave the default. You can still increase the storage capacity at a later time.

7.3.7 Configure Connectivity

<div><h3>Connectivity</h3><p>Virtual private cloud (VPC) Info VPC that defines the virtual networking environment for this DB instance.</p><p>AWS (vpc-03389964) ▼</p><p>Only VPCs with a corresponding DB subnet group are listed.</p><div><p>i After a database is created, you can't change its VPC.</p></div></div>	Under Connectivity , select the VPC that you previously created.
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------

7.3.8 Configure Connectivity - Additional Connectivity Configuration

<div><h3>▼ Additional connectivity configuration</h3><p>Subnet group Info DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.</p><p>ema-db-subnet-group ▼</p><p>Publicly accessible Info</p><p><input type="radio"/> Yes Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.</p><p><input checked="" type="radio"/> No RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.</p><p>VPC security group Choose one or more RDS security groups to allow access to your database. Ensure that the security group rules allow incoming traffic from EC2 instances and devices outside your VPC. (Security groups are required for publicly accessible databases.)</p><div><div><input checked="" type="radio"/> Choose existing Choose existing VPC security groups</div><div><input type="radio"/> Create new Create new VPC security group</div></div><p>Existing VPC security groups</p><p>Choose VPC security groups ▼</p><p>ema-db-sg ✕</p><p>Availability Zone Info</p><p>No preference ▼</p><p>Database port Info TCP/IP port that the database will use for application connections.</p><p>1433</p></div>	<p>Choose the Database Subnet Group that you previously created.</p> <p>De-select the default VPC security group and choose the existing security group that you previously created for the database.</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


7.3.9 Review and Create

Estimated monthly costs

DB instance	735.11 USD
Storage	2.76 USD
Provisioned IOPS	110.00 USD
Total	847.87 USD

This billing estimate is based on on-demand usage as described in [Amazon RDS Pricing](#). Estimate does not include costs for backup storage, I/Os (if applicable), or data transfer.

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#).

 You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

Cancel

Create database

Review the estimated cost and then click the **Create database** button.

7.4 Get Database Hostname

Connectivity & security

Monitoring

Connectivity & security

Endpoint & port

Endpoint

ema-db.creq7zxsavq4.us-west-1.rds.amazonaws.com

Port

1433

Once the database has finished deploying, the details page will show the database hostname that you will use to configure the Intel EMA software during the installation process.

8 Load Balancer Deployment (Distributed Server Only)

8.1 Overview

An AWS Network Load Balancer is a Layer-4 (TCP) load balancer that distributes user traffic across multiple instances of your applications. By spreading the load, load balancing reduces the risk that your applications become overburdened, slow, or nonfunctional. After the load balancer receives a connection request, it selects a healthy target from an associated target group according to the forwarding rules and forwards the connection to that target.

A *listener* checks for connection requests from clients, using the protocol and port that you configure, and forwards requests to a target group.

Each *target group* routes requests to one or more registered targets, such as EC2 instances, using the protocol and the port number that you specify. You can configure health checks on a per target group basis. Health checks are performed on all targets registered to a target group that is specified in a listener rule for your load balancer.

We will enable multiple Availability Zones for the load balancers we deploy so that we can route traffic to targets in either zone.

The load balancer will have an automatically generated hostname that will point to the public-facing addresses of the related load balancers in each AZ. You will want to create a DNS CNAME record aliasing that hostname in order to use your custom domain to reach the Intel EMA server(s).

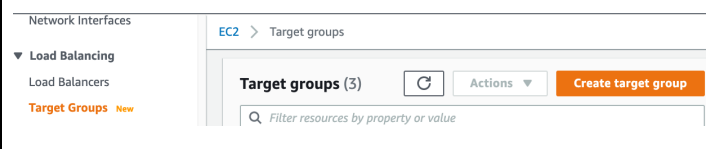
There are further load balancing configuration possibilities not covered in this document. You should consult with your IT department for any requirements or practices they may want to be implemented. For more information about load balancing in AWS, visit the following link:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>

8.2 Create Target Groups

Follow this procedure to create a target group for each TCP port that will be served by our load balancer, create health checks, and register our virtual machines to receive traffic for each target group.

