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.

Contenido

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

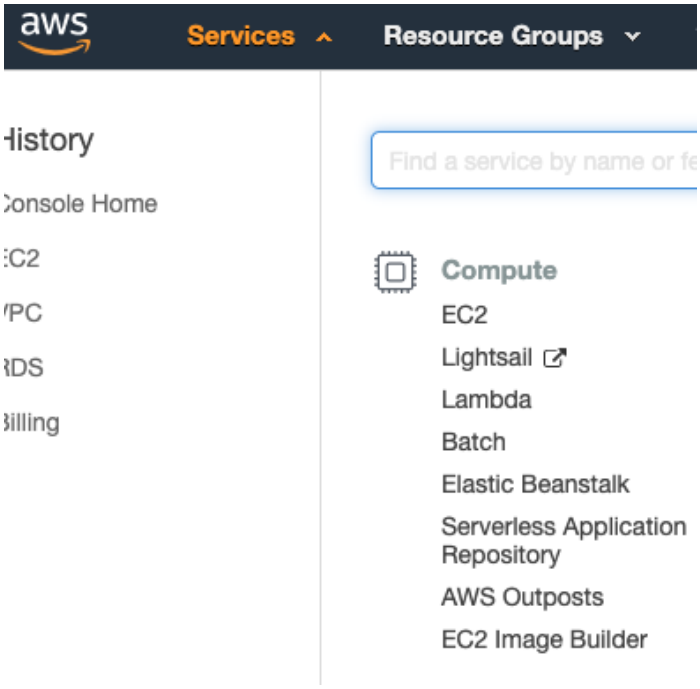
La informática en la nube es el suministro a pedido de recursos de TI a través de Internet con precios determinados por el uso del servicio. En lugar de comprar, poseer y mantener centros de datos físicos y servidores, puede acceder a servicios de tecnología, como potencia informática, almacenamiento 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

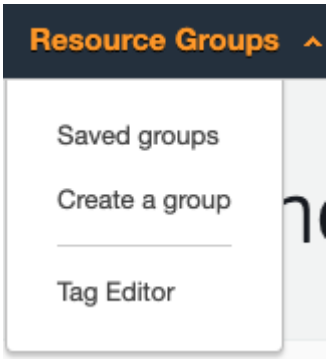


Después de haber iniciado sesión en la consola de administración de AWS en https://aws.amazon.com/console/, verá un menú Services en la esquina superior izquierda de la pantalla.

Si hace clic allí, abrirá una lista de todos los servicios que brinda AWS organizados por categoría, como Compute, Storage, Database, etc.

Cuando se brinden instrucciones para implementar servicios en esta guía, lo dirigiremos a esta pantalla para que seleccione el servicio apropiado.

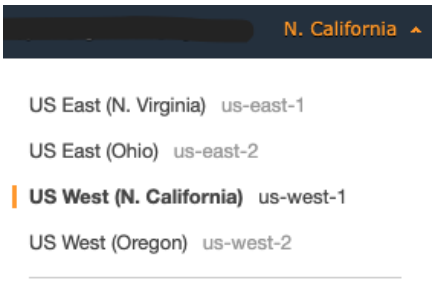
1.2.2 Grupos de recursos



Junto a Services, se encuentra el menú Resource Groups, donde puede crear grupos de recursos o ver los que haya creado.

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.

1.2.3 Regiones



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.

Solo podrá ver los recursos de la región que haya seleccionado.

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

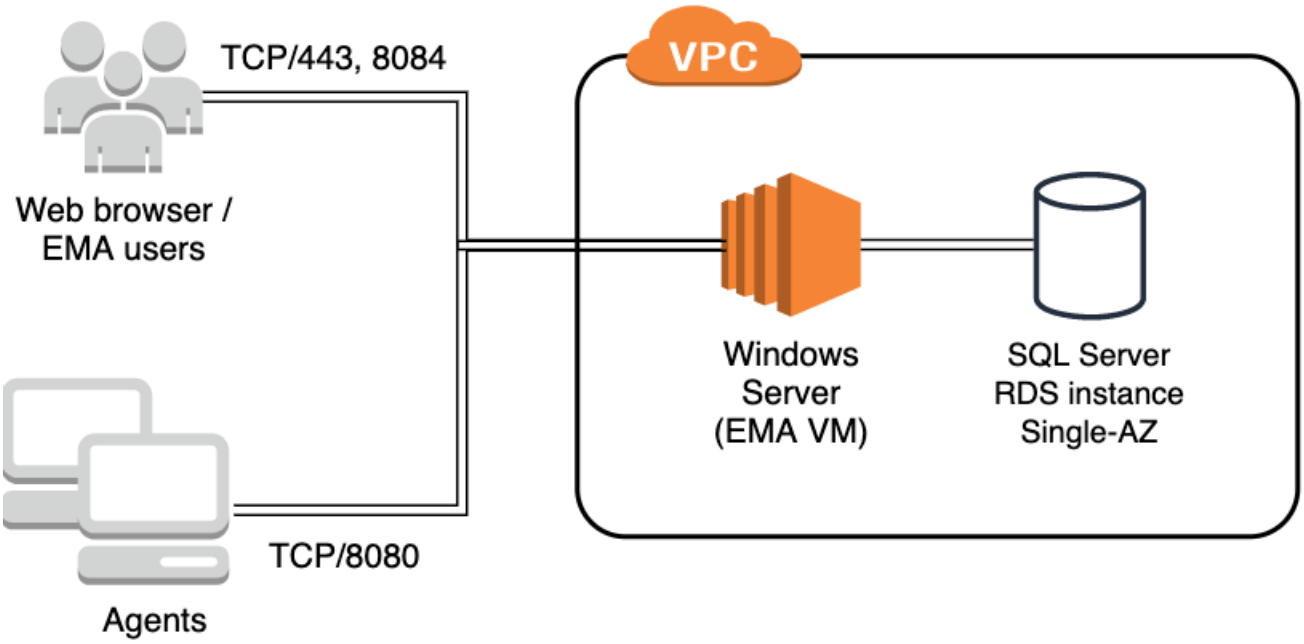
Si su organización ya tiene una cuenta de AWS, debería pedirle a un administrador de la nube que le conceda los accesos necesarios para poder crear todos los recursos enumerados en esta guía.

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**.

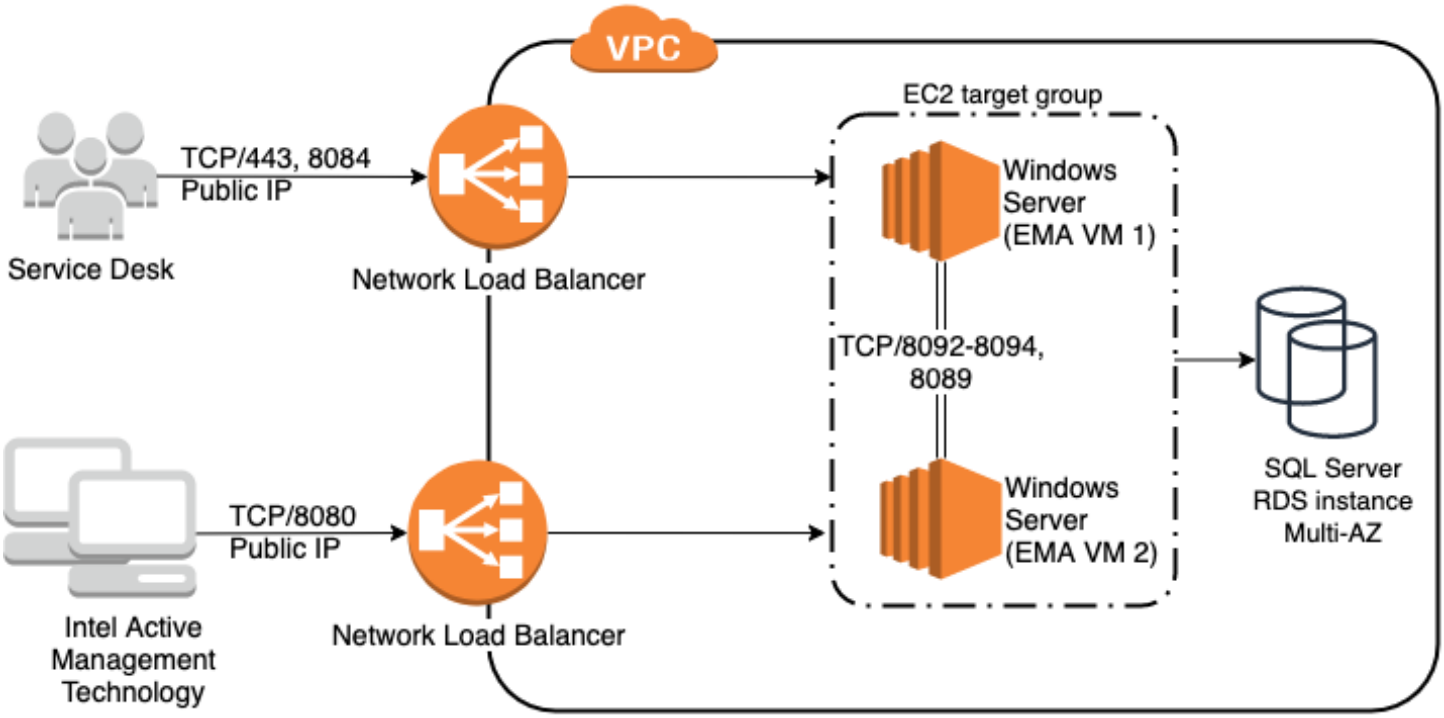
Consulte con su administrador de redes si existe algún espacio de dirección preferencial para utilizar. Es conveniente evitar la superposición con sus redes empresariales para prevenir problemas de enrutamiento si ya tiene una VPN establecida para el proveedor en la nube o si planea tenerla en el futuro. 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

