

Intel® Endpoint Management Assistant (Intel® EMA)

Guía de implementación para Amazon Web Services* (AWS)

Intel® Versión 1.3.3

Octubre de 2020

Descargo de responsabilidad

Las tecnologías Intel podrían requerir hardware y software habilitados o la activación de servicios.

Ningún producto o componente puede ser absolutamente seguro.

Sus costos y resultados pueden variar.

Este documento no concede ninguna licencia (explícita o implícita, por impedimento legal u otro medio) para derechos de propiedad intelectual.

Intel rechaza cualquier garantía explícita o implícita incluidas, entre otras, las garantías implícitas de comercialización, adecuación para un propósito en particular y las garantías de no infracción, así como también cualquier garantía relacionada con el curso de ejecución, curso de las negociaciones, o usos y costumbres en operaciones comerciales.

Los productos y servicios aquí descritos pueden contener defectos o errores conocidos como erratas que pueden hacer que varíen respecto a las especificaciones publicadas. Las erratas detectadas hasta el momento están disponibles a petición del interesado.

Las características y los beneficios de las tecnologías Intel dependen de la configuración del sistema y podrían requerir hardware y software habilitados o la activación del servicio. El desempeño varía según la configuración del sistema. Ningún sistema informático puede ser absolutamente seguro. Intel no asume responsabilidad alguna por las pérdidas o los robos de datos o sistemas, ni por los daños ocasionados por dichas pérdidas. Consulte con el fabricante del sistema o con el distribuidor minorista. También puede encontrar más información en <http://www.intel.com/technology/vpro>.

© Intel Corporation. Intel, el logotipo Intel y otras marcas Intel son marcas comerciales de Intel Corporation o sus filiales.

* Otros nombres y marcas podrían ser reclamados como propiedad de terceros.

Contenido

1	Introducción.....	1
1.1	Sobre la informática en la nube.....	1
1.2	Navegación en la consola de administración de AWS.....	1
1.2.1	Servicios.....	1
1.2.2	Grupos de recursos.....	2
1.2.3	Regiones.....	2
1.3	Etiquetas y grupos de recursos.....	2
1.4	Antes de comenzar.....	2
2	Diagramas de arquitectura de alto nivel.....	3
2.1	Implementación de un servidor único.....	3
2.2	Implementación de servidores distribuidos.....	3
3	Seleccionar la región de implementación.....	4
4	Implementación de red.....	5
4.1	Descripción general.....	5
4.2	Crear una VPC.....	5
4.2.1	Ir al servicio de VPC.....	5
4.2.2	Crear una VPC.....	6
4.2.3	Configurar los detalles de la VPC.....	6
4.3	Crear subredes.....	7
4.3.1	Ir a la pantalla Subnets.....	7
4.3.2	Crear la primera subred privada.....	7
4.3.3	Crear la segunda subred privada.....	8
4.3.4	Crear la primera subred pública.....	8
4.3.5	Crear la segunda subred pública.....	9
4.3.6	Revisar sus subredes.....	9
4.4	Crear una puerta de enlace a Internet para las subredes públicas.....	9
4.4.1	Crear puertas de enlace a Internet.....	9
4.4.2	Asociar la puerta de enlace a Internet a la VPC.....	10
4.4.3	Ingresar los detalles de la asociación.....	10
4.5	Crear puertas de enlace NAT para las subredes privadas.....	11
4.5.1	Ir a las puertas de enlace NAT.....	11
4.5.2	Crear la primera puerta de enlace NAT.....	11
4.5.3	Crear la segunda puerta de enlace NAT.....	12
4.6	Crear y configurar las tablas de rutas.....	12
4.6.1	Ir a las tablas de rutas.....	12
4.6.2	Crear la tabla de rutas para las subredes públicas.....	13
4.6.3	Crear la tabla de rutas para la primera subred privada.....	13
4.6.4	Crear la tabla de rutas para la segunda subred privada.....	13
4.6.5	Revisar la lista de tabla de rutas.....	14
4.6.6	Editar las rutas para la tabla de la primera subred privada.....	14
4.6.7	Editar las asociaciones de subred para la tabla de rutas de la primera subred privada.....	15
4.6.8	Editar las rutas para la tabla de la segunda subred privada.....	15
4.6.9	Editar las asociaciones de subred para la tabla de rutas de la segunda subred privada.....	16
4.6.10	Editar las rutas para la tabla de subredes públicas.....	16
4.6.11	Editar las asociaciones de subred para la tabla de rutas de subredes públicas.....	17
4.7	Grupos de seguridad.....	17
4.7.1	Crear un grupo de seguridad para las VMs.....	17
4.7.2	Actualizar el grupo de seguridad para permitir el tráfico entre las VMs Intel® EMA (solo para servidores distribuidos).....	20
4.7.3	Crear un grupo de seguridad para la base de datos.....	21

5	Implementación de la máquina virtual	23
5.1	Descripción general	23
5.2	Crear máquinas virtuales	23
5.2.1	Ir al servicio EC2	23
5.2.2	Iniciar una instancia de EC2	23
5.2.3	Seleccionar una imagen de máquina de Amazon	24
5.2.4	Seleccionar el tipo de máquina	24
5.2.5	Configurar los detalles de la instancia	25
5.2.6	Agregar almacenamiento	25
5.2.7	Agregar etiquetas	25
5.2.8	Configurar el grupo de seguridad	26
5.2.9	Revisar el lanzamiento de la instancia	26
5.2.10	Seleccionar un par de claves de EC2	26
5.3	Crear una segunda instancia de EC2 (solo para servidores distribuidos)	26
6	Configurar AWS Systems Manager (solo para servidores distribuidos)	27
6.1	Ir al servicio Systems Manager	27
6.2	Comenzar la configuración rápida	27
6.3	Seleccionar las opciones de permisos	28
6.4	Seleccionar las opciones de configuración	28
6.5	Seleccionar los destinos	29
6.6	Verificar la lista de instancias gestionadas	29
6.7	Iniciar sesión en sus máquinas virtuales a través de Session Manager	29
7	Implementación de Relational Database Service (RDS)	30
7.1	Navegación al servicio RDS	30
7.2	Crear un grupo de subredes de base de datos	30
7.2.1	Detalles del grupo de subredes	31
7.3	Crear una base de datos	31
7.3.1	Seleccionar el método de creación de la base de datos	32
7.3.2	Seleccionar el tipo y la edición del motor	32
7.3.3	Seleccionar la plantilla de implementación	32
7.3.4	Configurar el nombre de la instancia y las credenciales del usuario maestro	33
7.3.5	Configurar el tamaño de la instancia de DB	33
7.3.6	Configurar el almacenamiento (opcional)	33
7.3.7	Configurar la conectividad	34
7.3.8	Configurar la conectividad (configuración adicional)	34
7.3.9	Revisar y crear	35
7.4	Obtener el nombre del host de la base de datos	35
8	Implementación del equilibrador de cargas (solo para servidores distribuidos)	36
8.1	Descripción general	36
8.2	Crear grupos de destinos	36
8.2.1	Crear grupos de destinos	36
8.2.2	Configurar un grupo de destinos para TCP/443	37
8.2.3	Crear o configurar un destino para TCP/8084	38
8.2.4	Configurar un destino para TCP/8080	38
8.2.5	Revisar los grupos de destinos	39
8.2.6	Habilitar la permanencia para el grupo de destinos TCP/443	39
8.2.7	Habilitar la permanencia para el grupo de destinos TCP/8084	40
8.2.8	Nota sobre la supervisión del estado del grupo de destinos	40
8.3	Crear un equilibrador de carga de red para el tráfico web	40
8.3.1	Crear el equilibrador de carga	40
8.3.2	Seleccionar el tipo de equilibrador de carga	40
8.3.3	Configurar el equilibrador de carga	41

8.3.4	Corregir las reglas de reenvío del equilibrador de carga.....	43
8.4	Crear un equilibrador de carga de red para el tráfico Swarm.....	45
8.4.1	Crear el equilibrador de carga	45
8.4.2	Seleccionar el tipo de equilibrador de carga.....	45
8.4.3	Configurar el equilibrador de carga.....	45
8.4.4	Tomar nota del nombre de DNS del equilibrador de carga	47
9	Apéndice A: notas sobre la integración de Active Directory*	49
10	Diagrama de arquitectura con integración de Active Directory.....	50
10.1	Implementación de un servidor único.....	50
10.2	Implementación de servidores distribuidos	50
10.3	Usar el conector de AD de AWS para extender Active Directory a la nube.....	50

1 Introducción

En este documento, se describe el procedimiento para implementar infraestructura en Amazon Web Services*, una plataforma informática en la nube, la cual es necesaria para admitir una o más instancias del servidor Intel® Endpoint Management Assistant (Intel® EMA). Está pensado para administradores de TI con conocimientos intermedios o avanzados de la infraestructura de TI que podrían tener conocimiento limitado sobre informática en la nube.

Se necesitan varios componentes para crear un entorno completo de infraestructura en la nube, por eso recomendamos que lea esta guía con detenimiento para comprender cómo están configurados para funcionar juntos. Antes del procedimiento de implementación, se incluye una descripción de cada componente con un enlace a la documentación del proveedor en la nube oficial en el que podrá obtener más información si fuera necesario.

1.1 Sobre la informática en la nube

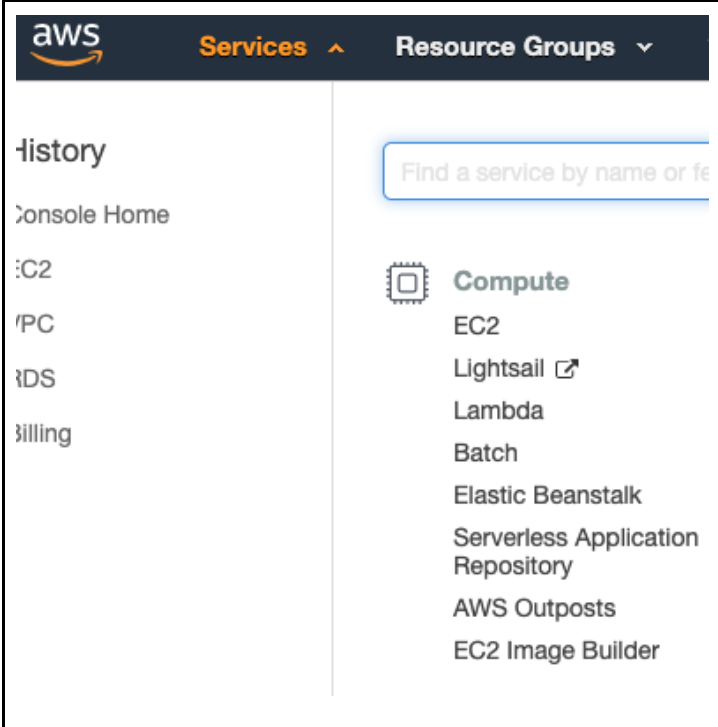
La informática en la nube es el suministro a pedido de recursos de TI a través de Internet con precios determinados por el uso del servicio. En lugar de comprar, poseer y mantener centros de datos físicos y servidores, puede acceder a servicios de tecnología, como potencia informática, almacenamiento y bases de datos de un proveedor en la nube según lo requiera. Puede disponer solo de lo que necesita en el momento y escalar la capacidad para crecer y contraerse a medida que se modifiquen sus necesidades empresariales.

Los grandes proveedores en la nube tienen centros de datos en todo el mundo, lo que le permite implementar recursos que estén cerca de la ubicación geográfica de sus clientes y usuarios finales.

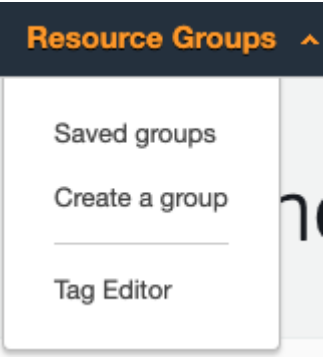
Con los servicios totalmente administrados, como Amazon Relational Database Service, puede enfocarse en sus datos mientras el proveedor de nube gestiona todo el hardware y software subyacente que proporciona el servicio. Las máquinas virtuales que se ejecutan en la nube permiten administrar solo el sistema operativo huésped y el software que tenga instalado, mientras el proveedor en la nube gestiona el hardware subyacente y trabaja para brindarle la mejor disponibilidad y confiabilidad.

1.2 Navegación en la consola de administración de AWS

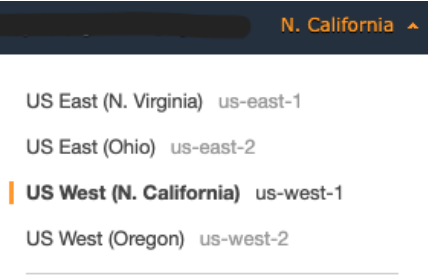
1.2.1 Servicios

 The screenshot shows the AWS console interface. At the top, there is a dark navigation bar with the AWS logo on the left, the word "Services" in orange with an upward arrow, and "Resource Groups" with a downward arrow. Below this, a sidebar on the left contains a "history" section with links for "Console Home", "EC2", "EBS", "EFS", "IAM", "Lambda", "S3", and "Billing". The main content area features a search bar with the placeholder text "Find a service by name or feature". Below the search bar, a list of services is displayed under the heading "Compute". The listed services are: EC2, Lightsail (with an external link icon), Lambda, Batch, Elastic Beanstalk, Serverless Application Repository, AWS Outposts, and EC2 Image Builder.	<p>Después de haber iniciado sesión en la consola de administración de AWS en https://aws.amazon.com/console/, verá un menú Services en la esquina superior izquierda de la pantalla.</p> <p>Si hace clic allí, abrirá una lista de todos los servicios que brinda AWS organizados por categoría, como Compute, Storage, Database, etc.</p> <p>Cuando se brinden instrucciones para implementar servicios en esta guía, lo dirigiremos a esta pantalla para que seleccione el servicio apropiado.</p>
--	---

1.2.2 Grupos de recursos

 A screenshot of the AWS console showing the 'Resource Groups' dropdown menu. The menu is open, displaying three options: 'Saved groups', 'Create a group', and 'Tag Editor'. The 'Resource Groups' header is at the top with an upward-pointing arrow.	<p>Junto a Services, se encuentra el menú Resource Groups, donde puede crear grupos de recursos o ver los que haya creado.</p> <p>Normalmente, verá todos los recursos implementados en la región actual, independientemente de quién los haya implementado o a qué proyecto pertenezcan, de modo que usar grupos de recursos le permite tener una lista filtrada de recursos basada en las etiquetas personalizadas que haya asociado a cada recurso.</p>
--	--

1.2.3 Regiones

 A screenshot of the AWS console showing the region selection dropdown menu. The menu is open, displaying four options: 'US East (N. Virginia) us-east-1', 'US East (Ohio) us-east-2', 'US West (N. California) us-west-1', and 'US West (Oregon) us-west-2'. The 'US West (N. California) us-west-1' option is highlighted with a vertical bar on the left.	<p>En la esquina superior derecha de la consola de administración, verá un menú donde tendrá que seleccionar la región en la que desea implementar recursos.</p> <p>Solo podrá ver los recursos de la región que haya seleccionado.</p>
---	---

Cada región de AWS contiene varias ubicaciones distintas, que se denominan zonas de disponibilidad o AZ. Cada zona de disponibilidad está diseñada para aislarse de los errores que puedan tener otras zonas de disponibilidad.