8.2.1 Create Target Groups



The screenshot shows the AWS Management Console interface for EC2 Target Groups. On the left, the 'Network Interfaces' sidebar is expanded, and 'Load Balancing' is selected, with 'Target Groups' highlighted. The main panel shows 'Target groups (3)' with a search bar and a 'Create target group' button.

From the **EC2** sidebar, under **Load Balancing**, select **Target Groups**.

Click the **Create target group** button.

8.2.2 Configure a Target Group for TCP/443

<div><h3>Target group name</h3><div>ema-web</div><p>Up to 32 alphanumeric characters, including</p><p>Protocol : Port</p><div>TCP ▼ : 443</div><p>VPC</p><p>Select the VPC containing the instances you</p><div>intel-ema-network vpc-05506a755ff48bf6e IPv4: 10.250.0.0/24</div><div><h4>Health checks</h4><p>The associated load balanc</p><p>Health check protocol</p><div>TCP ▼</div></div></div>	<p>Configure the target group as follows</p> <ul style="list-style-type: none">• Target type: <i>Instances</i>• Target group name: Enter a unique name Example: <i>ema-web</i>• Protocol: <i>TCP</i>• Port: <i>443</i>• VPC: Select the VPC that you previously created• Health check protocol: <i>TCP</i> <p>Click Next to advance to the Register targets screen.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

8.2.2.1 Register Both EC2 Instances as Targets

Register targets

Step 2 of 2

Select instances, specify ports, and add the instances to the list of pending targets. Repeat to add additional combinations of instances and ports to the list of pending targets. You can skip this step if you prefer to register targets after creating the target group.

Available instances (2)

Filter resources by property or value

<input type="checkbox"/>	Instance ID	Name	State	Security groups	Zone	Subnet ID
<input type="checkbox"/>	i-00f8db1dd6650c6c8	ema-server-1	running	ema-servers-sg	us-west-1a	subnet-080e857
<input type="checkbox"/>	i-0f180ebc233227eda	ema-server-2	running	ema-servers-sg	us-west-1c	subnet-0a16634

0 selected

Ports for the selected instances

Ports for routing traffic to the selected instances (separate multiple ports with commas):

443

Include as pending below

2 selections are now pending below. Include more or register targets when ready.

Targets (2)

Remove all pending

All

Filter resources by property or value

Remove	Status	Instance ID	Name	Port	State	Security groups
<input type="checkbox"/>	Pending	i-00f8db1dd6650c6c8	ema-server-1	443	running	ema-servers-sg
<input type="checkbox"/>	Pending	i-0f180ebc233227eda	ema-server-2	443	running	ema-servers-sg

2 pending

CancelPreviousCreate target group

Select both EMA VM instances and click the **Include as pending below** button

Click the **Create target group** button.

8.2.3 Create/Configure a Target for TCP/8084

Repeat the above steps to another target group named “ema-websocket” for TCP/8084.

8.2.4 Configure a Target for TCP/8080

Repeat the above steps to another target group named “ema-swarm” for TCP/8080.

Intel® EMA Web Deployment Guide for AWS – February 2022

38




8.2.5 Review Target Groups

Target groups (3)

Ac

🔍

Filter resources by property or value

<input type="checkbox"/>	Name ▲	ARN	Port ▼	Protocol
<input type="checkbox"/>	ema-swarm	 arn:aws:elasticload...	8080	TCP
<input type="checkbox"/>	ema-web	 arn:aws:elasticload...	443	TCP
<input type="checkbox"/>	ema-websocket	 arn:aws:elasticload...	8084	TCP

8.2.6 Enable Stickiness for the TCP/443 Target Group

8.2.6.1 Target group details

Attributes

Stickiness
Disabled

Deregistration delay
300 seconds

Slow start duration
0 seconds

Load balancing algorithm
Round robin

Edit

Click the *ema-web* target group name to access the Group details screen.