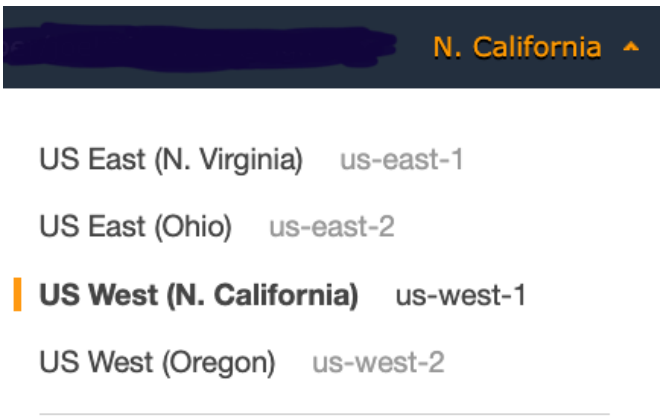


2.2 Implementación de servidores distribuidos



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.



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

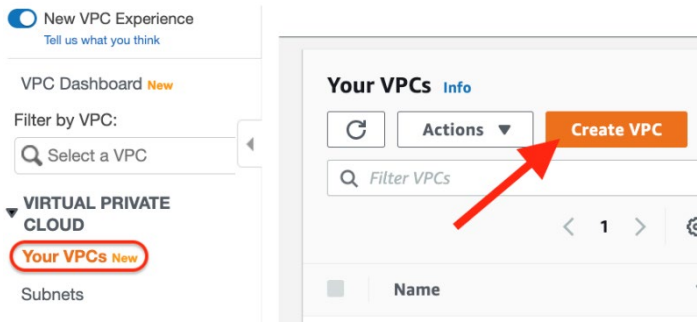
4.2 Crear una VPC

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

	En el menú **Services**, en **Network & Content Delivery**, seleccione **VPC**.

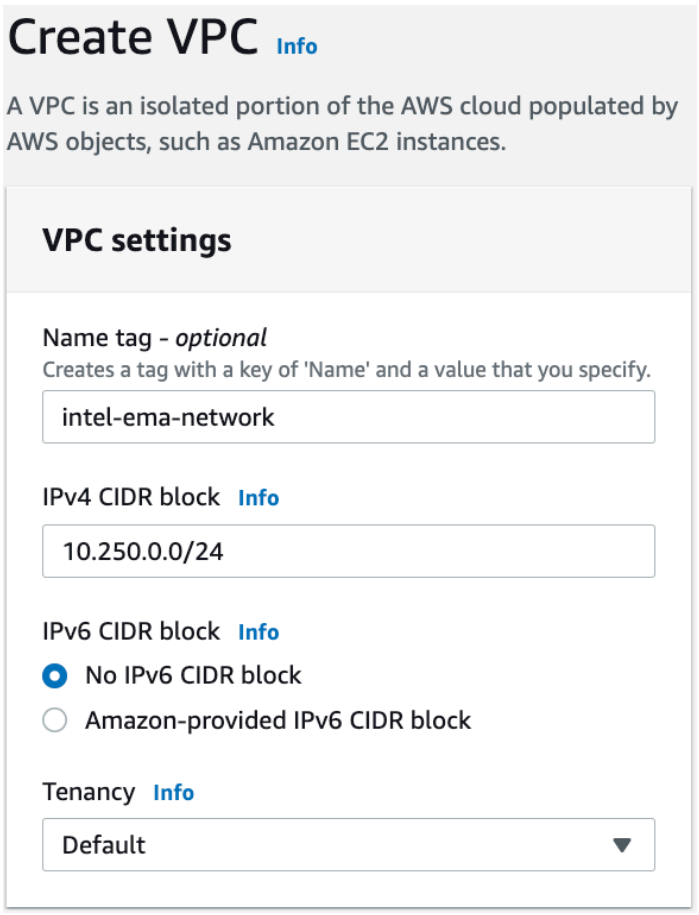
4.2.2 Crear una VPC



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



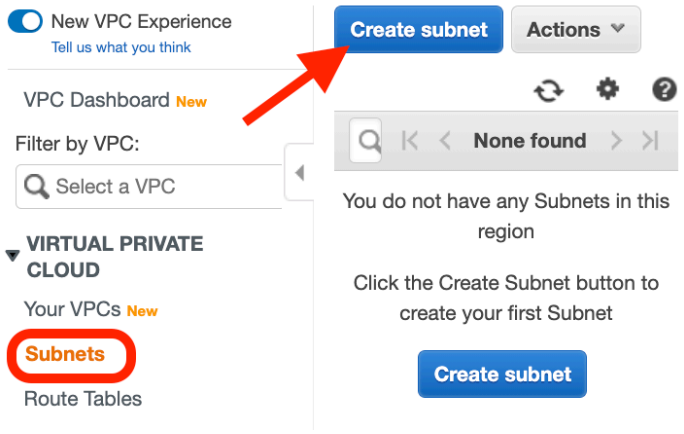
Ingrese los detalles de la red de la siguiente manera:

- **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**.

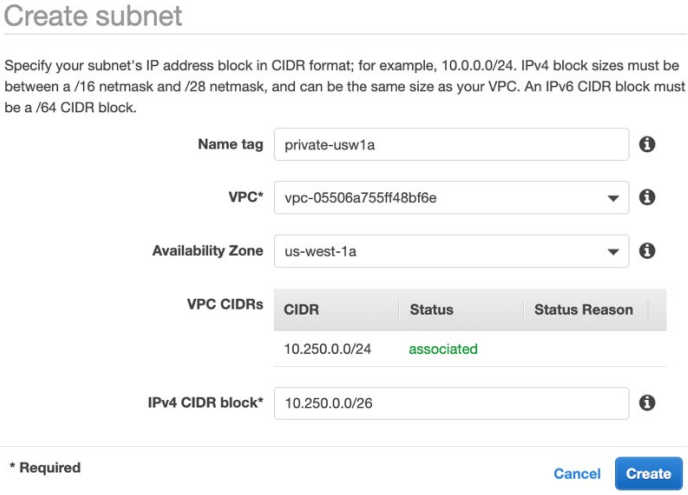
4.3 Crear subredes

4.3.1 Ir a la pantalla Subnets



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

4.3.2 Crear la primera subred privada



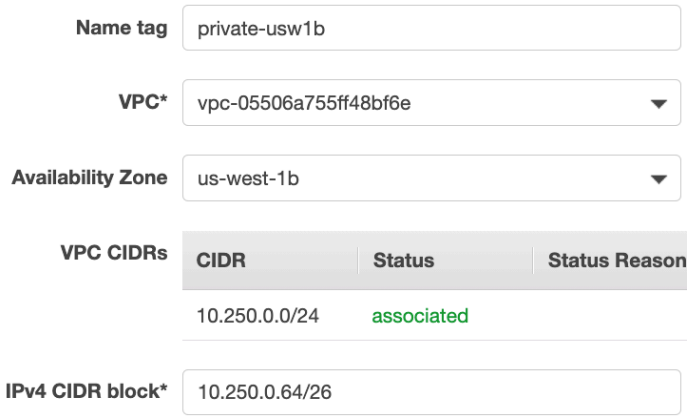
Haga clic en el botón **Create subnet**.

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



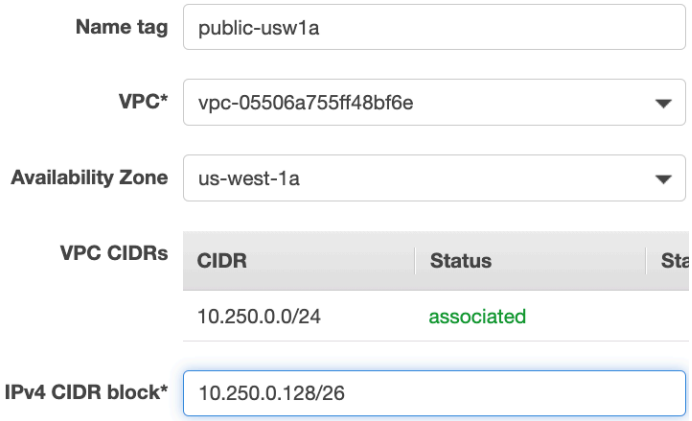
Haga clic en el botón **Create subnet**.

Configure la subred de la siguiente manera:

- **Name tag**: proporcione un nombre de subred único.
  Ejemplo: *private-usw1b*
- **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: *us-west-1b*
- **IPv4 CIDR block**: seleccione un bloque de IP sin usar en el espacio de dirección de su VPC.
  Ejemplo: *10.250.0.64/26*

Haga clic en el botón **Create**.