1.3 Etiquetas y grupos de recursos

Las etiquetas son pares clave-valor personalizados que se pueden asignar a muchos tipos diferentes de recursos que puede implementar en AWS. Se recomienda etiquetar los recursos cuando se crean para poder realizar un seguimiento sencillo del propietario de los recursos y averiguar a qué proyecto pertenecen, y también para tener grupos de recursos e informes de facturación basados en etiquetas.

En esta guía no explicaremos cómo se hace el etiquetado ni la creación de grupos de recursos, ya que existen muchas maneras diferentes de hacerlo y se agregarían muchos pasos adicionales, pero debe tener en cuenta que existen estas opciones en caso de que desee implementar una estrategia de etiquetado y agrupación de recursos.

Para obtener más información sobre cómo usar etiquetas, visite el siguiente enlace:

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

1.4 Antes de comenzar

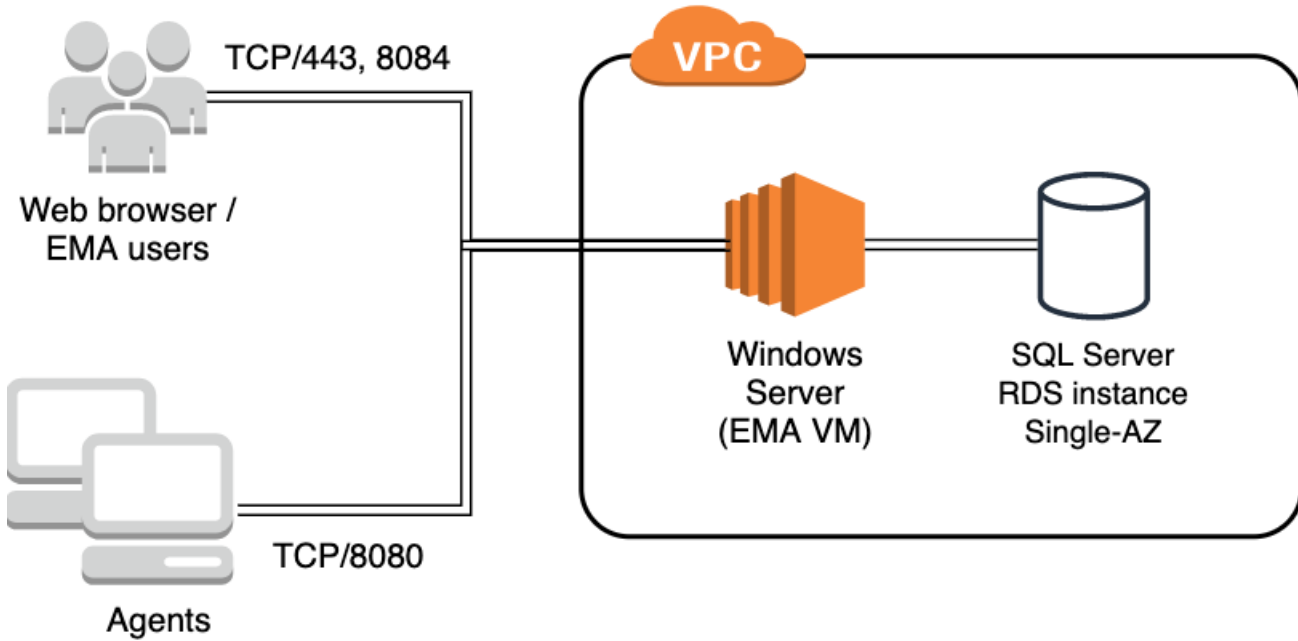
Si su organización ya tiene una cuenta de AWS, debería pedirle a un administrador de la nube que le conceda los accesos necesarios para poder crear todos los recursos enumerados en esta guía.

Si su organización no tiene una cuenta de AWS o quiere evaluarla de forma particular, puede ir a <https://aws.amazon.com/console/> y hacer clic en el botón **Create a Free Account**.

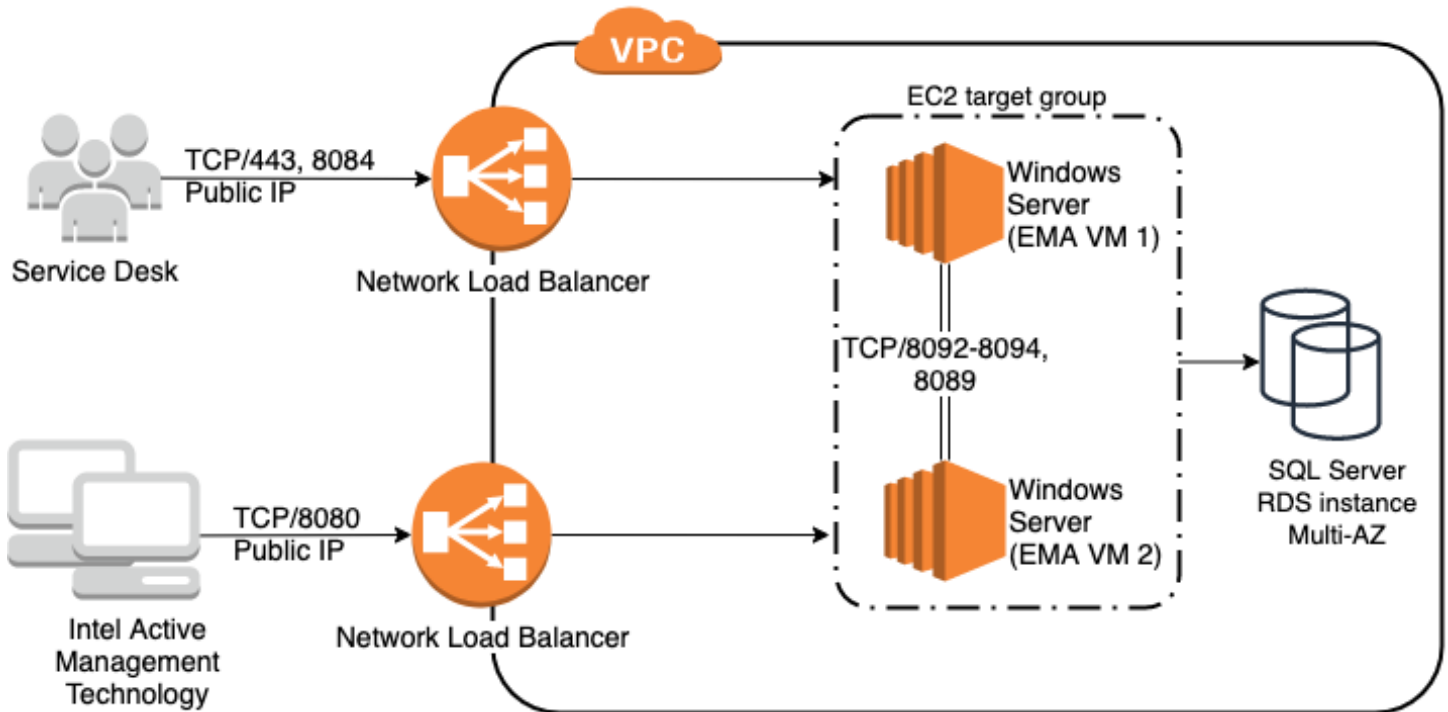
Consulte con su administrador de redes si existe algún espacio de dirección preferencial para utilizar. Es conveniente evitar la superposición con sus redes empresariales para prevenir problemas de enrutamiento si ya tiene una VPN establecida para el proveedor en la nube o si planea tenerla en el futuro. También tendrá que saber cuál será la dirección IP de origen del tráfico que sale de su organización para llegar a la nube. De este modo, podrá permitirles solo a redes confiables que lleguen a la máquina virtual de Intel® EMA desde Internet.

2 Diagramas de arquitectura de alto nivel

2.1 Implementación de un servidor único



2.2 Implementación de servidores distribuidos



3 Seleccionar la región de implementación

En el menú de la región en la esquina superior derecha, elija la región en la que desea implementar recursos.



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 Implementación de red

4.1 Descripción general

Para que las máquinas virtuales se comuniquen entre sí, con el proveedor en la nube o con internet, tenemos que configurar un entorno de red en primer lugar. La nube privada virtual (VPC) es el módulo fundamental que se necesita para crear su red privada en AWS, y se asemeja mucho a una red tradicional, excepto que está virtualizada dentro de AWS. Las VPC están aisladas lógicamente entre sí.

Cuando cree una VPC, deberá proporcionar un espacio de dirección IP privada y personalizada. AWS asignará recursos a la dirección IP privada desde este espacio de dirección cuando sea necesario. Recomendamos que evite usar un espacio de dirección que se superponga con los demás rangos de red de su organización para evitar el enrutamiento si las redes se conectan a través de una VPN. Deberá consultar con su equipo de ingeniería de redes para elegir un bloqueo de dirección IP disponible a fin de evitar conflictos de enrutamiento en caso de que su empresa ya tenga una conectividad IP privada a la nube o la vaya a tener en el futuro.

Después de crear la VPC, también crearemos nuestras subredes. Las subredes le permiten segmentar la red de la VPC mediante la asignación de una porción del espacio de dirección de la red a cada subred. Nuestras subredes existirán en dos zonas de disponibilidad (AZ) separadas en nuestra región seleccionada para que podamos proporcionar una mayor disponibilidad en nuestra base de datos y la aplicación Intel® EMA. Vamos a crear las subredes públicas y privadas para utilizar una u otra según si el recurso necesita acceso directo a Internet con una dirección de IP pública.

Por defecto, el firewall de AWS no permite un acceso de entrada a nuestros recursos, por lo que parte de la implementación de la red incluirá crear grupos de seguridad para habilitar la comunicación de red con esos recursos.


Para reducir la superficie de ataque de nuestras máquinas virtuales, no se permitirá el acceso de RDP a través del firewall de la VPC. En su lugar, vamos a utilizar AWS Session Manager para habilitar la administración remota de las máquinas virtuales (VM). Además, en las implementaciones de servidores distribuidos, ninguna de las máquinas virtuales tendrá una dirección IP pública.

Para obtener más información sobre las VPC, visite los siguientes enlaces:
<https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-vpc.html>

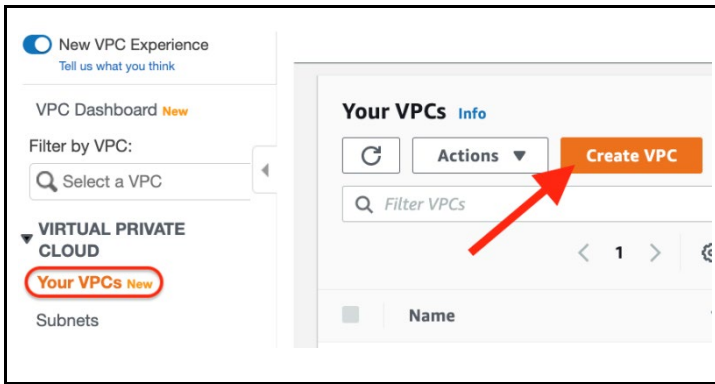
4.2 Crear una VPC

Podría utilizar el asistente de VPC si está realizando una implementación de un único servidor con una subred pública, pero aquí vamos a crear todos los componentes de red de forma manual para mostrar mejor lo que necesitamos y porque el asistente no sería suficiente para una implementación de servidores distribuidos.

4.2.1 Ir al servicio de VPC

 <p>Networking & Content Delivery</p> <p>VPC</p> <p>CloudFront</p>	<p>En el menú Services, en Network & Content Delivery, seleccione VPC.</p>
--	---

4.2.2 Crear una VPC



New VPC Experience
Tell us what you think

VPC Dashboard **New**

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD
Your VPCs **New**
Subnets

Your VPCs **Info**

Actions **Create VPC**

Filter VPCs

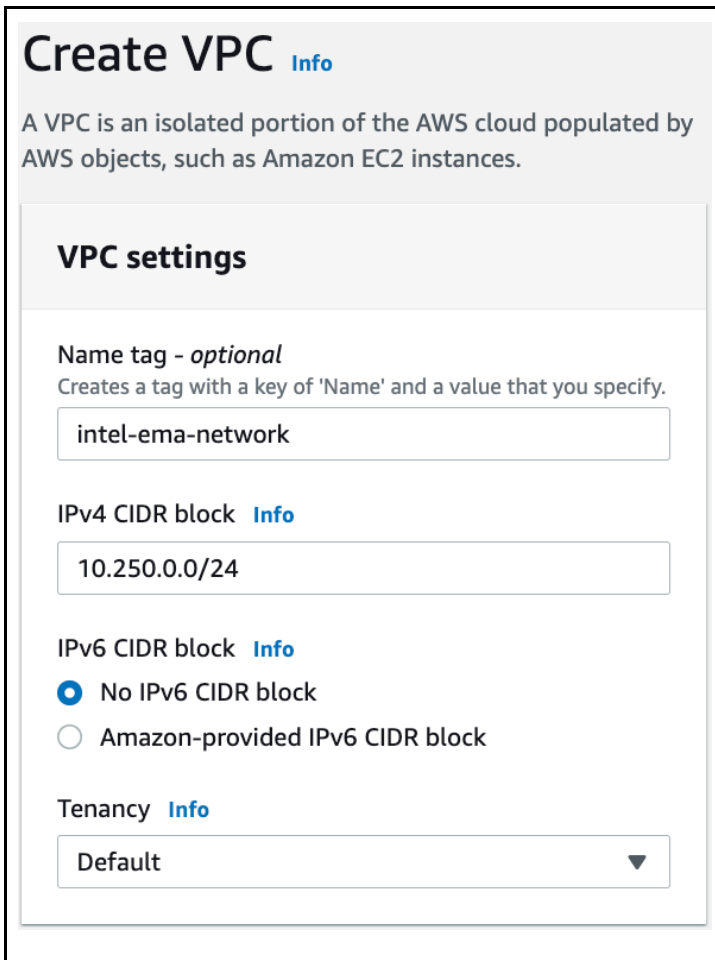
< 1 >

Name

En la barra lateral de la VPC, seleccione **Your VPCs**.

Haga clic en el botón **Create VPC**.

4.2.3 Configurar los detalles de la VPC



Create VPC **Info**

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
intel-ema-network

IPv4 CIDR block **Info**
10.250.0.0/24

IPv6 CIDR block **Info**
 No IPv6 CIDR block
 Amazon-provided IPv6 CIDR block

Tenancy **Info**
Default

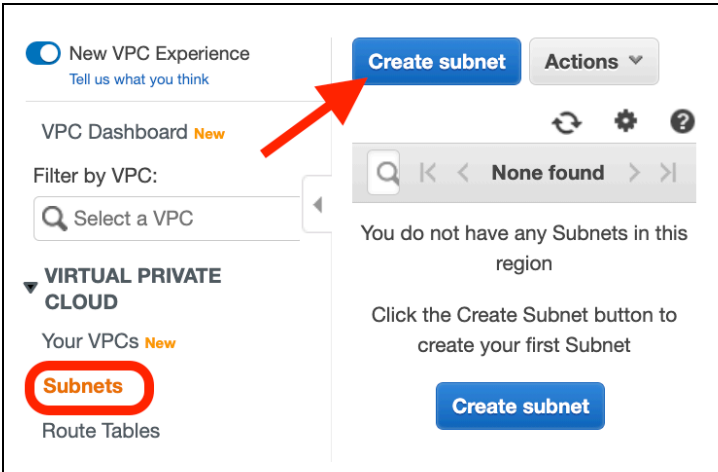
Ingrese los detalles de la red de la siguiente manera:

- **Name Tag:** ingrese un nombre único para la VPC.
Ejemplo: *intel-ema-network*
- **IPv4 CIDR block:** elija una red sin usar lo suficientemente grande como para contener subredes.
Ejemplo: *10.250.0.0/24*

Haga clic en el botón **Create VPC**.