In the **Attributes** section, click the **Edit** button

8.2.6.2 Edit Attributes

Edit attributes

Attributes

Restore defaults

Deregistration delay

The time to wait for in-flight requests to complete while deregistering a target. During this time, the state of the target is draining.

seconds

0-3600

Slow start duration

During this period, a newly registered target receives an increasing share of requests, until it reaches its fair share.

seconds

Requires 30 to 900 seconds to enable, or 0 seconds to disable. This attribute cannot be combined with the Least outstanding requests algorithm.

Load balancing algorithm

Determines how the load balancer selects targets from this target group when routing requests.

☒ Round robin

☐ Least outstanding requests

Cannot be combined with the Slow start duration attribute.

☒ Stickiness

The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to a specific instance within the target group.

Stickiness type

☒ Load balancer generated cookie

☐ Application-based cookie

Stickiness duration

days

▼

1 second - 7 days

Cancel

Save changes

Enable the **Stickiness** flag.

Click the **Save changes** button.

8.2.7 Enable Stickiness for the TCP/8084 Target Group

Repeat the previous instructions to enable Stickiness for the ema-websocket (TCP/8084) target group.

8.2.8 Note on Monitoring Target Group Health

In any of the target groups, you can check the **Targets** and **Monitoring** tabs to see the health check status of the target instances. Those health checks will initially fail until the Intel EMA software has been installed.

8.3 Create a Network Load Balancer for web traffic

Follow this procedure to create a Network Load Balancer to distribute traffic to healthy target groups.

8.3.1 Create the Load Balancer

Placement Groups **New**

Key Pairs **New**

Network Interfaces

▼ Load Balancing

Load Balancers

Target Groups **New**

Create Load Balancer

Actions ▼

☐

Name

▲

DNS name

▼

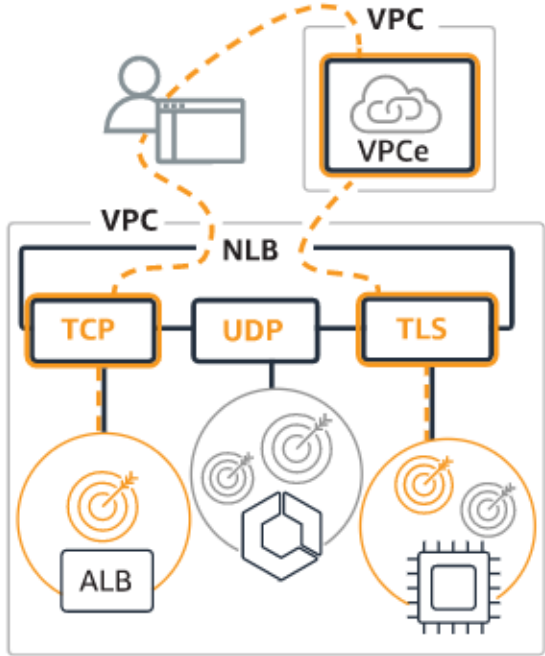
State

You do not have any load balancers in this region.

From the **EC2** sidebar, under **Load Balancing**, select **Load Balancers** and click on **Create Load Balancer**.

8.3.2 Choose Load Balancer Type

Network Load Balancer [Info](#)



Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Create

Click the **Create** button under the **Network Load Balancer** heading.