4.3.4 Crear la primera subred pública



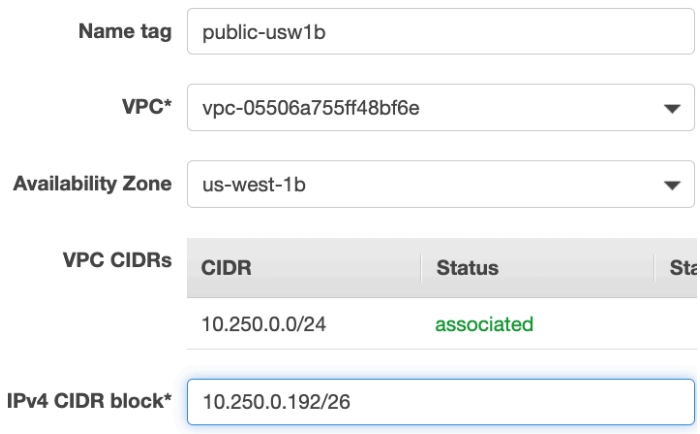
Haga clic en el botón **Create subnet**.

Configure la subred de la siguiente manera:

- **Name tag**: proporcione un nombre de subred único.
  Ejemplo: *public-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: *10.250.0.128/26*

Haga clic en el botón **Create**.

4.3.5 Crear la segunda subred pública



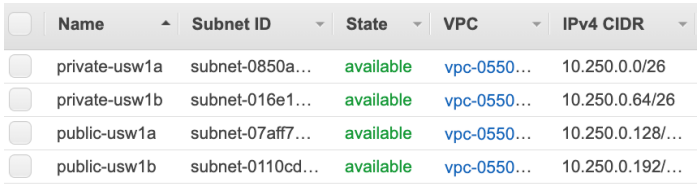
Haga clic en el botón **Create subnet**.

Configure la subred de la siguiente manera:

- **Name tag**: proporcione un nombre de subred único. Ejemplo: *public-usw1b*
- **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: *us-west-1b*
- **IPv4 CIDR block**: seleccione un bloque de IP sin usar en el espacio de dirección de su VPC.
  Ejemplo: *10.250.0.196/26*

Haga clic en el botón **Create**.

4.3.6 Revisar sus subredes



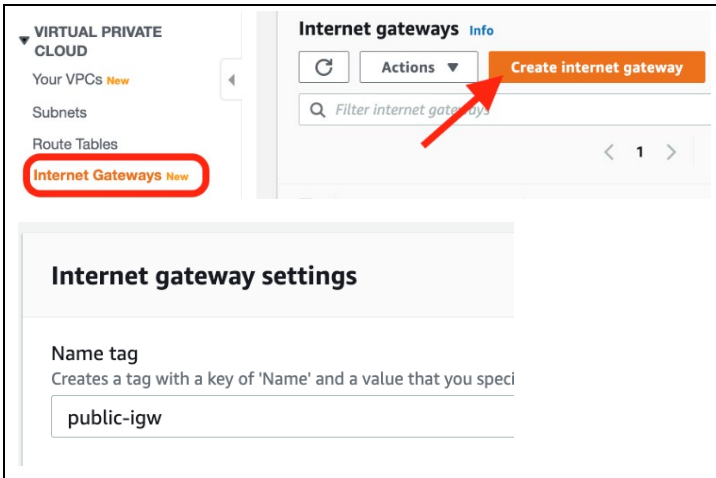
Name	Subnet ID	State	VPC	IPv4 CIDR
private-usw1a	subnet-0850a…	available	vpc-0550…	10.250.0.0/26
private-usw1b	subnet-016e1…	available	vpc-0550…	10.250.0.64/26
public-usw1a	subnet-07aff7…	available	vpc-0550…	10.250.0.128/…
public-usw1b	subnet-0110cd…	available	vpc-0550…	10.250.0.192/…

Revise su lista de subredes. Ahora debería tener cuatro subredes creadas.

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



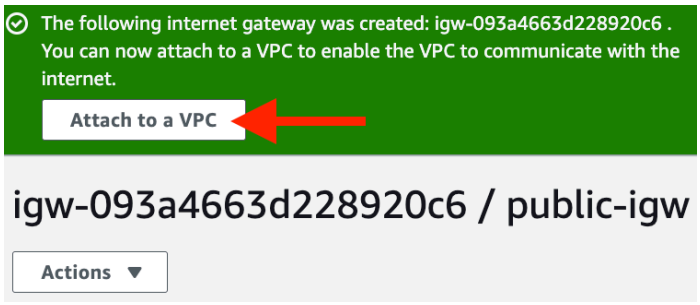
En la barra lateral de VPC, seleccione Internet Gateways.

Haga clic en **Create Internet gateway**.

Ingrese una etiqueta de nombre. Ejemplo: *public-igw*

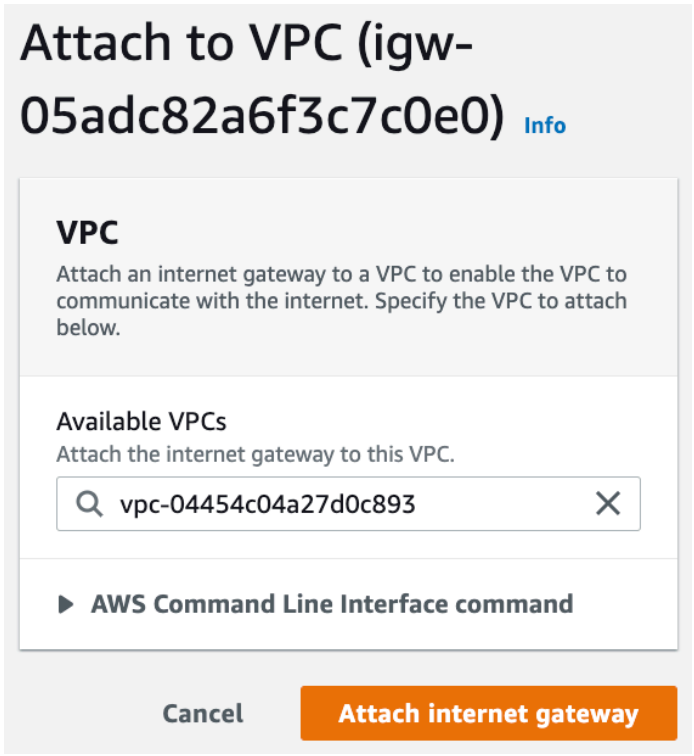
Haga clic en el botón **Create Internet gateway** en la parte inferior de la pantalla para terminar.

4.4.2 Asociar la puerta de enlace a Internet a la VPC



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.

4.4.3 Ingresar los detalles de la asociación



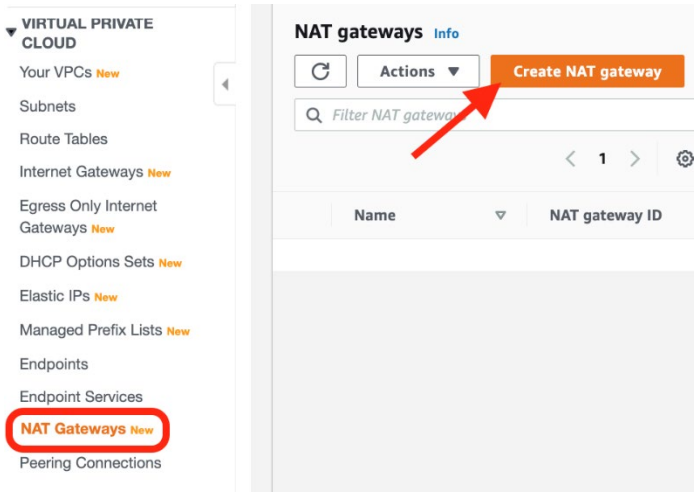
Seleccione la VPC que creó anteriormente.

Haga clic en el botón **Attach internet gateway**.

4.5 Crear puertas de enlace NAT para las subredes privadas

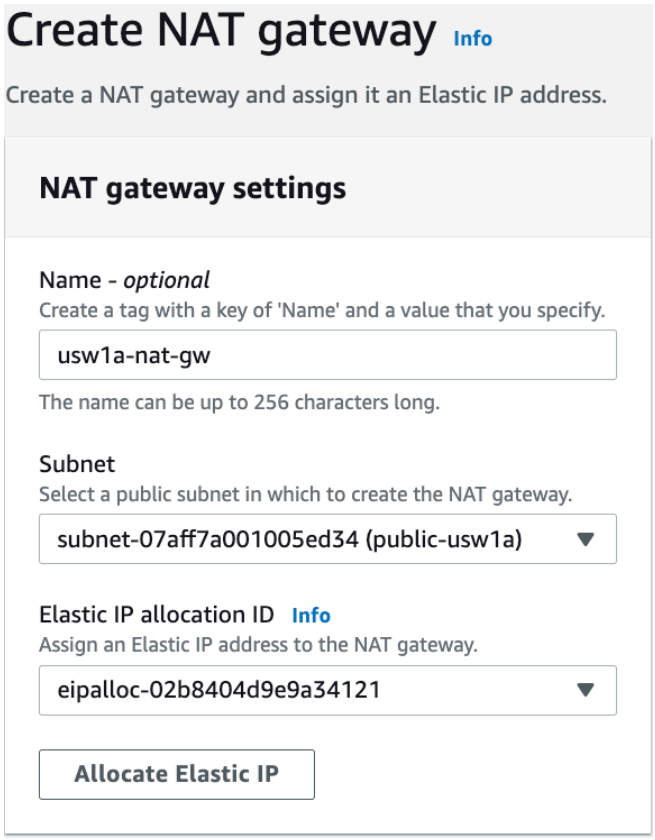
Una puerta de enlace NAT es un recurso zonal que puede usarse con los recursos de esa zona como un punto de salida del tráfico de Internet. La puerta de enlace NAT realizará la traducción de dirección y enviará el tráfico a la puerta de enlace a Internet en su VPC. Vamos a crear una puerta de enlace 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