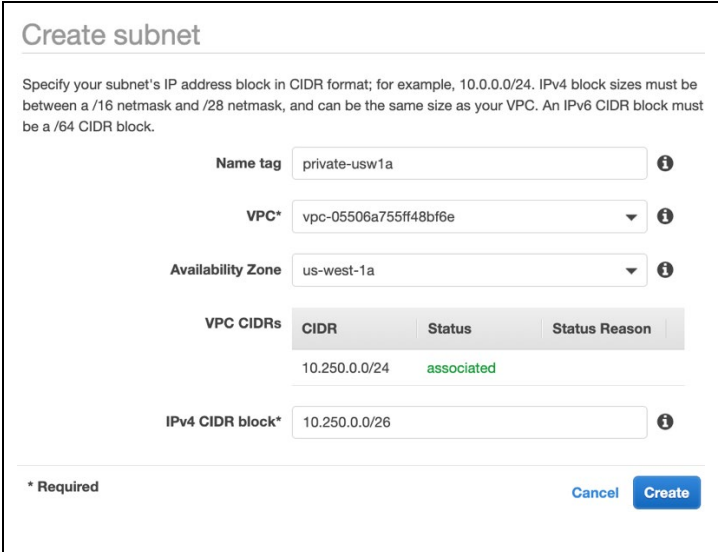
4.3 Crear subredes

4.3.1 Ir a la pantalla Subnets



En la barra lateral de VPC, seleccione **Subnets**.

4.3.2 Crear la primera subred privada



Haga clic en el botón **Create subnet**.

Configure la subred de la siguiente manera:

- **Name tag:** proporcione un nombre de subred único. Ejemplo: *private-usw1a*
- **VPC:** seleccione la red virtual que creó anteriormente.
- **Availability Zone:** en nuestro diseño, queremos usar dos zonas distintas, así que aquí use la primera zona que eligió. Ejemplo: *us-west-1a*
- **IPv4 CIDR block:** seleccione un bloque de IP sin usar en el espacio de dirección de su VPC. Ejemplo: *10.250.0.0/26*

Haga clic en el botón **Create**.

4.3.3 Crear la segunda subred privada

<p>Name tag <input type="text" value="private-usw1b"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> <p>Availability Zone <input type="text" value="us-west-1b"/></p> <p>VPC CIDRs</p> <table border="1"><thead><tr><th>CIDR</th><th>Status</th><th>Status Reason</th></tr></thead><tbody><tr><td>10.250.0.0/24</td><td>associated</td><td></td></tr></tbody></table> <p>IPv4 CIDR block* <input type="text" value="10.250.0.64/26"/></p>	CIDR	Status	Status Reason	10.250.0.0/24	associated		<p>Haga clic en el botón Create subnet.</p> <p>Configure la subred de la siguiente manera:</p> <ul style="list-style-type: none">• Name tag: proporcione un nombre de subred único. Ejemplo: <i>private-usw1b</i>• VPC: seleccione la red virtual que creó anteriormente.• Availability Zone: en nuestro diseño, queremos usar dos zonas distintas, así que use la segunda zona que eligió aquí. Ejemplo: <i>us-west-1b</i>• IPv4 CIDR block: seleccione un bloque de IP sin usar en el espacio de dirección de su VPC. Ejemplo: <i>10.250.0.64/26</i> <p>Haga clic en el botón Create.</p>
CIDR	Status	Status Reason					
10.250.0.0/24	associated						

4.3.4 Crear la primera subred pública

<p>Name tag <input type="text" value="public-usw1a"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> <p>Availability Zone <input type="text" value="us-west-1a"/></p> <p>VPC CIDRs</p> <table border="1"><thead><tr><th>CIDR</th><th>Status</th><th>Status Reason</th></tr></thead><tbody><tr><td>10.250.0.0/24</td><td>associated</td><td></td></tr></tbody></table> <p>IPv4 CIDR block* <input type="text" value="10.250.0.128/26"/></p>	CIDR	Status	Status Reason	10.250.0.0/24	associated		<p>Haga clic en el botón Create subnet.</p> <p>Configure la subred de la siguiente manera:</p> <ul style="list-style-type: none">• Name tag: proporcione un nombre de subred único. Ejemplo: <i>public-usw1a</i>• VPC: seleccione la red virtual que creó anteriormente.• Availability Zone: en nuestro diseño, queremos usar dos zonas distintas, así que aquí use la primera zona que eligió. Ejemplo: <i>us-west-1a</i>• IPv4 CIDR block: seleccione un bloque de IP sin usar en el espacio de dirección de su VPC. Ejemplo: <i>10.250.0.128/26</i> <p>Haga clic en el botón Create.</p>
CIDR	Status	Status Reason					
10.250.0.0/24	associated						

4.3.5 Crear la segunda subred pública

<p>Name tag <input type="text" value="public-usw1b"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> <p>Availability Zone <input type="text" value="us-west-1b"/></p> <p>VPC CIDRs</p> <table border="1"><thead><tr><th>CIDR</th><th>Status</th><th>Sta</th></tr></thead><tbody><tr><td>10.250.0.0/24</td><td>associated</td><td></td></tr></tbody></table> <p>IPv4 CIDR block* <input type="text" value="10.250.0.192/26"/></p>	CIDR	Status	Sta	10.250.0.0/24	associated		<p>Haga clic en el botón Create subnet.</p> <p>Configure la subred de la siguiente manera:</p> <ul style="list-style-type: none">• Name tag: proporcione un nombre de subred único. Ejemplo: <i>public-usw1b</i>• VPC: seleccione la red virtual que creó anteriormente.• Availability Zone: en nuestro diseño, queremos usar dos zonas distintas, así que use la segunda zona que eligió aquí. Ejemplo: <i>us-west-1b</i>• IPv4 CIDR block: seleccione un bloque de IP sin usar en el espacio de dirección de su VPC. Ejemplo: <i>10.250.0.192/26</i> <p>Haga clic en el botón Create.</p>
CIDR	Status	Sta					
10.250.0.0/24	associated						

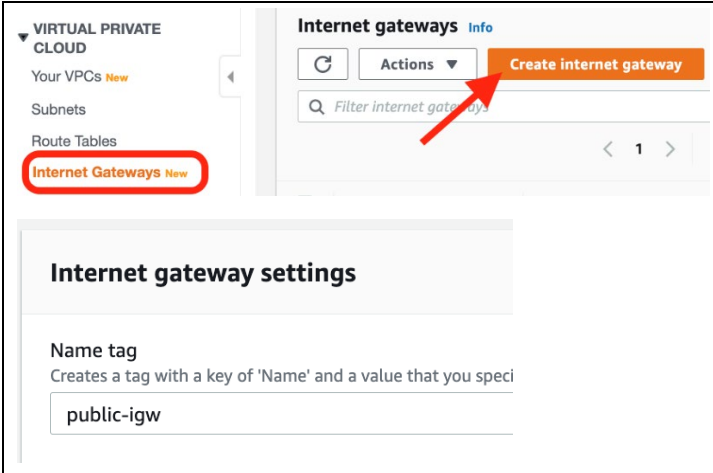
4.3.6 Revisar sus subredes

<table border="1"><thead><tr><th><input type="checkbox"/></th><th>Name</th><th>Subnet ID</th><th>State</th><th>VPC</th><th>IPv4 CIDR</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>private-usw1a</td><td>subnet-0850a...</td><td>available</td><td>vpc-0550...</td><td>10.250.0.0/26</td></tr><tr><td><input type="checkbox"/></td><td>private-usw1b</td><td>subnet-016e1...</td><td>available</td><td>vpc-0550...</td><td>10.250.0.64/26</td></tr><tr><td><input type="checkbox"/></td><td>public-usw1a</td><td>subnet-07aff7...</td><td>available</td><td>vpc-0550...</td><td>10.250.0.128/...</td></tr><tr><td><input type="checkbox"/></td><td>public-usw1b</td><td>subnet-0110cd...</td><td>available</td><td>vpc-0550...</td><td>10.250.0.192/...</td></tr></tbody></table>	<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/...	<p>Revise su lista de subredes. Ahora debería tener cuatro subredes creadas.</p>
<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/...																										

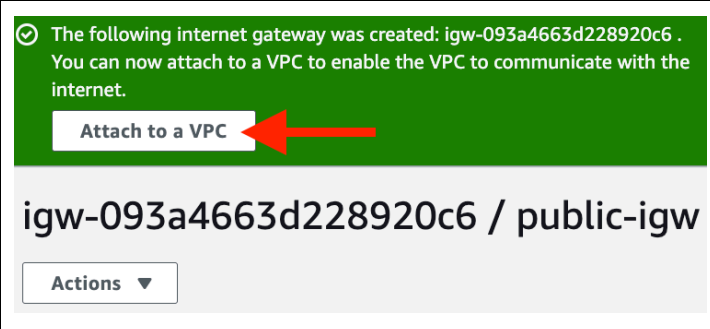
4.4 Crear una puerta de enlace a Internet para las subredes públicas

Para dirigir el tráfico de las subredes públicas a Internet, tenemos que implementar una puerta de enlace a Internet y asociarla a la VPC. Vamos a configurar el enrutamiento para la puerta de enlace en una sección posterior.

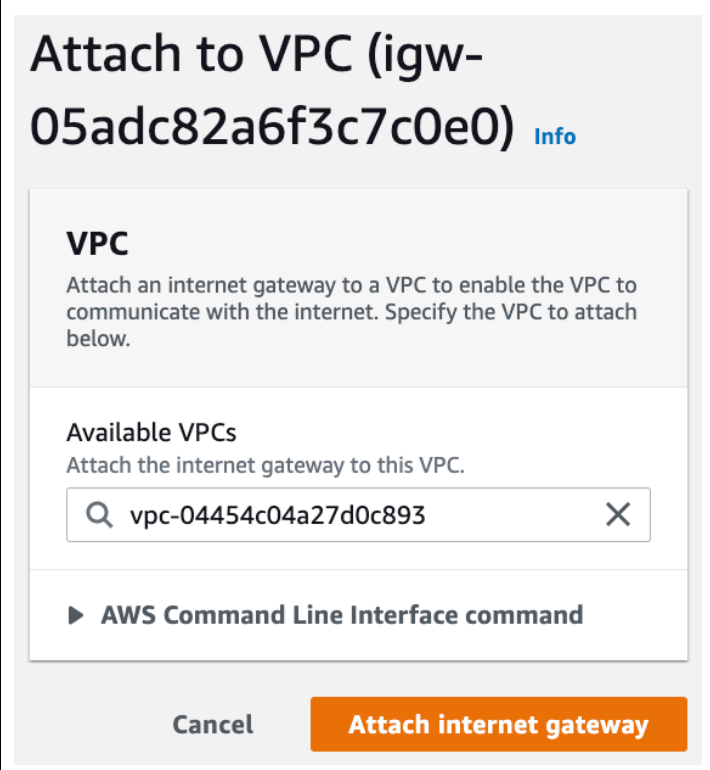
4.4.1 Crear puertas de enlace a Internet

 <p>The screenshot shows the AWS VPC console interface. On the left sidebar, 'Internet Gateways' is selected and highlighted with a red circle. In the main content area, the 'Internet gateways' section is visible, with a red arrow pointing to the 'Create internet gateway' button. Below this, the 'Internet gateway settings' section is shown, with the 'Name tag' field containing the value 'public-igw'.</p>	<p>En la barra lateral de VPC, seleccione Internet Gateways.</p> <p>Haga clic en Create Internet gateway.</p> <p>Ingrese una etiqueta de nombre. Ejemplo: <i>public-igw</i></p> <p>Haga clic en el botón Create Internet gateway en la parte inferior de la pantalla para terminar.</p>
---	---

4.4.2 Asociar la puerta de enlace a Internet a la VPC

	<p>Después de crear la puerta de enlace a Internet, se le solicitará que la asocie a una VPC. Haga clic en el botón como se indica. También puede hacer esto en el menú Actions.</p>
--	--

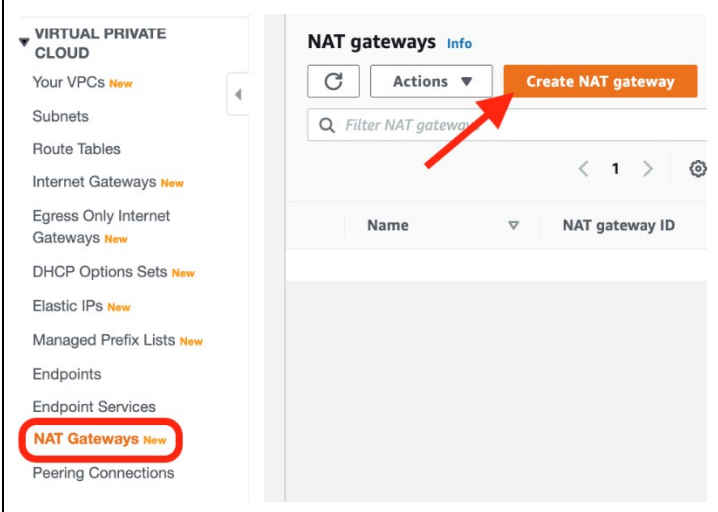
4.4.3 Ingresar los detalles de la asociación

	<p>Seleccione la VPC que creó anteriormente.</p> <p>Haga clic en el botón Attach internet gateway.</p>
---	---

4.5 Crear puertas de enlace NAT para las subredes privadas

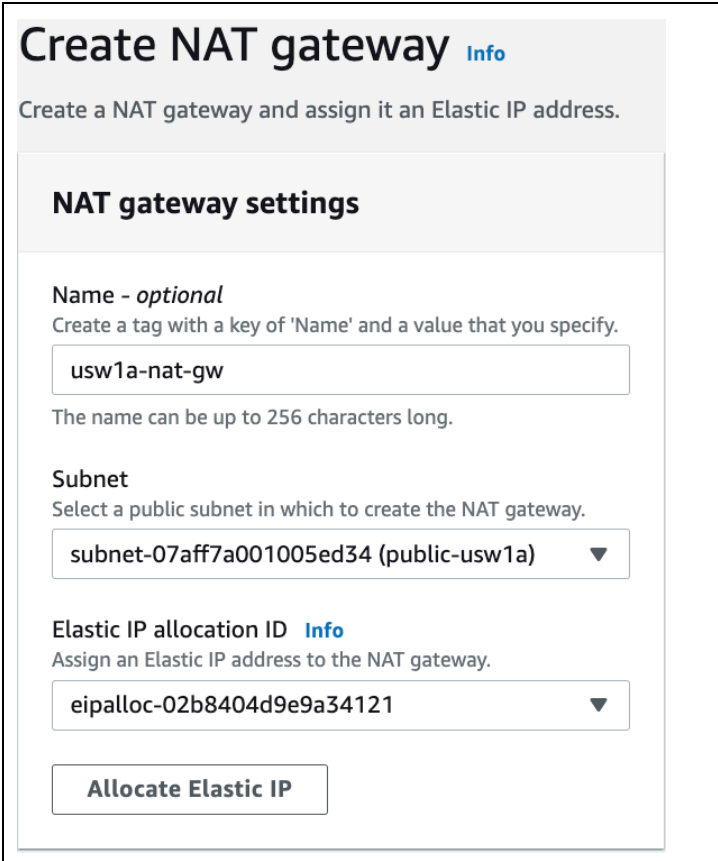
Una puerta de enlace NAT es un recurso zonal que puede usarse con los recursos de esa zona como un punto de salida del tráfico de Internet. La puerta de enlace NAT realizará la traducción de dirección y enviará el tráfico a la puerta de enlace a Internet en su VPC. Vamos a crear una puerta de enlace para cada una de nuestras dos zonas de disponibilidad, de modo que no se pierda conectividad si una de las zonas deja de funcionar.