8.3.3 Configure Load Balancer

8.3.3.1 Basic Configuration

<div>Basic configuration</div> <div><p>Load balancer name Name must be unique within your AWS account and cannot be changed after the load balancer is created.</p><input type="text" value="ema-web-balancer"/> <small>A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.</small><p>Scheme Scheme cannot be changed after the load balancer is created.</p><p><input checked="" type="radio"/> Internet-facing An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more</p><p><input type="radio"/> Internal An internal load balancer routes requests from clients to targets using private IP addresses.</p><p>IP address type Info Select the type of IP addresses that your subnets use.</p><p><input checked="" type="radio"/> IPv4 Recommended for internal load balancers.</p><p><input type="radio"/> Dualstack Includes IPv4 and IPv6 addresses.</p></div>	<p>Enter the basic configuration.</p> <p>Name: Enter a unique name Example: <i>ema-web-balancer</i></p> <p>Scheme: internet-facing Note: If your organization has a site-to-site VPN with AWS giving you private IP access, then this could be an internal load balancer bound to the private subnets.</p> <p>For this guide, we assume no such access so it will be an internet-facing load balancer bound to the public subnets.</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

8.3.3.2 Availability Zones

<div>Network mapping Info</div> <div><p>The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.</p></div> <div><p>VPC Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.</p><div><div>AWS</div><div>vpc-03389964</div><div>IPv4: 10.0.0.0/16</div></div><div></div></div> <div><p>Mappings 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. Subnets cannot be removed after the load balancer is created, but additional subnets can be added.</p><div><div><input checked="" type="checkbox"/> us-west-2a</div><div><p>Subnet</p><div>subnet-e55d8e82</div><div>subnet2</div></div><div><p>The subnet for your internet-facing load balancer must have a route to an internet gateway. You can update the subnet's route table in the VPC Console.</p></div></div><div><p>IPv4 settings</p><p>IPv4 address</p><div>Assigned by AWS</div></div><div><div><input checked="" type="checkbox"/> us-west-2b</div><div><p>Subnet</p><div>subnet-fc6d768a</div><div>subnet1</div></div><div><p>IPv4 settings</p><p>IPv4 address</p><div>Assigned by AWS</div></div></div></div>	<p>Configure the Network Mapping section as follows:</p> <ul style="list-style-type: none">• VPC: Select the VPC that you previously created.• Mappings: Enable both availability zones and select both of your public subnets. IPv4 address should be set to <i>Assigned by AWS</i> <p>Click the Next: Configure Security Settings button.</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

8.3.3.3 Listeners

Listeners and routing [Info](#)

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification.

▼ Listener TCP:443 [Remove](#)

ProtocolPortDefault action [Info](#)

TCP:4431-65535

Forward toSelect a target group

[Create target group](#)

▼ Listener TCP:8084 [Remove](#)

ProtocolPortDefault action [Info](#)

TCP:80841-65535

Forward toSelect a target group

[Create target group](#)

[Add listener](#)

In the **Listeners** section, add listeners for these protocols and ports.

- TCP 443
- TCP 8084

8.3.3.4 Review

Summary
Review and confirm your configurations. [Estimate cost](#)

Basic configuration [Edit](#)
ema-web-balancer

- Internet-facing
- IPv4

Network mapping [Edit](#)
VPC [vpc-03389964](#)
AWS

- us-west-2a
[subnet-e55d8e82](#)
subnet2
- us-west-2b
[subnet-fc6d768a](#)
subnet1

Listeners and routing [Edit](#)

- TCP:443 defaults to [ema-web](#)
- TCP:8084 defaults to [ema-websocket](#)

Tags [Edit](#)
None

Attributes

[i](#) Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

[Cancel](#) [Create load balancer](#)

8.4 Create a Network Load Balancer for swarm traffic

8.4.1 Create the Load Balancer

Placement Groups [New](#)

Key Pairs [New](#)

Network Interfaces

▼ Load Balancing

[Load Balancers](#)

Target Groups [New](#)

[Create Load Balancer](#) [Actions](#)

<input type="checkbox"/>	Name	DNS name	State
You do not have any load balancers in this region.			

From the **EC2** sidebar, under **Load Balancing**, select **Load Balancers** and click on **Create Load Balancer**.

Intel® EMA Web Deployment Guide for AWS – February 2022

43

8.4.2 Choose Load Balancer Type

Network Load Balancer [Info](#)

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Create

Click the **Create** button under the **Network Load Balancer** heading.