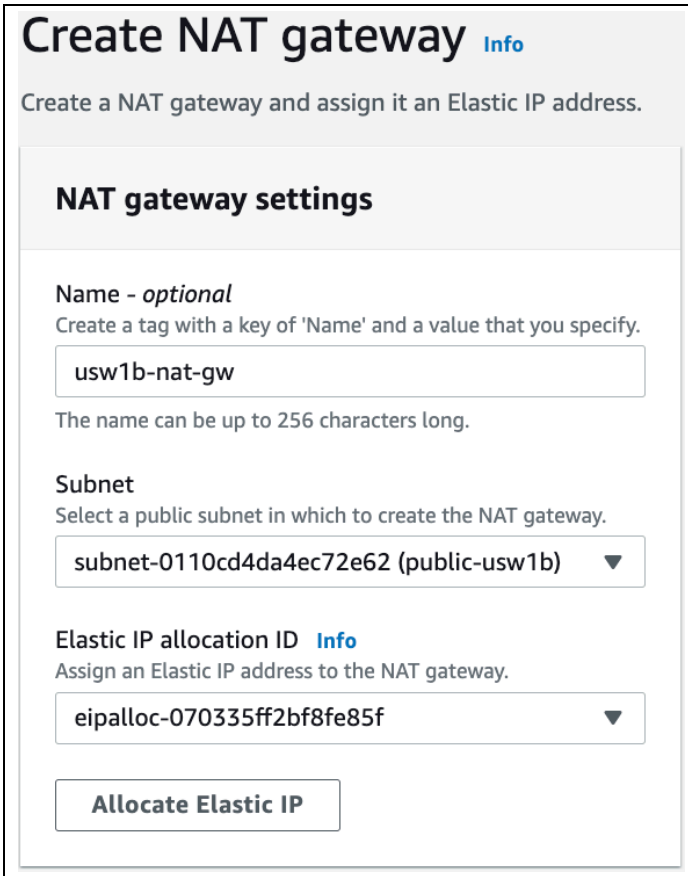
Haga clic en el botón **Create NAT gateway**.

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



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

Configure la puerta de enlace NAT de la siguiente manera:

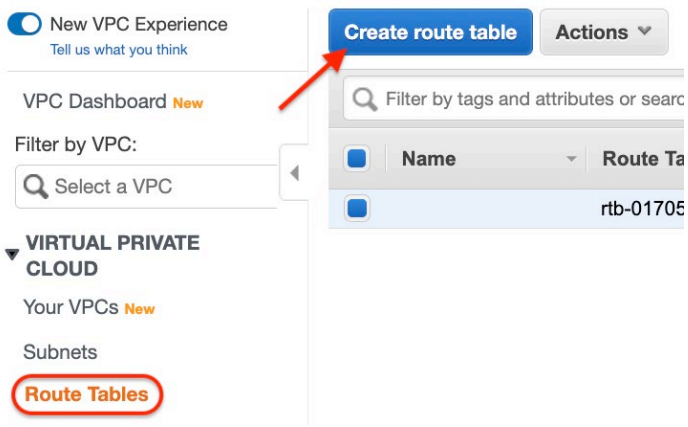
- **Name** (optional): ingrese un nombre único para la puerta de enlace.
  Ejemplo: *usw1b-nat-gw*
- **Subnet**: seleccione la segunda subred pública.
  Ejemplo: *public-usw1b*
- **Elastic IP allocation ID**: haga clic en el botón Allocate Elastic IP para llenar este campo de manera automática.

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



4.6.2 Crear la tabla de rutas para las subredes públicas

Haga clic en el botón **Create route table**.

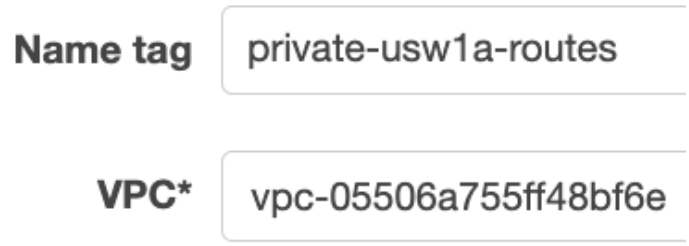
Configure la tabla de rutas de la siguiente manera:

- **Name Tag**: ingrese un nombre único para la tabla de rutas.
  Ejemplo: *public-usw-routes*
- **VPC**: seleccione la red virtual que creó anteriormente.

Haga clic en el botón **Create**.

Haga clic en el botón **Close**.

4.6.3 Crear la tabla de rutas para la primera subred privada



Haga clic en el botón **Create route table**.

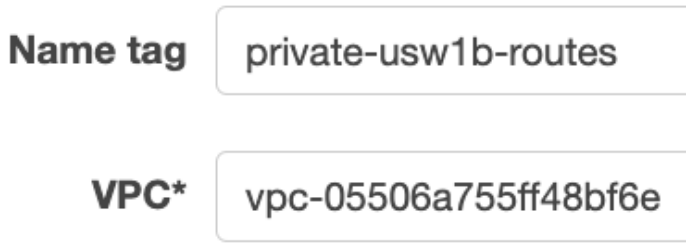
Configure la tabla de rutas de la siguiente manera:

- **Name Tag**: ingrese un nombre único para la tabla de rutas.
  Ejemplo: *private-usw1a-routes*
- **VPC**: seleccione la red virtual que creó anteriormente.

Haga clic en el botón **Create**.

Haga clic en el botón **Close**.

4.6.4 Creer la tabla de rutas para la segunda subred privada



Haga clic en el botón **Create route table**.

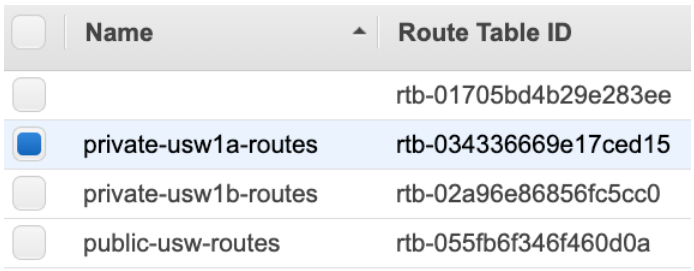
Configure la tabla de rutas de la siguiente manera:

- **Name Tag**: ingrese un nombre único para la tabla de rutas.
  Ejemplo: *private-usw1b-routes*
- **VPC**: seleccione la red virtual que creó anteriormente.

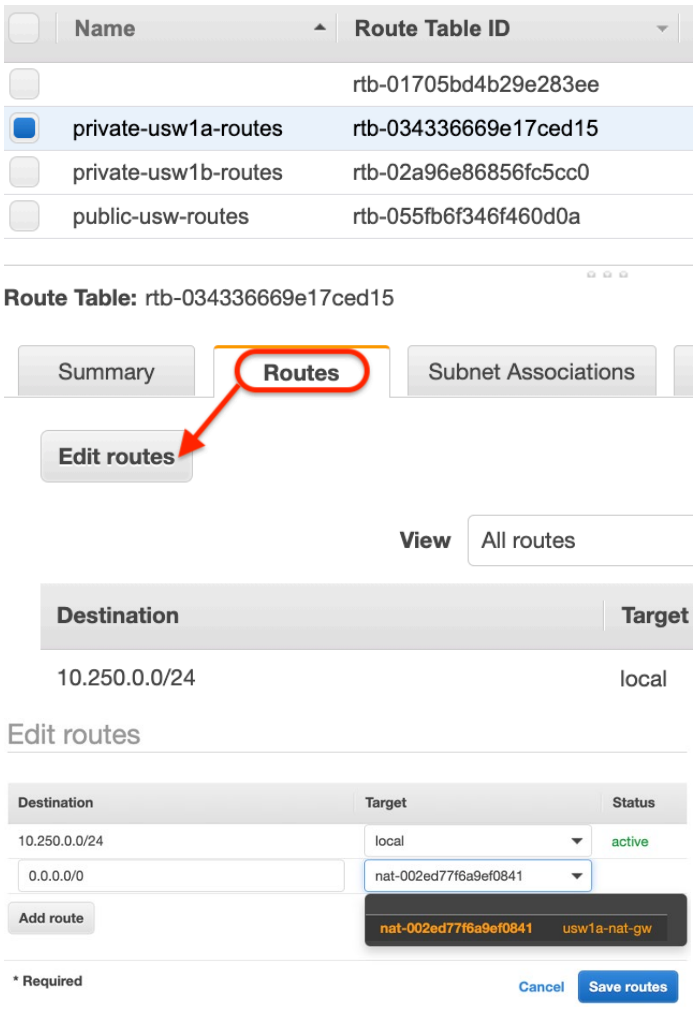
Haga clic en el botón **Create**.

Haga clic en el botón **Close**.

4.6.5 Revisar la lista de tabla de rutas

	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



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**.