4.5.1 Ir a las puertas de enlace NAT



En la barra lateral de VPC, seleccione **NAT Gateways**.

4.5.2 Crear la primera puerta de enlace NAT



Haga clic en el botón **Create NAT gateway**.

Configure la puerta de enlace NAT de la siguiente manera:

- **Name** (optional): ingrese un nombre único para la puerta de enlace.
Ejemplo: *usw1a-nat-gw*
- **Subnet**: seleccione la primera subred pública.
Ejemplo: *public-usw1a*
- **Elastic IP allocation ID**: haga clic en el botón Allocate Elastic IP para llenar este campo de manera automática.

Haga clic en el botón **Create NAT gateway** para terminar.

4.5.3 Crear la segunda puerta de enlace NAT

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.

Haga clic en el botón **Create NAT gateway**.

Configure la puerta de enlace NAT de la siguiente manera:

- **Name** (optional): ingrese un nombre único para la puerta de enlace.
Ejemplo: *usw1b-nat-gw*
- **Subnet**: seleccione la segunda subred pública.
Ejemplo: *public-usw1b*
- **Elastic IP allocation ID**: haga clic en el botón Allocate Elastic IP para llenar este campo de manera automática.

Haga clic en el botón **Create NAT gateway** para terminar.

4.6 Crear y configurar las tablas de rutas

Una tabla de rutas es un conjunto de reglas, llamadas rutas, que se usan para determinar hacia dónde se dirige el tráfico de red. La VPC ya incluye una tabla de rutas predeterminada que se usa para cualquier subred que no esté explícitamente asociada a una tabla de rutas. Vamos a ignorar esto y a crear tres nuevas tablas de rutas, de las cuales una se asociará a nuestras subredes públicas, y las otras dos a nuestras subredes privadas. Vamos a agregar las rutas predeterminadas a las puertas de enlace NAT y a la puerta de enlace a Internet.

4.6.1 Ir a las tablas de rutas

New VPC Experience
Tell us what you think

VPC Dashboard New

Filter by VPC:

VIRTUAL PRIVATE CLOUD

Your VPCs New

Subnets

Route Tables

Actions ▼

<input type="checkbox"/>	Name	Route Ta
<input type="checkbox"/>		rtb-01705

4.6.2 Crear la tabla de rutas para las subredes públicas

<h3>Create route table</h3> <p>A route table specifies how packets are forwarded between the subnet your VPN connection.</p> <p>Name tag <input type="text" value="public-usw-routes"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p>	<p>Haga clic en el botón Create route table.</p> <p>Configure la tabla de rutas de la siguiente manera:</p> <ul style="list-style-type: none">• Name Tag: ingrese un nombre único para la tabla de rutas. Ejemplo: <i>public-usw-routes</i>• VPC: seleccione la red virtual que creó anteriormente. <p>Haga clic en el botón Create.</p> <p>Haga clic en el botón Close.</p>
--	--

4.6.3 Crear la tabla de rutas para la primera subred privada

<p>Name tag <input type="text" value="private-usw1a-routes"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p>	<p>Haga clic en el botón Create route table.</p> <p>Configure la tabla de rutas de la siguiente manera:</p> <ul style="list-style-type: none">• Name Tag: ingrese un nombre único para la tabla de rutas. Ejemplo: <i>private-usw1a-routes</i>• VPC: seleccione la red virtual que creó anteriormente. <p>Haga clic en el botón Create.</p> <p>Haga clic en el botón Close.</p>
--	---

4.6.4 Crear la tabla de rutas para la segunda subred privada

<p>Name tag <input type="text" value="private-usw1b-routes"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p>	<p>Haga clic en el botón Create route table.</p> <p>Configure la tabla de rutas de la siguiente manera:</p> <ul style="list-style-type: none">• Name Tag: ingrese un nombre único para la tabla de rutas. Ejemplo: <i>private-usw1b-routes</i>• VPC: seleccione la red virtual que creó anteriormente. <p>Haga clic en el botón Create.</p> <p>Haga clic en el botón Close.</p>
--	---

4.6.5 Revisar la lista de tabla de rutas

<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

Verifique que la lista de tablas de rutas tenga tres entradas nuevas con las etiquetas de nombre que elija.

4.6.6 Editar las rutas para la tabla de la primera subred privada

<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

Seleccione la tabla de rutas para la primera subred privada.
Ejemplo: *private-usw1a-routes*

Seleccione la pestaña **Routes** debajo del listado.

Haga clic en el botón **Edit routes**.

Haga clic en el botón **Add route** y establezca estos valores:

- **Destination:** *0.0.0.0/0*
- **Target:** seleccione la puerta de enlace NAT que implementó en la primera zona de disponibilidad.
Ejemplo: *usw1a-nat-gw*

Haga clic en el botón **Save routes**.

Haga clic en el botón **Close**.

4.6.7 Editar las asociaciones de subred para la tabla de rutas de la primera subred privada

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

Seleccione la pestaña **Subnet Associations**.

Haga clic en el botón **Edit subnet associations**.

Seleccione la primera subred privada para asociarla a esta tabla de rutas. Si siguió los nombres de ejemplo incluidos en esta guía, será fácil asociar el nombre de la tabla de rutas a la subred.

Haga clic en el botón **Save**.

4.6.8 Editar las rutas para la tabla de la segunda subred privada

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-06c46b8e4e4ed5c32	

Add route

nat-06c46b8e4e4ed5c32 | usw1b-nat-gw

* Required Cancel Save routes

Seleccione la tabla de rutas para la segunda subred privada. Ejemplo: *private-usw1b-routes*

Seleccione la pestaña **Routes** debajo del listado.

Haga clic en el botón **Edit routes**.

Haga clic en el botón **Add route** y establezca estos valores:

- Destination:** 0.0.0.0/0
- Target:** seleccione la puerta de enlace NAT que implementó en la segunda zona de disponibilidad. Ejemplo: *usw1b-nat-gw*

Haga clic en el botón **Save routes**.

Haga clic en el botón **Close**.

4.6.9 Editar las asociaciones de subred para la tabla de rutas de la segunda subred privada

Summary Routes **Subnet Associations**

Edit subnet associations

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/...

Seleccione la pestaña **Subnet Associations**.

Haga clic en el botón **Edit subnet associations**.

Seleccione la segunda subred privada para asociarla a esta tabla de rutas. Si siguió los nombres de ejemplo incluidos en esta guía, será fácil asociar el nombre de la tabla de rutas a la subred.

Haga clic en el botón **Save**.

4.6.10 Editar las rutas para la tabla de subredes públicas

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

* Required

Cancel Save routes

Seleccione la tabla de rutas para las subredes públicas.
Ejemplo: *public-usw-routes*

Seleccione la pestaña **Routes** debajo del listado.

Haga clic en el botón **Edit routes**.

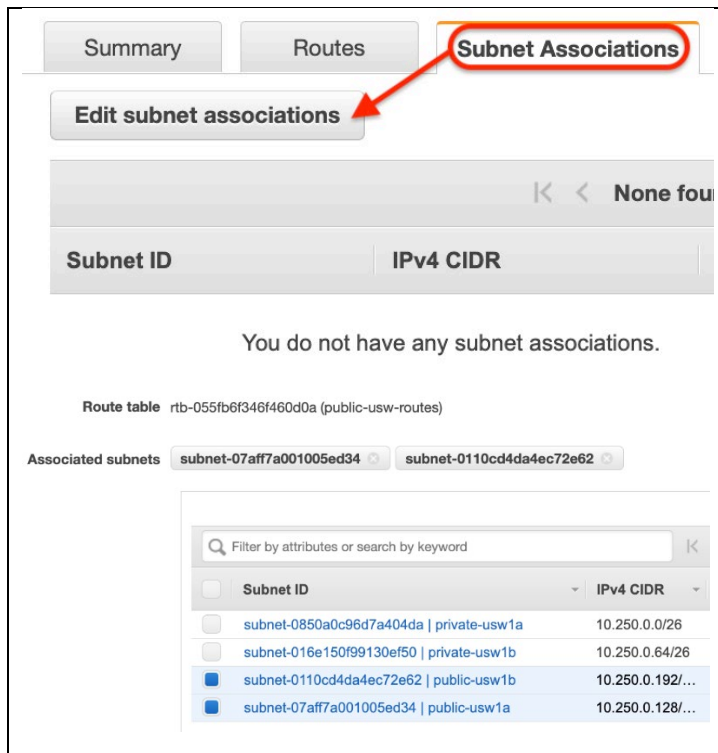
Haga clic en el botón **Add route** y establezca estos valores:

- **Destination:** *0.0.0.0/0*
- **Target:** seleccione la puerta de enlace a Internet que implementó.
Ejemplo: *public-igw*

Haga clic en el botón **Save routes**.

Haga clic en el botón **Close**.

4.6.11 Editar las asociaciones de subred para la tabla de rutas de subredes públicas



Seleccione la pestaña **Subnet Associations**.

Haga clic en el botón **Edit subnet associations**.

Seleccione las dos subredes públicas para asociarlas a esta tabla de rutas.

Haga clic en el botón **Save**.

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/...

4.7 Grupos de seguridad

Un grupo de seguridad actúa como firewall virtual para que sus instancias de máquina virtual controlen el tráfico entrante y saliente. Cuando creamos una máquina virtual (VM) más adelante, podremos asociarle uno o más grupos de seguridad en ese momento. Puede modificar las reglas de un grupo de seguridad en cualquier momento. Las reglas nuevas y modificadas se aplican automáticamente a todas las instancias asociadas al grupo de seguridad.

Cuando cree las reglas del grupo de seguridad, deberá especificar el origen y el destino. Estas se pueden expresar como una lista de redes IP o como un ID de grupo de seguridad. Cuando especifica un grupo de seguridad como origen o destino de una regla, esta afecta a todas las instancias asociadas al grupo de seguridad. Vamos a usar esta función para las implementaciones de servidores distribuidos a fin de facilitar el tráfico entre las VMs Intel® EMA sin que tenga que ser demasiado amplio y para permitir todo el tráfico dentro de la red privada, que sigue la mejor práctica de seguridad con menos privilegios.

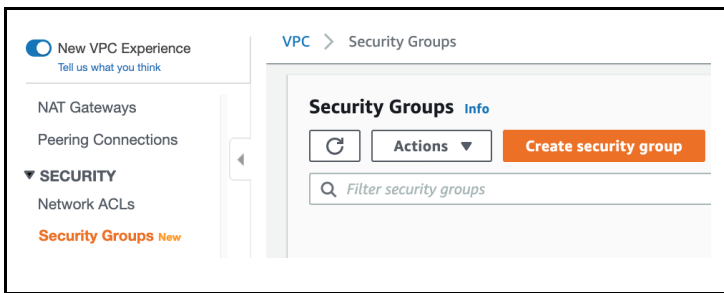
En los procedimientos que se incluyen a continuación, vamos a crear un grupo de seguridad para controlar el acceso a las VMs Intel® EMA y un grupo distinto para controlar el acceso a la base de datos.

Para obtener más información sobre los grupos de seguridad de la VPC, visite el siguiente enlace:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

4.7.1 Crear un grupo de seguridad para las VMs

Nota: algunas direcciones de origen en las imágenes de ejemplo que se incluyen a continuación serían específicas para su propio entorno de red y no deberían copiarse textualmente. En cambio, debería utilizar sus propias redes de confianza.

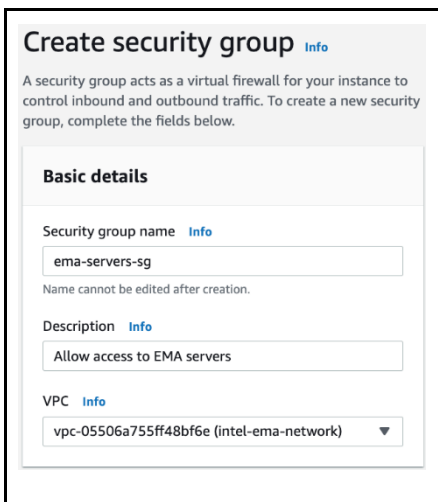
4.7.1.1 Cree un grupo de seguridad



En la barra lateral de la **VPC**, seleccione **Security Groups**.

Haga clic en el botón **Create security group**.

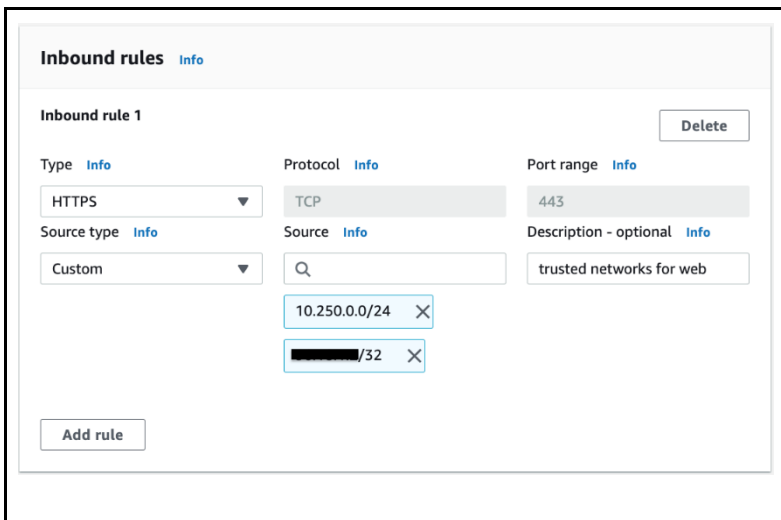
4.7.1.2 Configure los detalles básicos del grupo de seguridad



Ingrese los detalles básicos del grupo de seguridad que permitan el acceso al servidor EMA.

- **Security group name:** introduzca un nombre único.
Ejemplo: *ema-server-sg*
- **Description** (optional): ingrese una descripción para el grupo de seguridad.
Ejemplo: *Allow access to EMA servers*
- **VPC:** seleccione la VPC que creó anteriormente.

4.7.1.3 Agregue una regla de entrada para el tráfico web



Agregue una regla de entrada con la siguiente configuración.

- **Type:** *HTTPS*
- **Description:** *redes confiables para web*
- **Source:** ingrese el bloque CIDR de la VPC para permitir controles de estado.
Ejemplo: *10.250.0.0/24*
También puede ingresar redes adicionales que deberían tener permitido acceder a la IU web de EMA, como la red pública desde la cual se originaría el tráfico de su consola de servicio.