8.4.3 Configure Load Balancer

8.4.3.1 Basic Configuration

<div>Basic configuration</div> <div><p>Load balancer name Name must be unique within your AWS account and cannot be changed after the load balancer is created.</p><input type="text" value="ema-swarm-balancer"/><p>A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.</p><p>Scheme Scheme cannot be changed after the load balancer is created.</p><p><input checked="" type="radio"/> Internet-facing An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more</p><p><input type="radio"/> Internal An internal load balancer routes requests from clients to targets using private IP addresses.</p><p>IP address type Info Select the type of IP addresses that your subnets use.</p><p><input checked="" type="radio"/> IPv4 Recommended for internal load balancers.</p><p><input type="radio"/> Dualstack Includes IPv4 and IPv6 addresses.</p></div>	<p>Enter the basic configuration.</p> <p>Name: Enter a unique name Example: <i>ema-swarm-balancer</i></p> <p>Scheme: internet-facing</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------

8.4.3.2 Availability Zones

<div>Network mapping Info</div> <div>The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.</div> <div><p>VPC Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.</p><div><div>AWS</div><div>vpc-03389964</div><div>IPv4: 10.0.0.0/16</div></div><div></div></div> <div><p>Mappings 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. Subnets cannot be removed after the load balancer is created, but additional subnets can be added.</p><div><div><input checked="" type="checkbox"/> us-west-2a</div><div><p>Subnet</p><div>subnet-e55d8e82 subnet2 ▾</div><div><p>⚠ The subnet for your internet-facing load balancer must have a route to an internet gateway. You can update the subnet's route table in the VPC Console.</p></div></div><div><p>IPv4 settings</p><p>IPv4 address</p><div>Assigned by AWS ▾</div></div></div><div><div><input checked="" type="checkbox"/> us-west-2b</div><div><p>Subnet</p><div>subnet-fc6d768a subnet1 ▾</div></div><div><p>IPv4 settings</p><p>IPv4 address</p><div>Assigned by AWS ▾</div></div></div></div>	<p>Configure the Network Mapping section as follows:</p> <ul style="list-style-type: none">• VPC: Select the VPC that you previously created.• Mappings: Enable both availability zones and select both of your public subnets. IPv4 address should be set to <i>Assigned by AWS</i> <p>Click the Next: Configure Security Settings button.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

8.4.3.3 Listeners

Listeners and routing [Info](#)

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification.

▼ Listener TCP:8080 [Remove](#)

ProtocolPortDefault action [Info](#)

TCP:80801-65535Forward to: ema-swarm [Info](#)
Target type: Instance, IPv4

[Create target group](#)

[Add listener](#)

In the **Listeners** section, add listeners for these protocols and ports.

- *TCP 8080*

8.4.3.4 Review

Summary

Review and confirm your configurations. [Estimate cost](#)

Basic configuration [Edit](#)

ema-swarm-balancer

- Internet-facing
- IPv4

Network mapping [Edit](#)

VPC [vpc-03389964](#)

AWS

- us-west-2a
[subnet-e55d8e82](#)
subnet2
- us-west-2b
[subnet-fc6d768a](#)
subnet1

Listeners and routing [Edit](#)

- TCP:8080 defaults to [ema-swarm](#)

Tags [Edit](#)

None

Attributes

[i](#) Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

[Cancel](#)

[Create load balancer](#)

8.4.4 Note the Load Balancer DNS Name

Go back to the **Description** tab of the load balancers and make note of the DNS names. You will want to create CNAME records with your DNS provider for your custom domain name(s) so that you can direct your Intel EMA web traffic and swarm traffic to the load balancers.