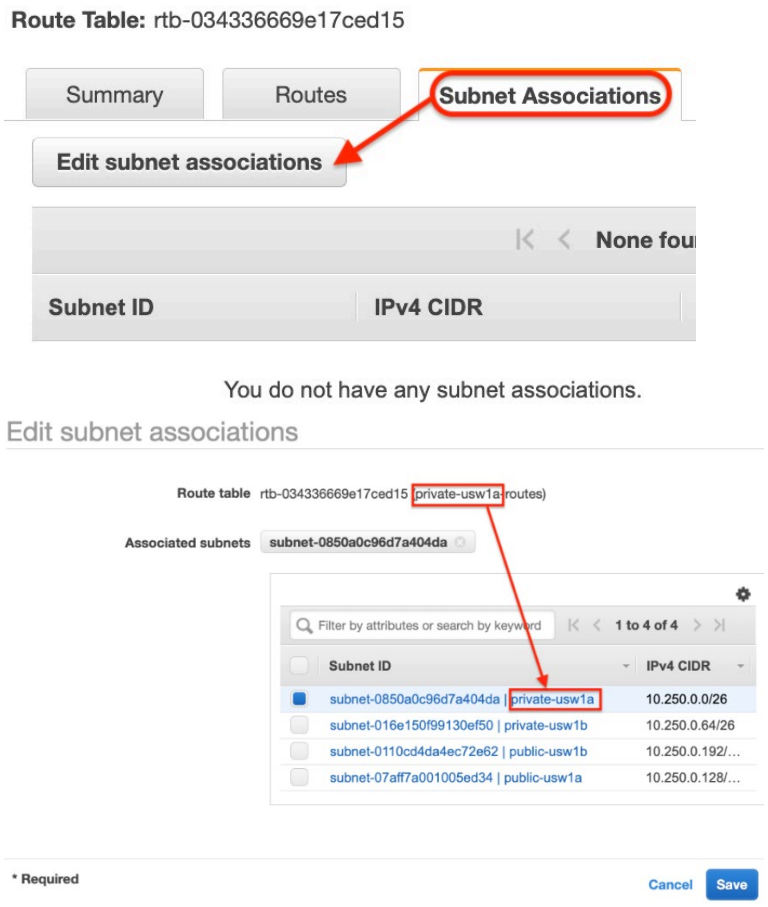
Haga clic en el botón **Add route** y establezca estos valores:

- **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



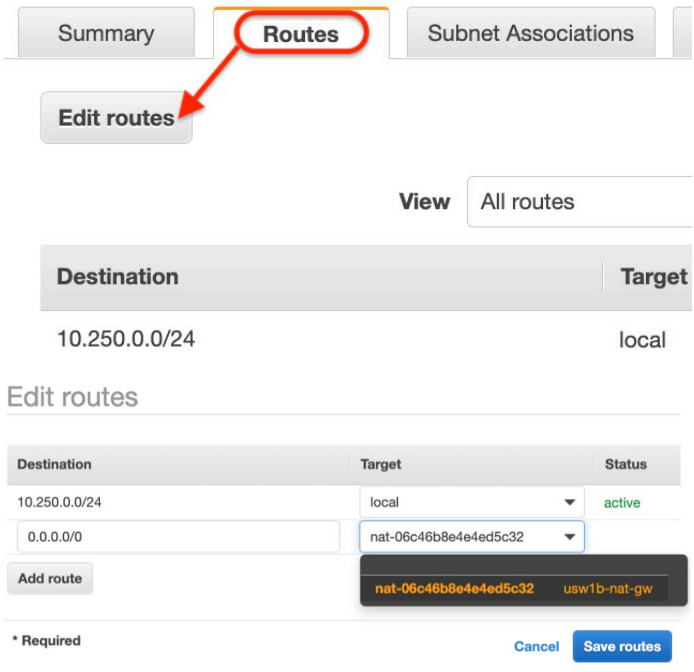
Seleccione la pestaña **Subnet Associations**.

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



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**.

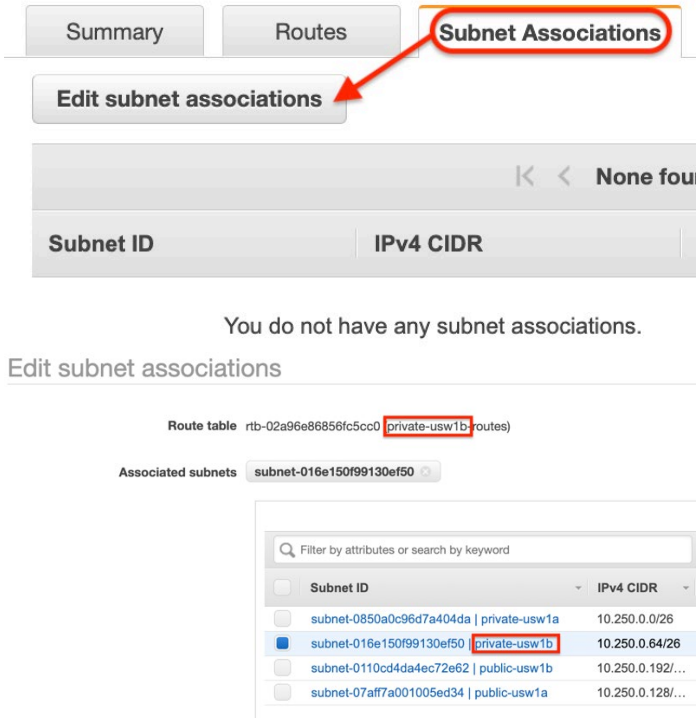
Haga clic en el botón **Add route** y establezca estos valores:

- **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



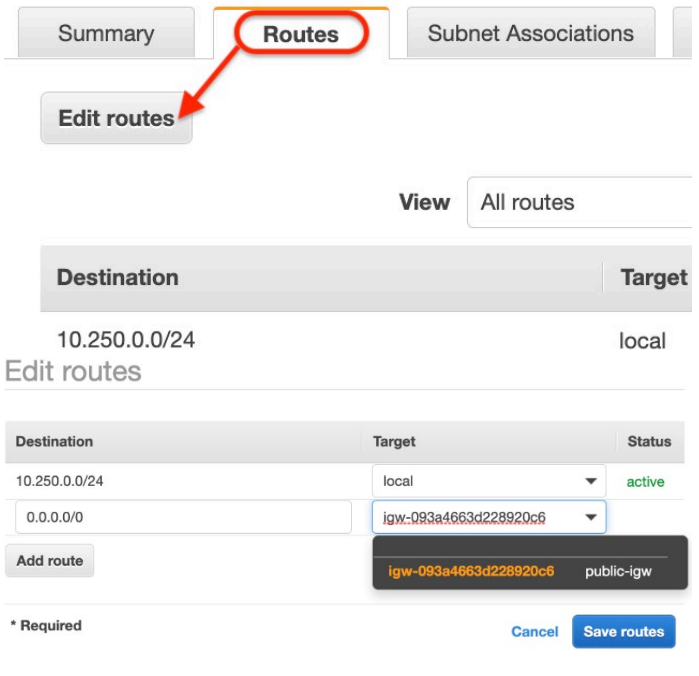
Seleccione la pestaña **Subnet Associations**.

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



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**.

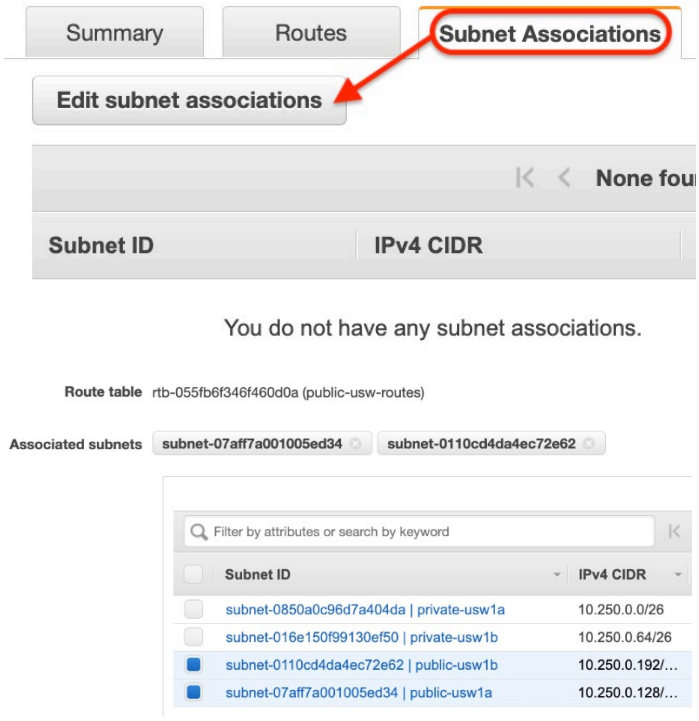
Haga clic en el botón **Add route** y establezca estos valores:

- **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**.

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 creemos 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.

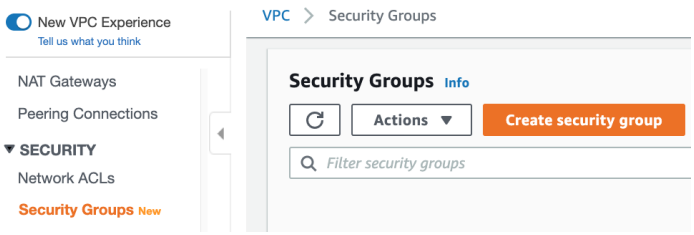
En los procedimientos que se incluyen a continuación, vamos a crear un grupo de seguridad para controlar el acceso a las VMs Intel® EMA y un grupo distinto para controlar el acceso a la base de datos.