4.7.1.4 Agregue una regla de entrada para el tráfico de WebSocket

<p>Inbound rule 2 Delete</p> <p>Type Info Protocol Info Port range Info</p> <p>Custom TCP TCP 8084</p> <p>Source type Info Source Info Description - optional Info</p> <p>Custom trusted networks for websocket</p> <p>10.250.0.0/24 X</p> <p>██████████/32 X</p> <p>Add rule</p>	<p>Agregue una regla de entrada con la siguiente configuración.</p> <ul style="list-style-type: none">● Type: <i>Custom TCP</i>● Port range: <i>8084</i>● Description: <i>redes confiables para WebSocket</i>● Source: ingrese el bloque CIDR de la VPC para permitir controles de estado. Ejemplo: <i>10.250.0.0/24</i> También puede ingresar redes adicionales que deberían tener permitido acceder a la IU web de EMA, como la red pública desde la cual se originaría el tráfico de su consola de servicio.
---	---

4.7.1.5 Agregue una regla de entrada para el tráfico Swarm

<p>Type Info Protocol Info Port range Info</p> <p>Custom TCP TCP 8080</p> <p>Source type Info Source Info Description - optional Info</p> <p>Custom EMA agent traffic</p> <p>0.0.0.0/0 X</p>	<p>Agregue una regla de entrada con la siguiente configuración.</p> <ul style="list-style-type: none">● Type: <i>Custom TCP</i>● Port range: <i>8080</i>● Description: <i>tráfico de Agente EMA</i>● Source: <i>0.0.0.0/0</i>
--	--

4.7.1.6 Crear y revisar

The screenshot shows the 'Details' section of a security group. It includes the following information:

- 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

Below the details, there are tabs for 'Inbound rules', 'Outbound rules', and 'Tags'. The 'Inbound rules' tab is selected, showing a table of 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

Haga clic en el botón **Create security group** para guardar las reglas.

Revise la lista de reglas para verificar si son correctas.

Nota: hemos dejado las reglas de salida predeterminadas que permiten todo el tráfico de salida.

4.7.2 Actualizar el grupo de seguridad para permitir el tráfico entre las VMs Intel® EMA (solo para servidores distribuidos)

Ahora que creamos el grupo de seguridad ema-server-sg, haga clic en el botón **Edit inbound rules** y realice los cambios que se incluyen a continuación.

4.7.2.1 Agregue una regla de entrada para el tráfico interno de los puertos 8092-8094

The screenshot shows the configuration form for adding a new inbound rule. The fields are filled with the following values:

- Type:** Custom TCP
- Protocol:** TCP
- Port range:** 8092 - 8094
- Source type:** Custom
- Source:** sg-06acbdce6cea22f15
- Description - optional:** EMA internal

Agregue una regla de entrada con la siguiente configuración.

- **Type:** Custom TCP
- **Port range:** 8092-8094
- **Description:** EMA interno
- **Source:** haga clic en el cuadro de texto vacío y seleccione el nombre del grupo de seguridad que creó en el paso anterior.

4.7.2.2 Agregue una regla de entrada para el tráfico interno del puerto 8089

Type [Info](#)
Custom TCP

Source type [Info](#)
Custom

Protocol [Info](#)
TCP

Source [Info](#)
Q
sg-06acbdce6cea22f15

Port range [Info](#)
8089

Description - optional [Info](#)
EMA admin port

Agregue una regla de entrada con la siguiente configuración.

- **Type:** *Custom TCP*
- **Port range:** *8089*
- **Description:** *puerto de admin. de EMA*
- **Source:** haga clic en el cuadro de texto vacío y seleccione el nombre del grupo de seguridad que creó en el paso anterior.

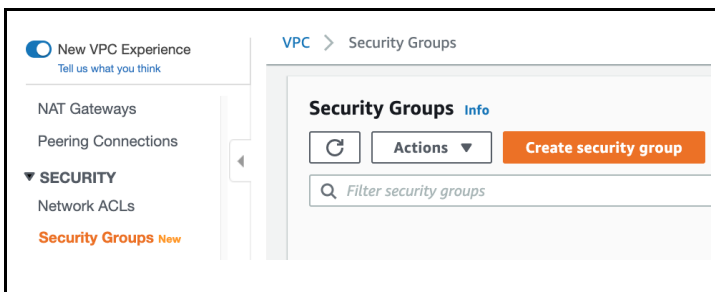
4.7.2.3 Guarde y revise la lista final para verificar si es correcta

Haga clic en el botón **Save rules**. Revise las reglas para verificar si son correctas.

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 Crear un grupo de seguridad para la base de datos

4.7.3.1 Cree un grupo de seguridad



En la barra lateral de la **VPC**, seleccione **Security Groups**.

Haga clic en el botón **Create security group**.

4.7.3.2 Configure los detalles básicos del grupo de seguridad

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

Ingrese los detalles básicos del grupo de seguridad que permitan el acceso al servidor EMA.

- **Security group name:** introduzca un nombre único.
Ejemplo: *ema-db-sg*
- **Description** (optional): ingrese una descripción para el grupo de seguridad.
Ejemplo: *Allow traffic from EMA server(s) to the database*
- **VPC:** seleccione la VPC que creó anteriormente.

4.7.3.3 Agregue una regla de entrada para MSSQL

Inbound rules Info

Inbound rule 1

Type Info

Source type Info

Security Groups

- sg-03661abff0a38ee50

Agree una regla de entrada con la siguiente configuración.

- **Type:** *MSSQL*
- **Source:** haga clic en el cuadro de texto vacío y seleccione el grupo de seguridad para los servidores EMA que creó anteriormente.

4.7.3.4 Crear y revisar

Haga clic en el botón **Create security group**. Revise la lista de reglas para verificar si son correctas.

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

5 Implementación de la máquina virtual

5.1 Descripción general

Amazon Elastic Compute Cloud* (Amazon EC2) le ofrece la flexibilidad de la virtualización informática sin tener que comprar ni mantener el hardware físico que la ejecuta. No obstante, usted sigue siendo responsable de mantener el sistema operativo huésped y el software que se ejecuta en él.

Usted decidirá la cantidad de CPU, memoria y almacenamiento que se asignará a la instancia de EC2 al momento de crearla, pero puede aumentar todas estas variables más tarde o disminuir la cantidad de CPU y memoria, lo que le permitirá optimizar la VM para la carga de trabajo a fin de reducir costos.

EC2 asegura los inicios de sesión para sus instancias mediante pares de claves EC2 (AWS almacena la clave pública y usted almacena la clave privada en un lugar seguro). Esto se puede generar antes o durante la creación de la instancia de EC2. Necesitará la clave privada para recuperar las credenciales de administrador generadas automáticamente para una instancia basada en Windows. Puede tener varios pares de claves en EC2, pero solo puede asociar una instancia a un par y no puede cambiar esto después de haberse creado la instancia.

El acceso de red a sus instancias de EC2 se puede asegurar asociando uno o más grupos de seguridad, ya sea cuando se crea la instancia o en cualquier momento posterior. Los grupos de seguridad que necesitamos ya se configuraron en una sección anterior.

En el procedimiento que se muestra a continuación, y en otras secciones, se incluyen pasos adicionales para las implementaciones de servidores distribuidos que se pueden omitir para las de servidor único. Estos incluyen crear una segunda VM, asociar las VMs a un grupo de destinos, asociar este grupo al equilibrador de carga y configurar las reglas de reenvío del equilibrador de carga.

Para obtener más información sobre las instancias de EC2 o los pares de claves, visite los siguientes enlaces:

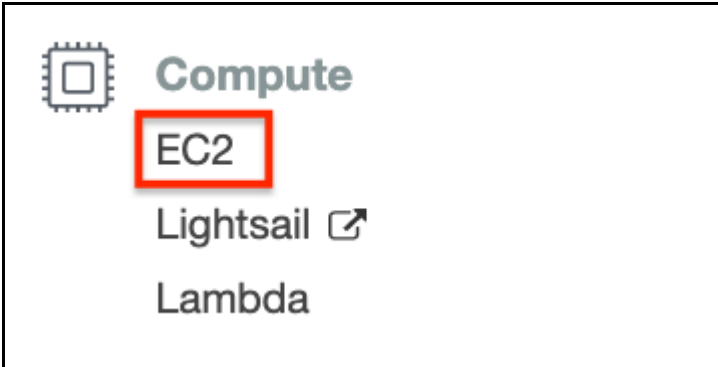
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html>

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

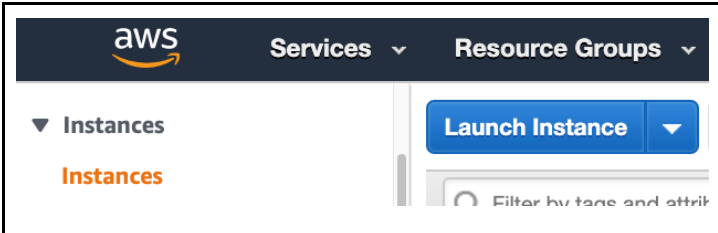
5.2 Crear máquinas virtuales

Siga el procedimiento que se incluye a continuación a fin de crear una instancia de EC2 para el servidor Intel® EMA utilizando la imagen más reciente del servidor de Windows y también asociar el grupo de seguridad que creamos anteriormente.

5.2.1 Ir al servicio EC2

	En el menú Services , en la sección Compute , seleccione EC2 .
--	---

5.2.2 Iniciar una instancia de EC2

	Seleccione Instances en la barra lateral y haga clic en el botón Launch Instance .
--	--

5.2.3 Seleccionar una imagen de máquina de Amazon

Step 1: Choose an Amazon Machine Image (AMI) Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select your own AMIs.

Q Windows Server | Search by Systems Manager param

AWS Launch Wizard for SQL Server offers an easy way to size, configure, and deploy Microsoft SQL Server Always On availability groups. [Use AWS Launch Wizard for this launch](#)

Quick Start (19) 1 to 19 of 19 AMIs

- My AMIs (0)
- AWS Marketplace (393)
- Community AMIs (2144)

Windows
Free tier eligible

Microsoft Windows Server 2019 Base - ami-0d1b8b740ddc3b78d **Select**

Microsoft Windows 2019 Datacenter edition. [English] 64-bit (x86)

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Busque la imagen de Microsoft Windows* Server Base compatible con Intel® EMA.

Consulte la Guía de instalación del servidor de Intel® Endpoint Management Assistant para conocer los sistemas operativos admitidos.

Haga clic en el botón **Select**.

5.2.4 Seleccionar el tipo de máquina

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Stor

Step 2: Choose an Instance Type

Filter by: **General purpose** **Current generation** Show/Hi

Currently selected: t3a.large (Variable ECUs, 2 vCPUs, 2.2 GHz, AMD EPYC)

	Family	Type	vCPUs	Memory (GiB)
<input type="checkbox"/>	General purpose	t2.nano	1	0.5
<input type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1
<input type="checkbox"/>	General purpose	t2.small	1	2
<input type="checkbox"/>	General purpose	t2.medium	2	4
<input type="checkbox"/>	General purpose	t2.large	2	8

Seleccione el tipo de máquina con la cantidad de recursos de CPU y memoria que necesita. Puede cambiar esto más tarde cuando se apaga la instancia, si es necesario.

Consulte la Guía de instalación del servidor Intel® Endpoint Management Assistant para conocer los requisitos del sistema.

Haga clic en el botón **Next: Configure Instance Details**.

5.2.5 Configurar los detalles de la instancia

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. 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 [Launch into Auto Scal](#)

Purchasing option Request Spot instances

Network No default VPC found. [Create a new default VPC](#).

Subnet 59 IP Addresses available

Auto-assign Public IP

Configure los detalles de la instancia de la siguiente manera:

- **Network:** establezca esta opción en la VPC que creó anteriormente. Ejemplo: *intel-ema-network*
- **Subnet:** seleccione una de las subredes privadas. Ejemplo: *private-usw1a*
- **Auto-assign Public IP:** *Disable*

El resto de los detalles de la instancia en esta pantalla se puede dejar en los valores predeterminados.

Haga clic en el botón **Next: Add Storage**.

5.2.6 Agregar almacenamiento

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

La configuración del almacenamiento se puede dejar en los valores predeterminados, a menos que necesite más espacio. Consulte la Guía de instalación del servidor de Intel® Endpoint Management Assistant para conocer los requisitos del sistema.

Haga clic en el botón **Next: Add Tags**.

5.2.7 Agregar etiquetas

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"/>

Agregue una etiqueta con la clave "Name" y un valor del nombre del servidor que busca.

Agregue las etiquetas personalizadas adicionales que desee para ayudarse a organizar los recursos, como se comentó antes en la sección Etiquetas y grupos de recursos.

Haga clic en el botón **Next: Configure Security Group**.

5.2.8 Configurar el grupo de seguridad

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, you can allow 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-06acbdc6cea22f15	ema-servers-sg	Allow access to EMA servers

Establezca el botón de opción **Assign a security group** en *Select an existing security group*.

Seleccione el grupo de seguridad que creó anteriormente para los servidores de Intel® EMA. Ejemplo: *ema-servers-sg*

Haga clic en el botón **Next: Review and Launch**.

Es posible que reciba una advertencia en la que le informen que no podrá conectarse a la instancia porque el grupo de seguridad no tiene un puerto 3389 (RDP) abierto. Puede ignorar ese mensaje y continuar, ya que tenemos otra forma de acceder a la máquina virtual.

5.2.9 Revisar el lanzamiento de la instancia

Revise los detalles de la instancia y luego haga clic en el botón **Launch**.

5.2.10 Seleccionar un par de claves de EC2

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**

Se le solicitará que seleccione un par de claves existente o que cree uno nuevo.

Seleccione el par de claves apropiado en la lista, o bien use la opción para crear uno nuevo y haga clic en el botón **Download Key Pair** para guardar el archivo de claves privadas en su equipo.

Si elige usar un par de claves existente, debe tener acceso al archivo de claves privadas.

Haga clic en el botón **Launch Instances**.

5.3 Crear una segunda instancia de EC2 (solo para servidores distribuidos)

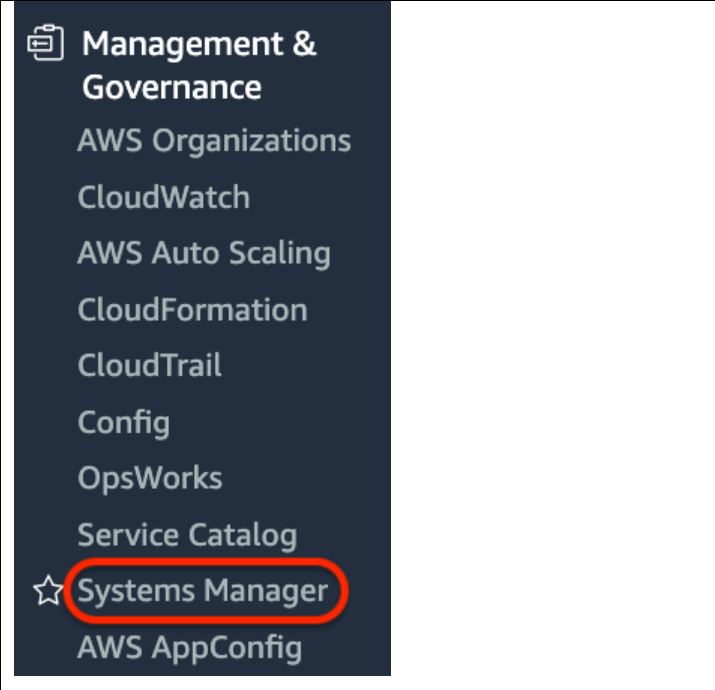
Para las implementaciones de servidores distribuidos, repita el procedimiento anterior para crear el segundo servidor de Intel® EMA mediante la selección de una subred diferente y una etiqueta de nombre diferente, como *ema-server-2*.