<input type="checkbox"/>	Name	DNS name	State
<input type="checkbox"/>	ema-swarm-balancer	ema-swarm-balancer-2dd41f...	active
<input checked="" type="checkbox"/>	ema-web-balancer	ema-web-balancer-9faa96fc...	active

Load balancer: ema-web-balancer

- Description
- Listeners
- Monitoring
- Integrated services
- Tags

Basic Configuration

Name	ema-web-balancer
ARN	arn:aws:elasticloadbalancing:us-west-1:802420695018:loadbalancer/net/errbalancer/9faa96fc630182c2
DNS name	ema-web-balancer-9faa96fc630182c2.elb.us-west-1.amazonaws.com (A Record)

9 Appendix A - Notes on Active Directory Integration

There are multiple ways that you can integrate Active Directory with AWS to be able to join your virtual machine(s) to a domain and use AD authentication. Because the needs of the organization can be so varied, this appendix only offers some brief pointers on how you might extend an existing on-premises directory to the cloud for this purpose. Cloud providers change and expand their service offerings from time to time, so you should do your own research before deploying a production solution so see what makes the most sense for your business.

For more information about Active Directory services in AWS, visit the following links:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>

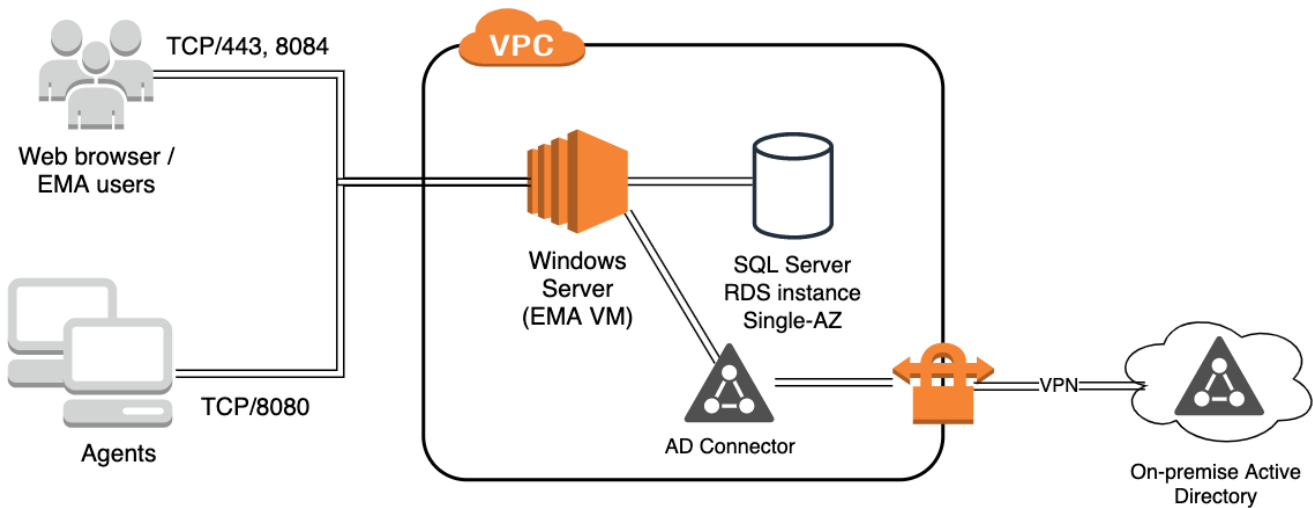
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq_connector.html