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.

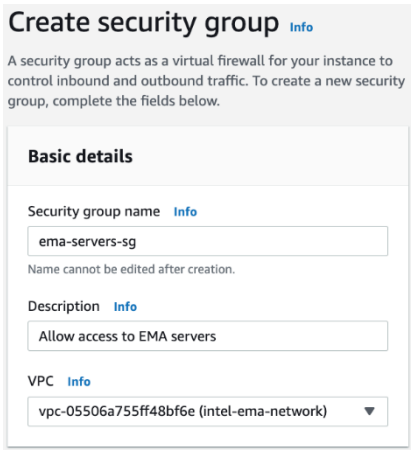
4.7.1.1 Cree un grupo de seguridad



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

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

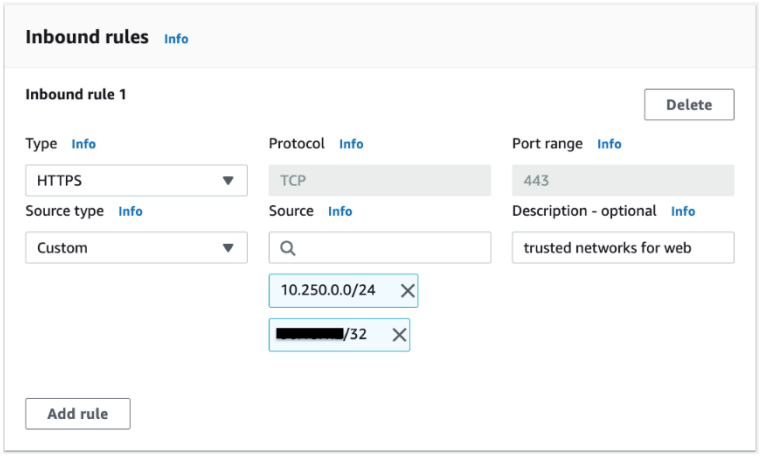
4.7.1.2 Configure los detalles básicos del grupo de seguridad



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.

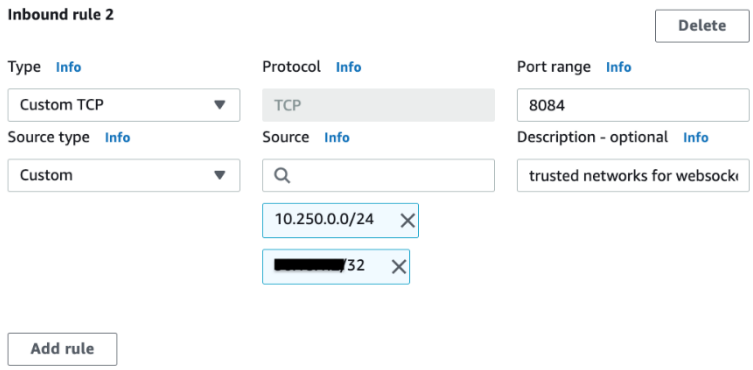
4.7.1.3 Agregue una regla de entrada para el tráfico web



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.

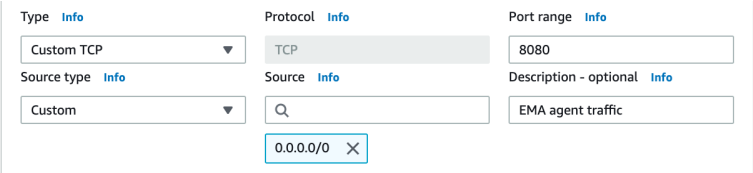
4.7.1.4 Agregue una regla de entrada para el tráfico de WebSocket



Agregue una regla de entrada con la siguiente configuración.

- **Type**: *Custom TCP*
- **Port range**: *8084*
- **Description**: *redes confiables para WebSocket*
- **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.

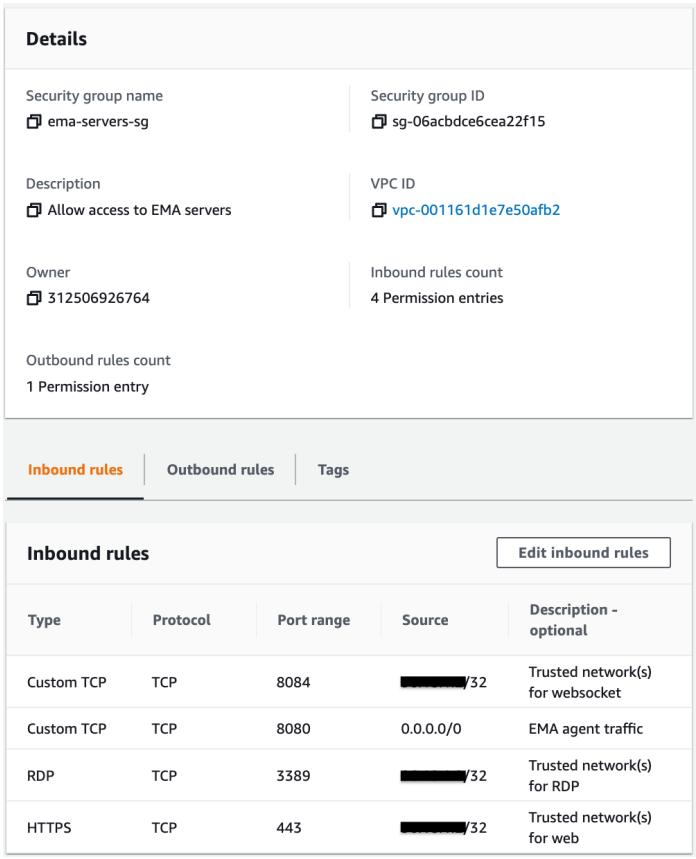
4.7.1.5 Agregue una regla de entrada para el tráfico Swarm



Agregue una regla de entrada con la siguiente configuración.

- **Type**: *Custom TCP*
- **Port range**: *8080*
- **Description**: *tráfico de Agente EMA*
- **Source**: *0.0.0.0/0*

4.7.1.6 Crear y revisar



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

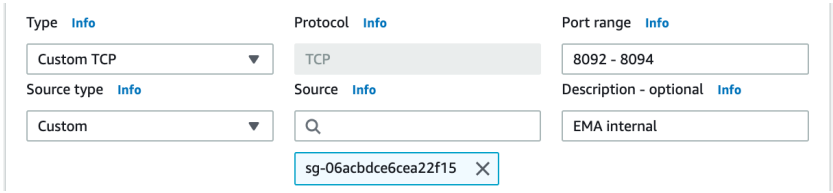
Revise la lista de reglas para verificar si son correctas.

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.

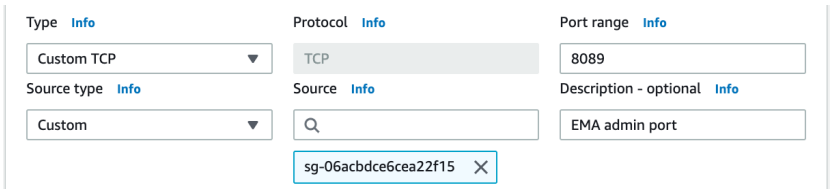
4.7.2.1 Agregue una regla de entrada para el tráfico interno de los puertos 8092-8094



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



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

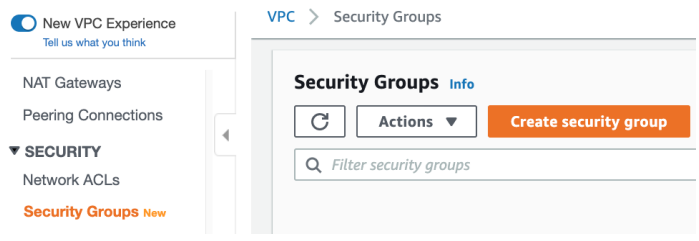
Haga clic en el botón **Save rules**. Revise las reglas para verificar si son correctas.

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	[redacted]/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	[redacted]/32	trusted networks for web

4.7.3 Crear un grupo de seguridad para la base de datos

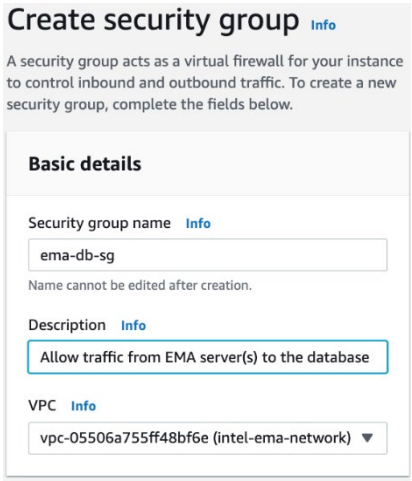
4.7.3.1 Cree un grupo de seguridad



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

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

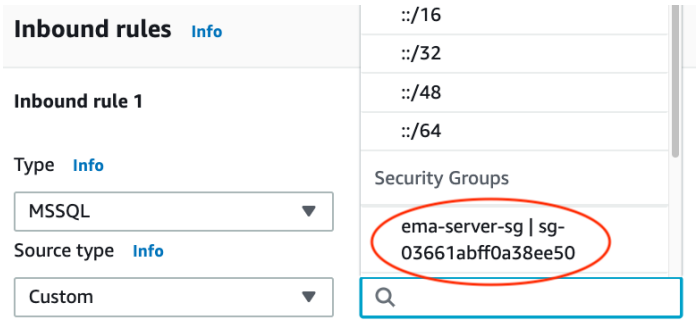
4.7.3.2 Configure los detalles básicos del grupo de seguridad



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



Agregue 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.