6 Configurar AWS Systems Manager (solo para servidores distribuidos)

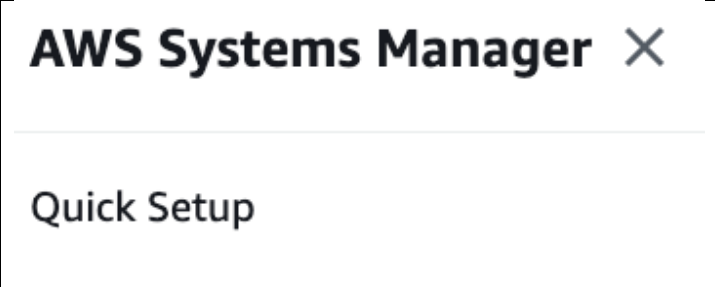
AWS Systems Manager es un servicio que ofrece mayor visibilidad y control de su infraestructura en AWS. Debemos habilitar este servicio para usar el componente Session Manager, el cual nos permitirá tener un acceso remoto a nuestras VMs que no tengan una dirección IP pública.

Para obtener más información sobre Systems Manager, visite el siguiente enlace: <https://aws.amazon.com/systems-manager/>

6.1 Ir al servicio Systems Manager

 <p>Management & Governance</p> <ul style="list-style-type: none">AWS OrganizationsCloudWatchAWS Auto ScalingCloudFormationCloudTrailConfigOpsWorksService Catalog★ Systems ManagerAWS AppConfig	<p>En el menú Services, en la sección Management & Governance, seleccione Systems Manager.</p>
--	--

6.2 Comenzar la configuración rápida

 <p>AWS Systems Manager ✕</p> <hr/> <p>Quick Setup</p>	
---	--

6.3 Seleccionar las opciones de permisos

Quick Setup Info

Configure required security roles and commonly used Systems Manager capabilities.

Permissions (Required)

Use the following options to configure two roles that give Systems Manager permission to access your instances and run commands on them.

Instance profile role

Use the default role

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.

Choose an existing role

Uses an existing instance profile. The instance profile must contain the required permissions policy. Choose the instance profile from the following list.

Assume role for Systems Manager

Use the default role

Quick Setup creates a new assume role that enables Systems Manager to securely run commands on your instances.

Choose an existing role

Uses an existing service role. The role must contain the required permissions policy. Choose the role from the following list

6.4 Seleccionar las opciones de configuración

Configuration options

Quick Setup configures the following Systems Manager components based on best practices. Select the check boxes for actions you want to schedule. [Learn more](#)

- Update Systems Manager (SSM) Agent every two weeks
- Collect inventory from your instances every 30 minutes
- Scan instances for missing patches daily
- Install and configure the CloudWatch agent
- Update the CloudWatch agent once every 30 days

If you run Quick Setup, [Systems Manager Explorer](#) is enabled.

Learn more about the metrics included in [the CloudWatch agent's basic configuration](#) and Amazon CloudWatch [pricing](#).

6.5 Seleccionar los destinos

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 Verificar la lista de instancias gestionadas

AWS Systems Manager > Managed Instances

Managed Instances Settings

Managed instances

Instance ID	Name	Ping status	Platform type	Platform name	Platform version	Agent version	IP address	Computer name	Association status
<input type="radio"/> i-0a6a82fc33afa0c7f	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-8BHE25G.WORKGROUP	Success

En la barra lateral de Systems Manager, seleccione Managed Instances.

Es posible que sus máquinas virtuales tarden unos minutos en aparecer en esta lista después de ejecutar la configuración rápida por primera vez.

Cuando sus VMs se hayan registrado con éxito en Systems Manager, las verá aquí.

6.7 Iniciar sesión en sus máquinas virtuales a través de Session Manager

Usar Session Manager a través de la consola de AWS solo le permitirá conectarse a una sesión de Powershell* en la VM. Para establecer conexión con el RDP, tenemos que invocar al administrador de sesiones desde una línea de comandos local mediante la interfaz de línea de comandos (CLI) de AWS y pasarle una opción para permitir el reenvío de puertos.

La instalación de la CLI de AWS está fuera del alcance de este documento. Consulte <https://aws.amazon.com/cli/> para obtener más información.

Cuando la CLI esté instalada y configurada, y sus VMs empiecen a aparecer en AWS Systems Manager, puede ejecutar un comando de la CLI con esta sintaxis:

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

Reemplace <instanceId> con el Id. de la instancia de EC2 a la que desee conectarte. Ejemplo: i-06364ced48ee5bb96

Si este comando tiene éxito, podrá utilizar un cliente de escritorio remoto para conectarlo al host local en el número de puerto local que específico. Luego, puede iniciar sesión con las credenciales para esa VM.

7 Implementación de Relational Database Service (RDS)

AWS tiene un motor de base de datos de plataforma como servicio totalmente administrado, que se denomina Amazon Relational Database Service (Amazon RDS). Este motor permite configurar, utilizar y escalar fácilmente una base de datos relacional en la nube de AWS. Proporciona una capacidad adaptable sumamente rentable y permite gestionar tareas comunes de administración de base de datos, como copias de seguridad, parches de software, detección automática de errores y recuperación.

El módulo básico de Amazon RDS es la instancia de DB. Esta instancia es un entorno de base de datos aislado en la nube de AWS. Su instancia de DB puede contener varias bases de datos creadas por el usuario. Puede acceder a la instancia de DB mediante las mismas herramientas y aplicaciones que utiliza con una instancia de base de datos independiente. La capacidad de cálculo y memoria de una instancia de DB es determinada por su clase de instancia de DB. Puede seleccionar la instancia de DB que mejor se ajuste a sus necesidades. Si sus necesidades cambian con el tiempo, puede cambiar las instancias de DB.

Dado que nuestra VPC se creó con varias subredes en diferentes zonas de disponibilidad, podremos lanzar una instancia de RDS con una opción llamada implementación Multi-AZ. Al elegir esta opción para nuestra implementación de producción, su instancia de DB principal se replica de forma automática y sincronizada en una instancia de DB secundaria en espera en una zona de disponibilidad diferente. Este enfoque ayuda a proporcionar compatibilidad con la redundancia de datos y la conmutación por error, elimina los bloqueos de E/S y minimiza los picos de latencia durante la copia de seguridad del sistema. Vamos a crear un grupo de subredes de base de datos que informará a RDS qué zonas de disponibilidad usar para este fin.


Un grupo de seguridad que creamos anteriormente en esta guía se usará para controlar el acceso a la instancia de RDS y para permitir que solo nuestras instancias de EC2 de Intel® EMA se conecten con ella.

Para obtener más información sobre RDS, visite el siguiente enlace:

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

Siga este procedimiento para crear una instancia de Relational Database Service (RDS) y asociar el grupo de seguridad que se creó anteriormente para permitir el tráfico de las instancias de EC2 de Intel® EMA a la base de datos.

7.1 Navegación al servicio RDS

	En el menú Services , en Database , seleccione RDS .
---	---

7.2 Crear un grupo de subredes de base de datos

	En la barra lateral de RDS , seleccione Subnet groups y, a continuación, haga clic en el botón Create DB Subnet Group .
--	--

7.2.1 Detalles del grupo de subredes

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

Ingrese los detalles del grupo de subredes de la siguiente manera.

- **Name:** introduzca un nombre único.
Ejemplo: *ema-db-subnet-group*
- **Description** (opcional)
Ejemplo: *identifique subredes para usar con la instancia DB de EMA*
- **VPC:** seleccione la VPC que creó anteriormente.
- **Availability Zones:** seleccione las dos zonas en las que creó las subredes.
- **Subnets:** seleccione las dos subredes privadas que se crearon anteriormente.

Haga clic en el botón **Create**.

7.3 Crear una base de datos

Amazon RDS X

RDS > Databases

Databases







Group resources

En la barra lateral de RDS, selecciona Databases y, a continuación, haga clic en el botón **Create database**.

7.3.1 Seleccionar el método de creación de la base de datos

<p>Create database</p> <p>Choose a database creation method Info</p> <p><input checked="" type="radio"/> Standard Create You set all of the configuration options, including ones for availability, security, backups, and maintenance.</p> <p><input type="radio"/> Easy Create Use recommended best-practice configurations. Some configuration options can be changed after the database is created.</p>	<p>Seleccione el método de creación de la base de datos Standard Create.</p>
--	---

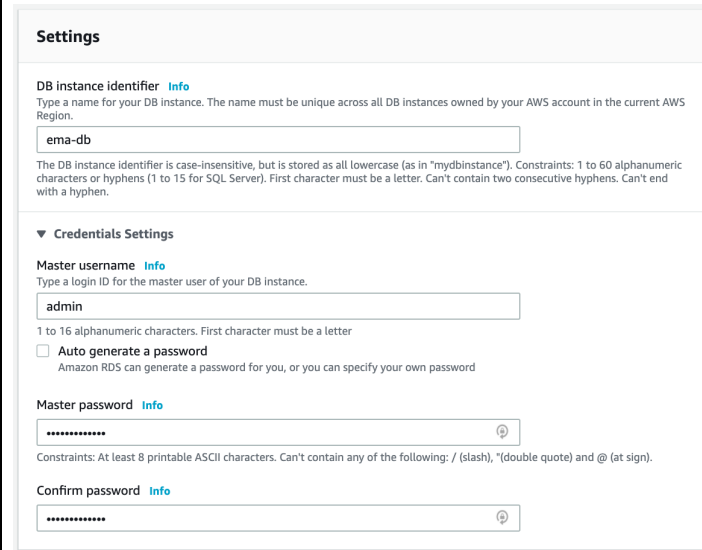
7.3.2 Seleccionar el tipo y la edición del motor

<p>Engine options</p> <p>Engine type Info</p> <p><input type="radio"/> Amazon Aurora </p> <p><input type="radio"/> MySQL </p> <p><input type="radio"/> MariaDB </p> <p><input type="radio"/> PostgreSQL </p> <p><input type="radio"/> Oracle </p> <p><input checked="" type="radio"/> Microsoft SQL Server </p> <p>Edition</p> <p><input type="radio"/> SQL Server Express Edition Affordable database management system that supports database sizes up to 10 GB.</p> <p><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.</p> <p><input checked="" type="radio"/> SQL Server Standard Edition Core data management and business intelligence capabilities for mission-critical applications and mixed workloads.</p> <p><input type="radio"/> SQL Server Enterprise Edition Comprehensive high-end capabilities for mission-critical applications with demanding database workloads and business intelligence requirements.</p> <p>Version Info</p> <p>SQL Server 2017 14.00.3281.6.v1</p> <p>License license-included</p>	<p>Seleccione el motor Microsoft SQL Server.</p> <p>Seleccione la edición apropiada del servidor SQL. En lo que respecta a esta documentación, suponemos una implementación de producción con la edición SQL Server Standard. La edición SQL Server Express podría usarse para las etapas de desarrollo y prueba a fin de reducir costos.</p>
---	--

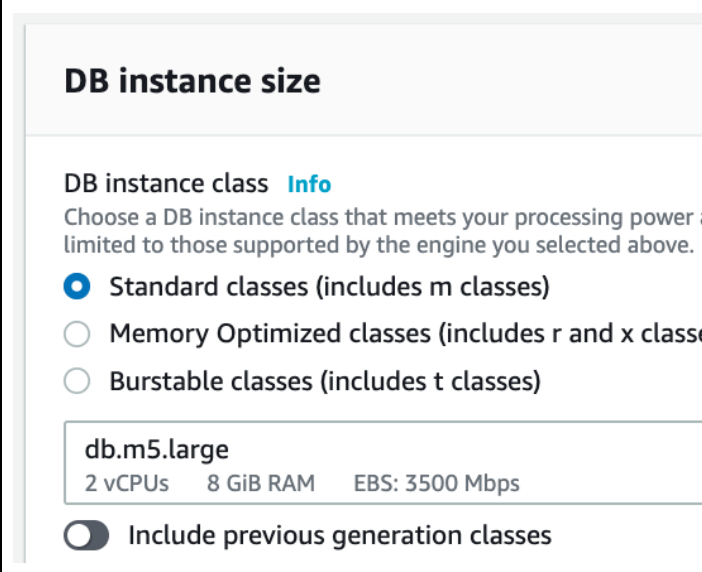
7.3.3 Seleccionar la plantilla de implementación

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

7.3.4 Configurar el nombre de la instancia y las credenciales del usuario maestro

 <p>Settings</p> <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> <p>ema-db</p> <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> <p>admin</p> <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> <p>*****</p> <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> <p>*****</p>	<p>Asigne un nombre único para la base de datos. Ejemplo: <i>ema-db</i></p> <p>Cree un nombre de usuario y una contraseña.</p>
--	--

7.3.5 Configurar el tamaño de la instancia de DB

 <p>DB instance size</p> <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> <ul style="list-style-type: none"><input checked="" type="radio"/> Standard classes (includes m classes)<input type="radio"/> Memory Optimized classes (includes r and x classes)<input type="radio"/> Burstable classes (includes t classes) <p>db.m5.large 2 vCPUs 8 GiB RAM EBS: 3500 Mbps</p> <p><input type="checkbox"/> Include previous generation classes</p>	<p>Establezca la clase de instancia de DB para proporcionar los recursos adecuados. Sugerencia: <i>db.m5.large</i></p>
---	--

7.3.6 Configurar el almacenamiento (opcional)

Puede aumentar la cantidad predeterminada del almacenamiento que se asigne según sus necesidades. Ahora, dejaremos el valor predeterminado. Podrá aumentar la capacidad de almacenamiento más adelante.