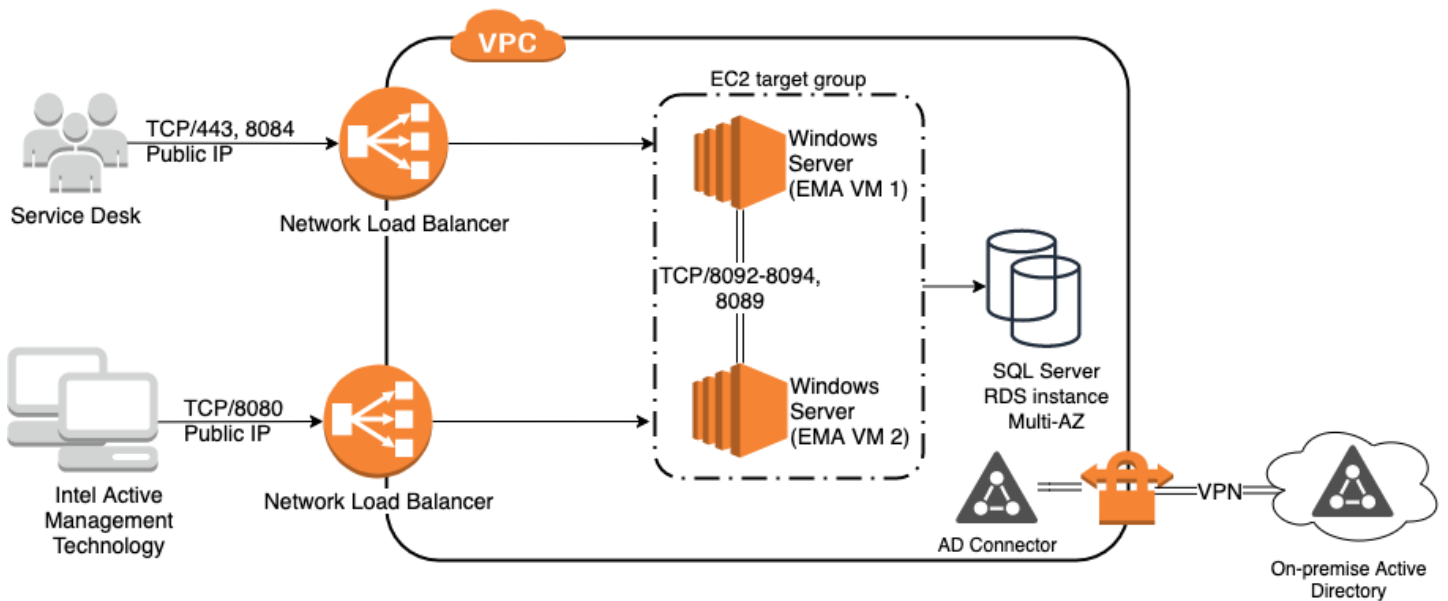
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_best_practices.html

10 Architecture Diagram with Active Directory Integration

10.1 Single Server Deployment



10.2 Distributed Server Deployment



10.3 Using AWS AD Connector to Extend Active Directory to the Cloud

- ❑ Create a VPN to connect to your on-premise network to provide connectivity to your domain controllers.
 - ❑ Create a Customer Gateway to represent the remote (on-prem) end of the VPN
 - ❑ Create a Virtual Private Gateway to provide routing between the VPN and your VPC
 - ❑ Attach the Virtual Private Gateway to your VPC
 - ❑ Create a VPN connection, selecting the new Customer Gateway and VPG.

- ❑ Select the Static routing option and enter the networks that are available through the VPN connection. This should include your on-premise domain controllers.
 - ❑ You can let Amazon generate your tunnel addresses and keys.
- ❑ Download the VPN connection configuration to help configure the other side.
- ❑ Go to your VPC route table and enable route propagation, so that the routes associate with the VPN connection are available to your VPC network.
- ❑ Create an AD Connector resource to act as a proxy to your on-prem AD
 - ❑ Select AD Connector as your directory type
 - ❑ Choose the directory size appropriate for the number of objects you need to support.
 - ❑ Choose your VPC and the two different subnets
 - ❑ Enter the information for the on-premise directory that you will connect to.
 - ❑ Note that a service account is required. The prerequisites are fully described in the documentation links provided below.
- ❑ Create a DHCP Options set and associate it with your VPC so that virtual machines will receive the proper DNS servers and domain name.
 - ❑ Provide the Active Directory domain name and DNS servers. Other parameters are optional.
 - ❑ Go to your VPC and associate the DHCP options set with it.
- ❑ When you are configuring the EC2 virtual machine instances, use the Domain join option to have the VM automatically joined to your AD domain.