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.

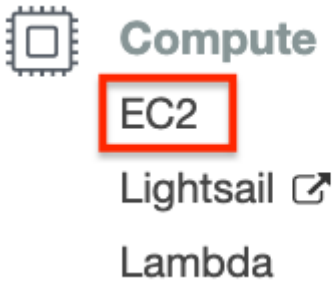
En el procedimiento que se muestra a continuación, y en otras secciones, se incluyen pasos adicionales para las implementaciones de servidores distribuidos que se pueden omitir para las de servidor único. Estos incluyen crear una segunda VM, asociar las VMs a un grupo de destinos, asociar este grupo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

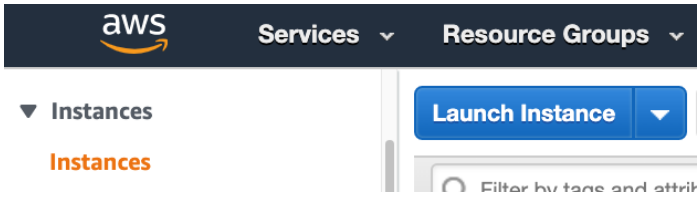
5.2 Crear máquinas virtuales

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.

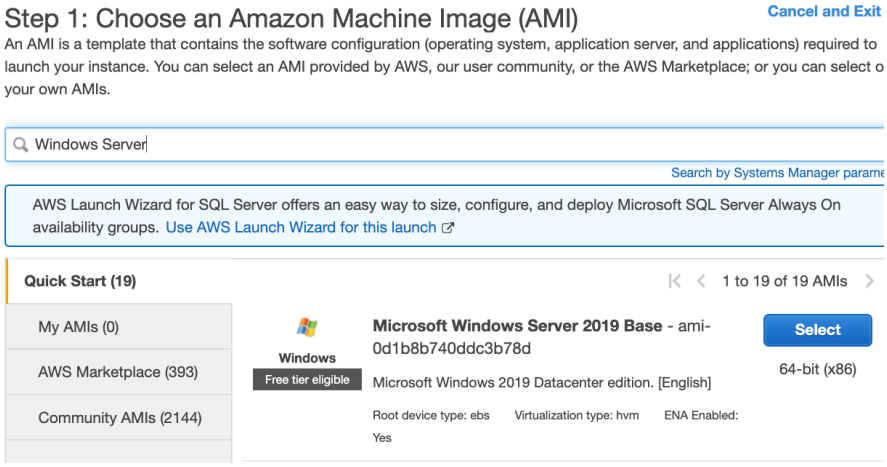
5.2.1 Ir al servicio EC2

	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

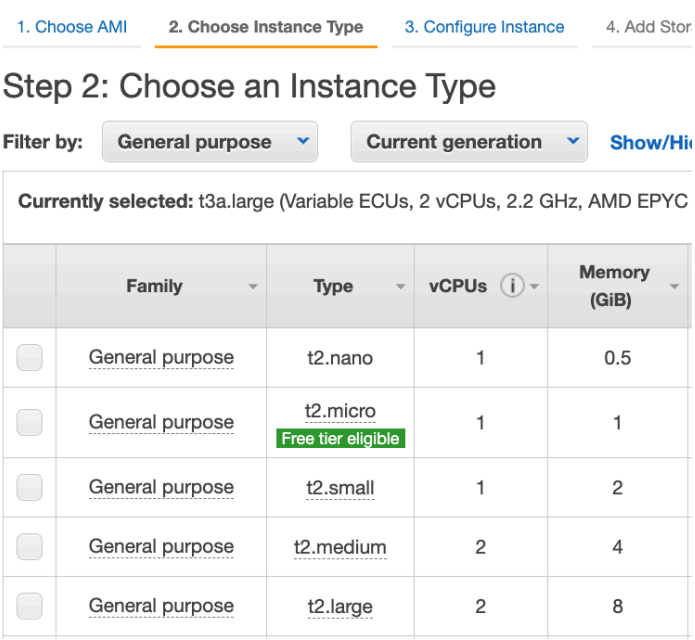


Busque la imagen de Microsoft Windows* Server Base compatible con Intel® EMA.

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

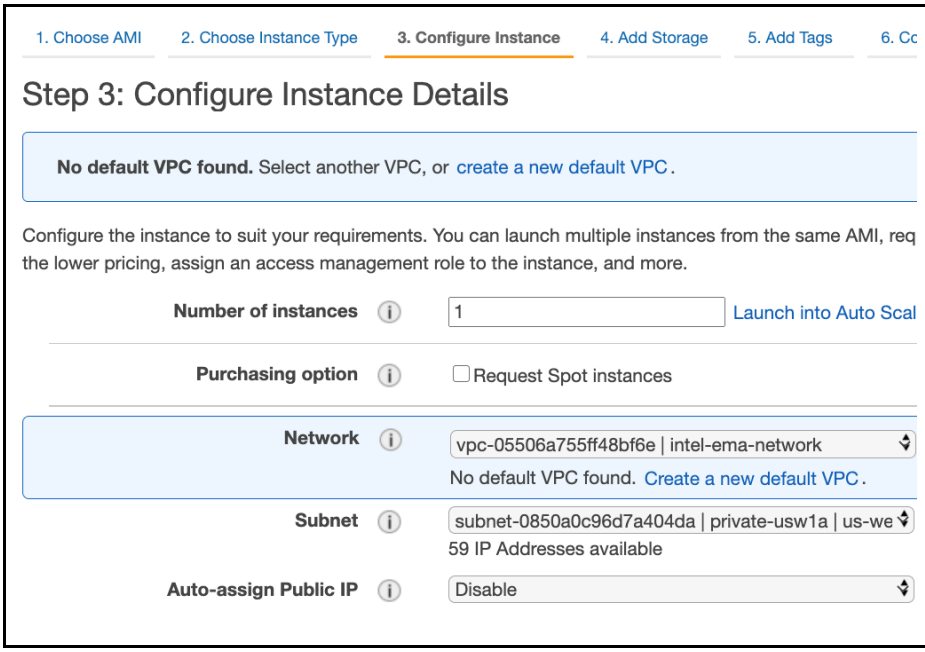


Seleccione el tipo de máquina con la cantidad de recursos de CPU y memoria que necesita. Puede cambiar esto más tarde cuando se apaga la instancia, si es necesario.

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



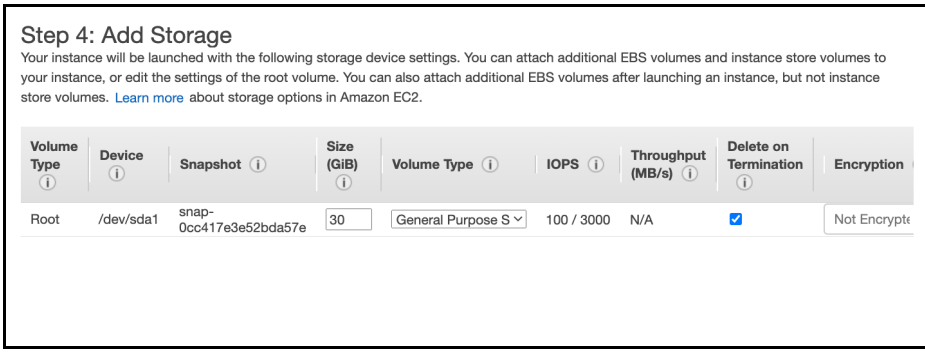
Configure los detalles de la instancia de la siguiente manera:

- **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**.

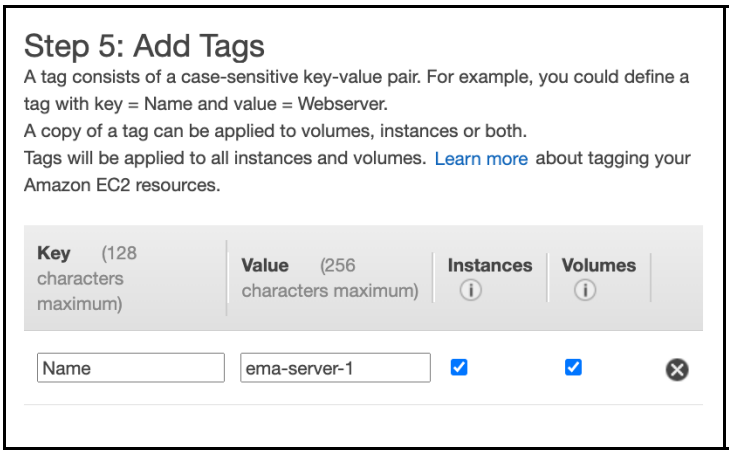
5.2.6 Agregar almacenamiento



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

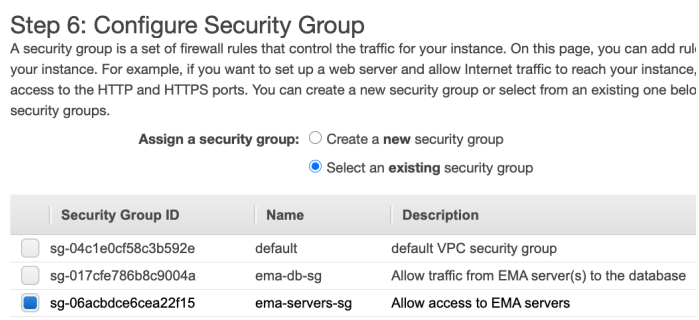


Agregue una etiqueta con la clave “Name” y un valor del nombre del servidor que busca.