7.3.7 Configurar la conectividad

<p>Connectivity</p> <p>Virtual private cloud (VPC) Info VPC that defines the virtual networking environment for this DB instance.</p> <p>intel-ema (vpc-001161d1e7e50afb2) ▼</p> <p>Only VPCs with a corresponding DB subnet group are listed.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"><p>ⓘ After a database is created, you can't change the VPC selection.</p></div> <p>▶ Additional connectivity configuration</p>	<p>En Connectivity, seleccione la VPC que creó anteriormente y, a continuación, expanda la sección Additional connectivity configuration.</p>
--	---

7.3.8 Configurar la conectividad (configuración adicional)

<p>▼ Additional connectivity configuration</p> <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> <p><input checked="" type="radio"/> Choose existing Choose existing VPC security groups</p> <p><input type="radio"/> Create new Create new VPC security group</p> <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>	<p>Seleccione el grupo de subredes de base de datos que creó anteriormente.</p> <p>Anule la selección del grupo de seguridad de la VPC predeterminado y elija el que creó anteriormente para la base de datos.</p>
---	--

7.3.9 Revisar y crear

<p>Estimated monthly costs</p> <table><tr><td>DB instance</td><td>735.11 USD</td></tr><tr><td>Storage</td><td>2.76 USD</td></tr><tr><td>Provisioned IOPS</td><td>110.00 USD</td></tr><tr><td>Total</td><td>847.87 USD</td></tr></table> <p>This billing estimate is based on on-demand usage as described in Amazon RDS Pricing. Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.</p> <p>Estimate your monthly costs for the DB Instance using the AWS Simple Monthly Calculator.</p> <p><small>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.</small></p> <p>Cancel Create database</p>	DB instance	735.11 USD	Storage	2.76 USD	Provisioned IOPS	110.00 USD	Total	847.87 USD	<p>Revise el costo estimado y, luego, haga clic en el botón Create database.</p>
DB instance	735.11 USD								
Storage	2.76 USD								
Provisioned IOPS	110.00 USD								
Total	847.87 USD								

7.4 Obtener el nombre del host de la base de datos

<p>Connectivity & security Monitoring</p> <hr/> <p>Connectivity & security</p> <p>Endpoint & port</p> <p>Endpoint</p> <p>ema-db.creq7zxsavq4.us-west-1.rds.amazonaws.com</p> <p>Port</p> <p>1433</p>	<p>Una vez que la base de datos haya terminado de implementarse, la página de detalles mostrará el nombre del host de base de datos que usará para configurar el software Intel® EMA durante el proceso de instalación.</p>
---	---

8 Implementación del equilibrador de cargas (solo para servidores distribuidos)

8.1 Descripción general

Un equilibrador de carga de red AWS es un equilibrador de capa 4 (TCP) que distribuye el tráfico del usuario en múltiples instancias de sus aplicaciones. Al distribuir la carga, el equilibrador reduce el riesgo de que sus aplicaciones se sobrecarguen, disminuyan la velocidad o se vuelvan disfuncionales. Después de que el equilibrador de carga reciba una solicitud de conexión, seleccione un destino en buen estado de un grupo de destinos asociado de acuerdo con las reglas de reenvío y reenvíe la conexión a ese destino.

Un *objeto de escucha* comprueba las solicitudes de conexión de los clientes con el protocolo y el puerto que configure y reenvía solicitudes a un grupo de destinos.

Cada *grupo de destino* dirige las solicitudes a uno o más destinos registrados, como las instancias de EC2, con el protocolo y el número de puerto que especifique. Puede configurar los controles de estado de cada grupo de destinos. Los controles de estado se realizan en todos los destinos que se encuentren registrados en un grupo de destinos especificado en una regla de objeto de escucha para su equilibrador de carga.

Vamos a habilitar varias zonas de disponibilidad para los equilibradores de carga que implementemos para que podamos dirigir el tráfico a los destinos en cualquiera de las zonas.

El equilibrador de carga tendrá un nombre de host generado automáticamente que indicará las direcciones de acceso público de los equilibradores de carga relacionados en cada zona de disponibilidad. Se recomienda crear un registro DNS CNAME que cree un alias para ese nombre de host con el fin de usar su dominio personalizado y llegar a los servidores de Intel® EMA.

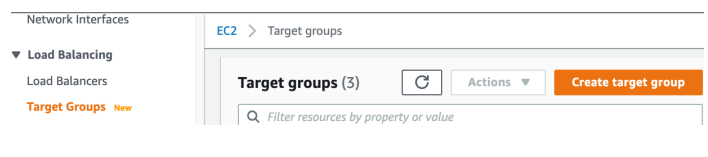
Existen otras posibilidades de configuración del equilibrador de carga que no se explican en este documento. Consulte con su departamento de TI para conocer los requisitos o las prácticas que necesitan que implemente. Para obtener más información sobre los equilibradores de carga en AWS, visite el siguiente enlace:

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

8.2 Crear grupos de destinos

Siga este procedimiento para crear un grupo de destinos para cada puerto TCP que atenderá nuestro equilibrador de carga, crear controles de estado y registrar nuestras máquinas virtuales para recibir tráfico en cada grupo de destinos.

8.2.1 Crear grupos de destinos

	<p>En la barra lateral de EC2, en Load Balancing, seleccione Target Groups.</p> <p>Haga clic en el botón Create target group.</p>
--	---

8.2.2 Configurar un grupo de destinos para TCP/443

<p>Target group name</p> <input type="text" value="ema-web"/> <p>Up to 32 alphanumeric characters, including hyphens and periods.</p> <p>Protocol : Port</p> <p>TCP ▼ : 443</p> <p>VPC</p> <p>Select the VPC containing the instances you want to register.</p> <input type="text" value="intel-ema-network"/> <p>vpc-05506a755ff48bf6e IPv4: 10.250.0.0/24</p> <p>Health checks</p> <p>The associated load balancer will use the health check protocol you select here.</p> <p>Health check protocol</p> <p>TCP ▼</p>	<p>Configure el grupo de destinos de la siguiente manera:</p> <ul style="list-style-type: none">• Target type: <i>Instances</i>• Target group name: introduzca un nombre único. Ejemplo: <i>ema-web</i>• Protocol: <i>TCP</i>• Port: <i>443</i>• VPC: seleccione la VPC que creó anteriormente.• Health check protocol: <i>TCP</i> <p>Haga clic en Next para avanzar a la pantalla Register targets.</p>
---	---

8.2.2.1 Registre ambas instancias de EC2 como destinos

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-Of180ebc233227eda	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
×	Pending	i-00f8db1dd6650c6c8	ema-server-1	443	running	ema-servers-sg
×	Pending	i-Of180ebc233227eda	ema-server-2	443	running	ema-servers-sg

2 pending

Cancel Previous **Create target group**

Seleccione ambas instancias de VM de EMA y haga clic en el botón **Include as pending below**.

Haga clic en el botón **Create target group**.

8.2.3 Crear o configurar un destino para TCP/8084

Repita los pasos anteriores en otro grupo de destinos denominado "ema-websocket" para TCP/8084.

8.2.4 Configurar un destino para TCP/8080

Repita los pasos anteriores en otro grupo de destinos denominado "ema-swarm" para TCP/8080.

8.2.5 Revisar los grupos de destinos

Verifique que haya creado tres grupos de destinos.

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 Habilitar la permanencia para el grupo de destinos TCP/443

8.2.6.1 Detalles del grupo de destinos

Attributes

Stickiness
Disabled

Deregistration delay
300 seconds

Slow start duration
0 seconds

Load balancing algorithm
Round robin

Edit

Haga clic en el nombre del grupo de destinos *ema-web* para acceder a la pantalla de detalles del grupo.

En la sección **Attributes**, haga clic en el botón **Edit**.

8.2.6.2 Editar atributos

	<p>Habilite el indicador Stickiness.</p> <p>Haga clic en el botón Save changes.</p>
---	---

8.2.7 Habilitar la permanencia para el grupo de destinos TCP/8084

Repita las instrucciones anteriores a fin de habilitar la permanencia para el grupo de destinos ema-websocket (TCP/8084).

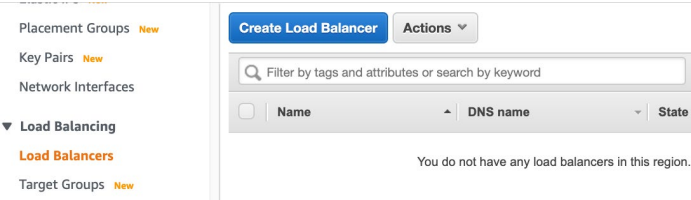
8.2.8 Nota sobre la supervisión del estado del grupo de destinos

En cualquiera de los grupos de destinos, puede revisar las pestañas **Targets** y **Monitoring** para ver los controles de estado de las instancias de destino. Al principio, esos controles de estado no serán satisfactorios hasta que se haya instalado el software Intel® EMA.

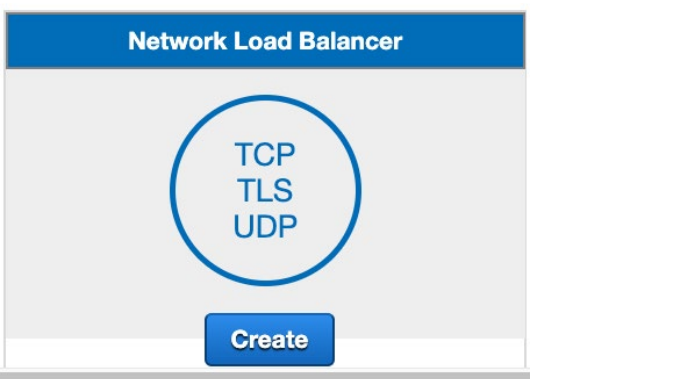
8.3 Crear un equilibrador de carga de red para el tráfico web

Siga este procedimiento para crear un equilibrador de carga de red a fin de distribuir el tráfico a los grupos de destinos en buen estado.

8.3.1 Crear el equilibrador de carga

	<p>En la barra lateral de EC2, en Load Balancing, seleccione Load Balancers y haga clic en Create Load Balancer.</p>
---	--

8.3.2 Seleccionar el tipo de equilibrador de carga

	<p>Haga clic en el botón Create en el encabezado Network Load Balancer.</p>
---	---

8.3.3 Configurar el equilibrador de carga

8.3.3.1 Configuración básica

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Routing

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives TCP traffic on port 80.

Name ⓘ

Scheme ⓘ internet-facing internal

Ingrese la configuración básica.

Name: introduzca un nombre único.
Ejemplo: *ema-web-balancer*

Scheme: internet-facing.

Nota: si su organización tiene una VPN de sitio a sitio, en la que AWS le otorga acceso a una IP privada, este podría ser un enlace del equilibrador de carga interno a las subredes privadas.

En esta guía, suponemos que no tiene un acceso de este tipo, por lo que será un enlace del equilibrador de carga con acceso a Internet a subredes públicas.

8.3.3.2 Objetos de escucha

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port	
TCP	443	✕
TCP	8084	✕

En la sección **Listeners**, agregue los objetos de escucha para estos protocolos y puertos.

- TCP 443
- TCP 8084

8.3.3.3 Zonas de disponibilidad

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.

[Create and manage Elastic IPs in the VPC console](#)

VPC ⓘ

Availability Zones

us-west-1a

IPv4 address ⓘ

us-west-1b

IPv4 address ⓘ

Configure la sección **Availability Zones** de la siguiente manera:

- **VPC:** seleccione la VPC que creó anteriormente.
- **Availability Zones:** habilite ambas zonas de disponibilidad y seleccione ambas subredes públicas. La dirección IPv4 debería establecerse en *Assigned by AWS*.

Haga clic en el botón **Next: Configure Security Settings**.

8.3.3.4 Configurar la seguridad

No hay nada para configurar en este paso. Haga clic en el botón **Next: Configure Routing**.

8.3.3.5 Configurar el enrutamiento

Step 3: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol health checks on the targets using these health check settings. Note that each target balancer.

Target group

Target group ⓘ Existing target group

Name ⓘ ema-web

Target type Instance
 IP

Protocol ⓘ TCP

Port ⓘ 443

Health checks

Protocol ⓘ TCP

En el **Step 3: Configure Routing**, configure el grupo de destinos de la siguiente manera.

- **Target group:** *Existing target group*
- **Name:** seleccione el nombre del grupo de destinos TCP/443 que creó anteriormente.
Ejemplo: *ema-web*

Haga clic en el botón **Next: Register Targets**.

8.3.3.6 Registrar los destinos

Step 4: Register Targets

Configure Security Groups

The security groups for your instances must allow traffic from the VPC CIDR on the health check port.

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

The following targets are registered with the target group that you selected. You can only modify this list after you create the load balancer.

Instance	Port
i-06364ced48ee5bb96	443
i-0a6a82fc33afa0cf7	443

[Cancel](#) [Previous](#) [Next: Review](#)

Verifique que vea dos instancias en la lista como destinos registrados.

Haga clic en el botón **Next: Review**.

8.3.3.7 Revisar

En el **Step 5: Review**, verifique que la configuración se vea similar al ejemplo proporcionado aquí y, luego, haga clic en el botón **Create**.

Step 5: Review

Please review the load balancer details before continuing

▼ Load balancer [Edit](#)

Name	ema-web-balancer
Scheme	internet-facing
Listeners	Port:443 - Protocol:TCP Port:8084 - Protocol:TCP
IP address type	ipv4
VPC	vpc-05506a755ff48bf6e (intel-ema-network)
Subnets	subnet-07aff7a001005ed34 (public-usw1a), subnet-0110cd4da4ec72e62 (public-usw1b) ▲
Tags	

▼ Routing [Edit](#)

Target group	Existing target group
Target group name	ema-web
Port	443
Target type	instance
Protocol	TCP
Health check protocol	TCP
Health check port	traffic port
Healthy threshold	3
Unhealthy threshold	3
Interval	30

[Cancel](#) [Previous](#) [Create](#)

8.3.4 Corregir las reglas de reenvío del equilibrador de carga

El destino de reenvío es adecuado para el objeto de escucha 443 del puerto, pero ahora tenemos que editar y cambiar el objeto de escucha para el puerto 8084 a fin de que el reenvío se realice al grupo de destinos correcto.

8.3.4.1 Editar los objetos de escucha del equilibrador de carga

Load balancer: **ema-web-balancer**

Description **Listeners** Monitoring Integrated services Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

Add listener Edit Delete

Listener ID	Security policy	SSL Certificate	ALPN policies	Default action
TCP : 443 arn...d7449b4094cd34d1	N/A	N/A	N/A	Forward to ema-web
<input checked="" type="checkbox"/> TCP : 8084 arn...40417262f99b8abc	N/A	N/A	N/A	Forward to ema-web

Seleccione el equilibrador de carga que creó.

Seleccione la pestaña **Listeners**.

Seleccione la casilla junto al objeto de escucha TCP/8084.

Haga clic en el botón **Edit**.

8.3.4.2 Actualice la acción de reenvío del objeto de escucha TCP/8084

View/edit listener. Each listener must include one action of type forward. **Update**

ema-web-balancer | **TCP : 8084**

Listeners belonging to Network Load Balancers check for connection requests using the protocol and port you configure. Each listener must include a default action to ensure all requests are routed. [Learn more](#)

ARN
arn:aws:elasticloadbalancing:us-west-1:802420695018:listener/net/ema-web-balancer/9faa96fc630182c2/40417262f99b8abc

Protocol : port
Select the protocol for connections from the client to your load balancer, and enter a port number from which to listen to for traffic.
TCP : 8084

Default action(s)
Indicate how this listener will route traffic

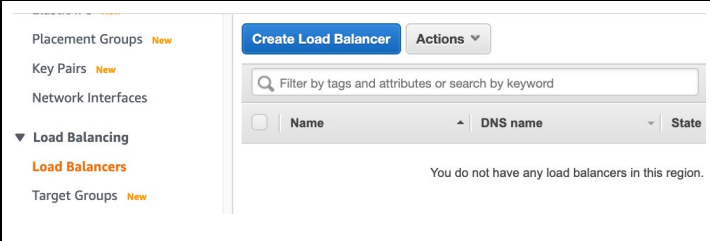
1. **Forward to...**
ema-websocket

Cambie la acción predeterminada de reenvío al objeto de escucha de WebSocket.

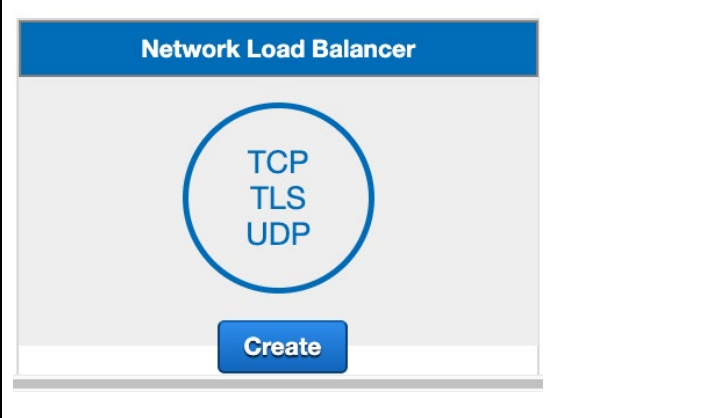
Haga clic en el botón **Update**.

8.4 Crear un equilibrador de carga de red para el tráfico Swarm

8.4.1 Crear el equilibrador de carga

 <p>The screenshot shows the AWS Management Console interface. On the left, there is a navigation menu with 'Load Balancing' expanded and 'Load Balancers' selected. The main content area shows a 'Create Load Balancer' button and a search bar. Below the search bar, there are fields for 'Name', 'DNS name', and 'State'. A message at the bottom states 'You do not have any load balancers in this region.'</p>	<p>En la barra lateral de EC2, en Load Balancing, seleccione Load Balancers y haga clic en Create Load Balancer.</p>
--	--

8.4.2 Seleccionar el tipo de equilibrador de carga

 <p>The screenshot shows the 'Network Load Balancer' selection screen. It features a blue header with the text 'Network Load Balancer'. In the center, there is a large blue circle containing the text 'TCP', 'TLS', and 'UDP'. Below the circle is a blue 'Create' button.</p>	<p>Haga clic en el botón Create en el encabezado Network Load Balancer.</p>
--	---

8.4.3 Configurar el equilibrador de carga

8.4.3.1 Configuración básica

<p>1. Configure Load Balancer 2. Configure Security Settings 3. Configure Routing</p> <h3>Step 1: Configure Load Balancer</h3> <h4>Basic Configuration</h4> <p>To configure your load balancer, provide a name, select a scheme, specify one or select a network. The default configuration is an Internet-facing load balancer in 1 with a listener that receives TCP traffic on port 80.</p> <p>Name ⓘ <input type="text" value="ema-swarm-balancer"/></p> <p>Scheme ⓘ <input checked="" type="radio"/> internet-facing <input type="radio"/> internal</p>	<p>Ingrese la configuración básica.</p> <p>Name: introduzca un nombre único. Ejemplo: <i>ema-swarm-balancer</i></p> <p>Scheme: internet-facing.</p>
--	---

8.4.3.2 Objetos de escucha

<h4>Listeners</h4> <p>A listener is a process that checks for connection requests, using the protocol and port configured.</p> <table border="1"><thead><tr><th>Load Balancer Protocol</th><th>Load Balancer Port</th></tr></thead><tbody><tr><td>TCP</td><td>8080</td></tr></tbody></table>	Load Balancer Protocol	Load Balancer Port	TCP	8080	<p>En la sección Listeners, agregue los objetos de escucha para estos protocolos y puertos.</p> <ul style="list-style-type: none">• <i>TCP 8080</i>
Load Balancer Protocol	Load Balancer Port				
TCP	8080				

8.4.3.3 Zonas de disponibilidad

<h4>Availability Zones</h4> <p>Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.</p> <p>Create and manage Elastic IPs in the VPC console</p> <p>VPC <i>i</i> vpc-05506a755ff48bf6e (10.250.0.0/24) intel-ema-network</p> <p>Availability Zones</p> <p><input checked="" type="checkbox"/> us-west-1a subnet-07aff7a001005ed34 (public-usw1a) <i>i</i></p> <p>IPv4 address <i>i</i> Assigned by AWS</p> <p><input checked="" type="checkbox"/> us-west-1b subnet-01110cd4da4ec72e62 (public-usw1b) <i>i</i></p> <p>IPv4 address <i>i</i> Assigned by AWS</p>	<p>Configure la sección Availability Zones de la siguiente manera:</p> <ul style="list-style-type: none">• VPC: seleccione la VPC que creó anteriormente.• Availability Zones: habilite ambas zonas de disponibilidad y seleccione ambas subredes públicas. La dirección IPv4 debería establecerse en <i>Assigned by AWS</i>. <p>Haga clic en el botón Next: Configure Security Settings.</p>
--	--

8.4.3.4 Configurar la seguridad

No hay nada para configurar en este paso. Haga clic en el botón **Next: Configure Routing**.

8.4.3.5 Configurar el enrutamiento

<p>1. Configure Load Balancer 2. Configure Security Settings 3. Configure Routing</p> <h4>Step 3: Configure Routing</h4> <p>Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.</p> <h4>Target group</h4> <p>Target group <i>i</i> Existing target group</p> <p>Name <i>i</i> ema-swarm</p> <p>Target type</p> <p><input checked="" type="radio"/> Instance</p> <p><input type="radio"/> IP</p> <p>Protocol <i>i</i> TCP</p> <p>Port <i>i</i> 8080</p> <h4>Health checks</h4> <p>Protocol <i>i</i> TCP</p> <p>Cancel Previous Next: Register Targets</p>	<p>En el Step 3: Configure Routing, configure el grupo de destinos de la siguiente manera.</p> <ul style="list-style-type: none">• Target group: <i>Existing target group</i>• Name: seleccione el nombre del grupo de destinos TCP/8080 que creó anteriormente. Ejemplo: <i>ema-swarm</i> <p>Haga clic en el botón Next: Register Targets.</p>
---	--

8.4.3.6 Registrar los destinos

Verifique que vea dos instancias en la lista como destinos registrados.

Haga clic en el botón **Next: Review**.

8.4.3.7 Revisar

En el **Step 5: Review**, verifique que la configuración se vea similar al ejemplo proporcionado aquí y, luego, haga clic en el botón **Create**.

[1. Configure Load Balancer](#) [2. Configure Security Settings](#) [3. Configure Routing](#)

Step 5: Review

Please review the load balancer details before continuing

▼ Load balancer [Edit](#)

Name ema-swarm-balancer
Scheme internet-facing
Listeners Port:8080 - Protocol:TCP
IP address type ipv4
VPC vpc-05506a755ff48bf6e (intel-ema-network)
Subnets subnet-07aff7a001005ed34 (public-usw1a),
subnet-0110cd4da4ec72e62 (public-usw1b) ▲
Tags

▼ Routing [Edit](#)

Target group Existing target group
Target group name ema-swarm
Port 8080
Target type instance
Protocol TCP
Health check protocol TCP
Health check port traffic port
Healthy threshold 3
Unhealthy threshold 3
Interval 30

[Cancel](#)

[Previous](#)

[Create](#)

8.4.4 Tomar nota del nombre de DNS del equilibrador de carga

Vuelva a la pestaña **Description** de los equilibradores de carga y tome nota de los nombres de DNS. Recomendamos que cree registros CNAME de sus nombres de dominio personalizados con su proveedor de DNS para que pueda dirigir el tráfico web y Swarm de EMA a los equilibradores de carga.

<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 Apéndice A: notas sobre la integración de Active Directory*

Existen varias maneras de integrar Active Directory* (AD) con AWS para poder conectar sus máquinas virtuales a un dominio y usar la autenticación de AD. Debido a que las necesidades de las organizaciones pueden ser bien diferentes, este apéndice solo proporciona algunos indicadores breves sobre como podría extender un directorio existente en las instalaciones a la nube para este fin. Los proveedores en la nube cambian y expanden sus ofertas de servicio periódicamente, por lo que deberá realizar su propia investigación antes de implementar una solución de producción para ver qué es lo que tiene más sentido para su empresa.

Para obtener más información sobre los servicios de Active Directory en AWS, visite los siguientes enlaces:

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/>

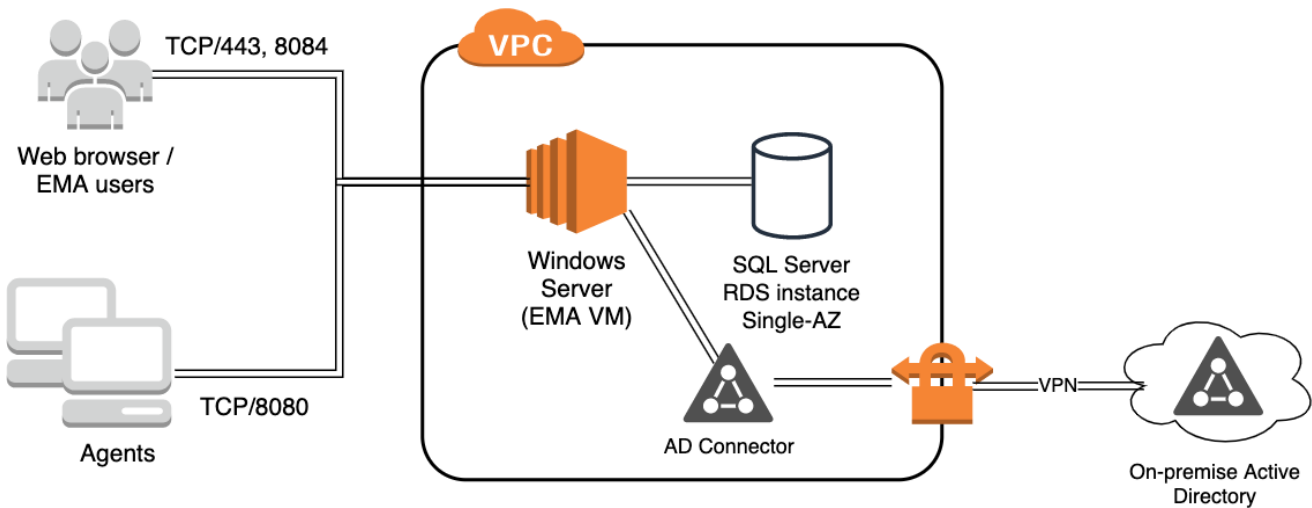
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html

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

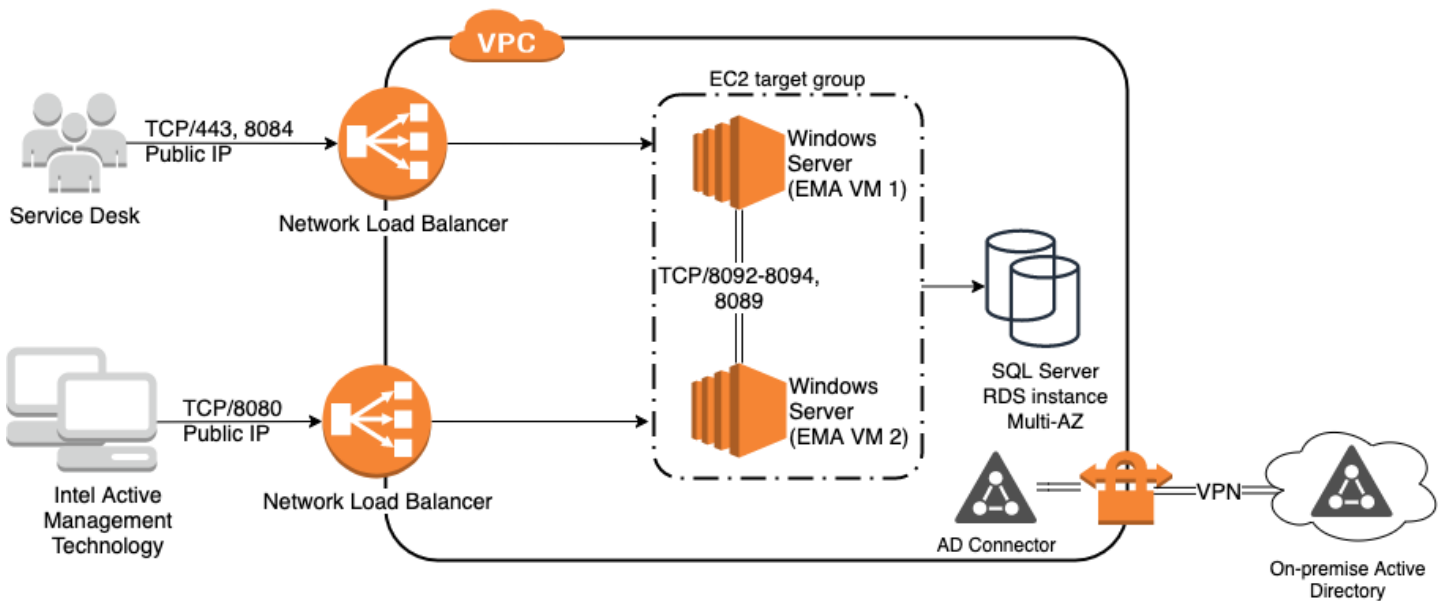
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_best_practices.html

10 Diagrama de arquitectura con integración de Active Directory

10.1 Implementación de un servidor único



10.2 Implementación de servidores distribuidos



10.3 Usar el conector de AD de AWS para extender Active Directory a la nube

- ❑ Cree una VPN para conectarse a su red en las instalaciones a fin de proporcionar conectividad a sus controladores de dominio.
 - ❑ Cree una puerta de enlace del lado del cliente para representar el extremo remoto (en las instalaciones) de la VPN.
 - ❑ Cree una puerta de enlace privada virtual para proporcionar enrutamiento entre la VPN y su VPC.
 - ❑ Asocie la puerta de enlace privada virtual a su VPC.

- ❑ Cree una conexión de VPN mediante la selección de la nueva puerta de enlace del lado del cliente y la puerta de enlace privada virtual (VPG).
 - ❑ Seleccione la opción Static routing e ingrese las redes disponibles a través de la conexión de VPN. Esto deberá incluir sus controladores de dominio en las instalaciones.
 - ❑ Puede permitir que Amazon genere sus claves y direcciones de túnel.
- ❑ Descargue la configuración de conexión de la VPN para ayudarse a configurar el otro lado.
- ❑ Vaya a la tabla de rutas de la VPC y habilite la propagación de rutas para que las rutas asociadas a la conexión de VPN estén disponibles para su red de VPC.
- ❑ Cree un recurso de conector de AD para que funcione como proxy para su AD en las instalaciones.
 - ❑ Seleccione el conector de AD como el tipo de directorio.
 - ❑ Seleccione el tamaño de directorio adecuado para la cantidad de objetos que necesita admitir.
 - ❑ Seleccione su VPC y las dos subredes diferentes.
 - ❑ Ingrese la información para el directorio en las instalaciones con el que se conectará.
 - ❑ Tenga en cuenta que se requiere una cuenta de servicio. Los requisitos previos se describen plenamente en los enlaces a la documentación que se proporcionan a continuación.
- ❑ Cree un conjunto de opciones de DHCP y asócielo a su VPC para que las máquinas virtuales reciban los servidores DNS y el nombre de dominio adecuados.
 - ❑ Proporcione los servidores DNS y el nombre de dominio de Active Directory. Los otros parámetros son opcionales.
 - ❑ Vaya a su VPC y asocie el conjunto de opciones de DHCP a ella.
- ❑ Cuando configure las instancias de máquina virtual de EC2, utilice la opción Domain join para que la VM se conecte automáticamente a su dominio de AD.