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



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*

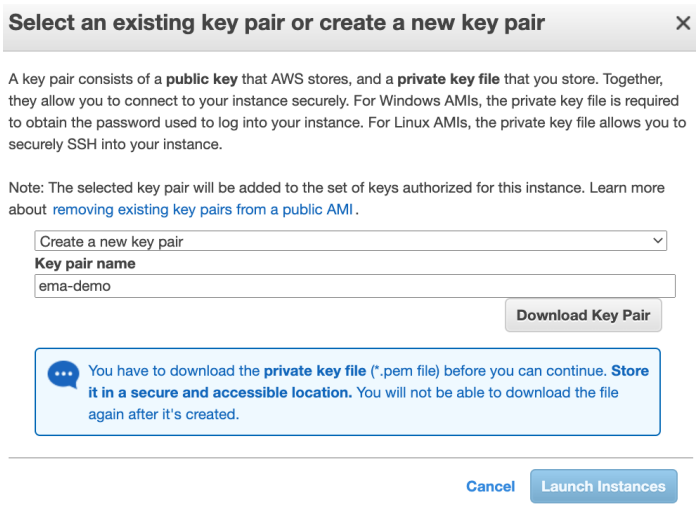
Haga clic en el botón **Next: Review and Launch**.

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



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)

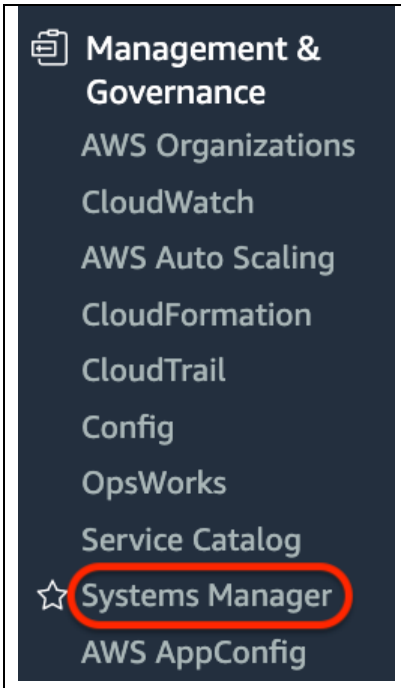
Para las implementaciones de servidores distribuidos, repita el procedimiento anterior para crear el segundo servidor de Intel® EMA mediante la selección de una subred diferente y una etiqueta de nombre diferente, como *ema-server-2*.

6 Configurar AWS Systems Manager (solo para servidores distribuidos)

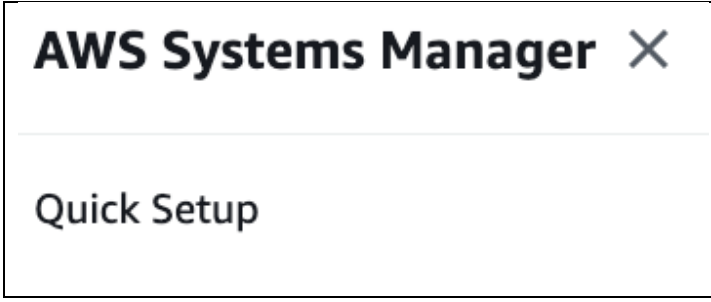
AWS Systems Manager es un servicio que ofrece mayor visibilidad y control de su infraestructura en AWS. Debemos habilitar este servicio para usar el componente Session Manager, el cual nos permitirá tener un acceso remoto a nuestras VMs que no tengan una dirección IP pública.

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

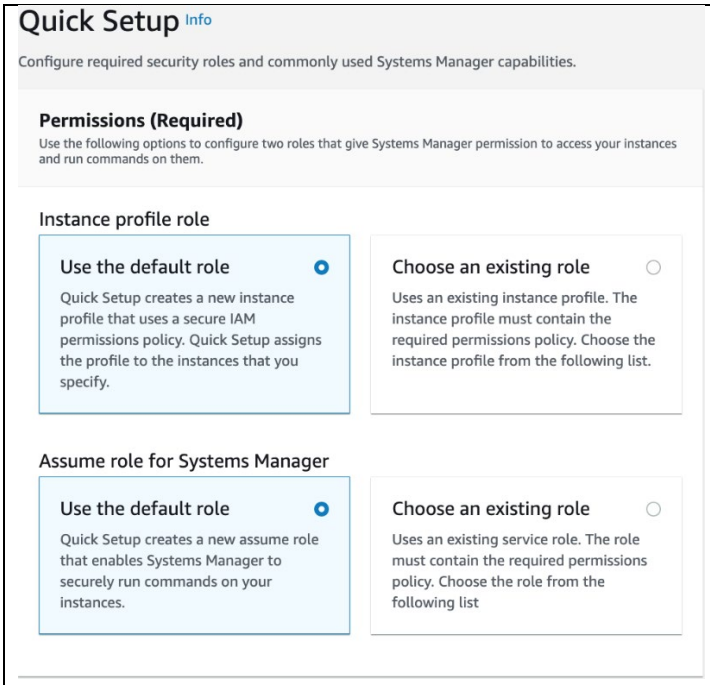
6.1 Ir al servicio Systems Manager

	En el menú Services, en la sección Management & Governance, seleccione Systems Manager.

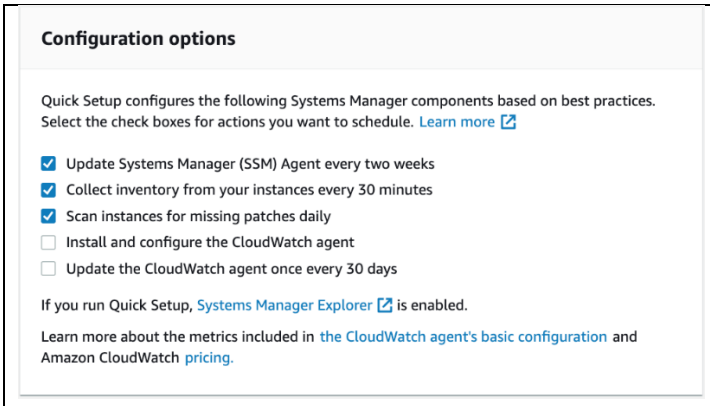
6.2 Comenzar la configuración rápida

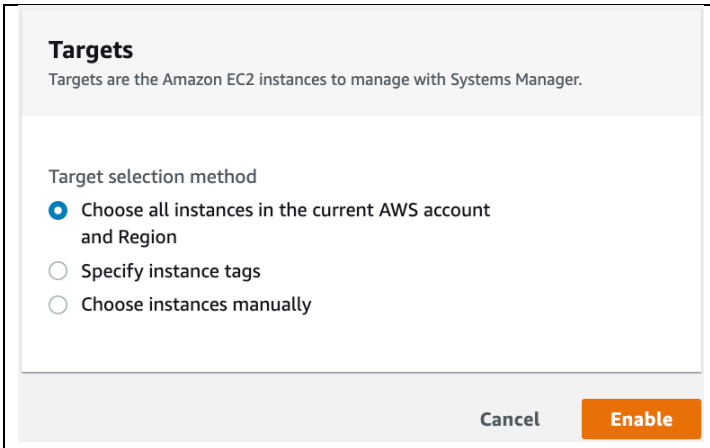
6.3 Seleccionar las opciones de permisos



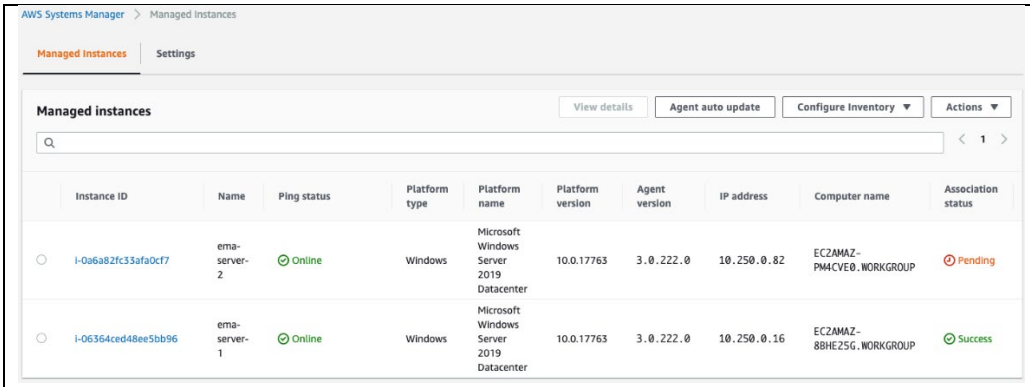
6.4 Seleccionar las opciones de configuración



6.5 Seleccionar los destinos



6.6 Verificar la lista de instancias gestionadas



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-06364ced48e5b96

Si este comando tiene éxito, podrá utilizar un cliente de escritorio remoto para conectarlo al host local en el número de puerto local que especifico. 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.

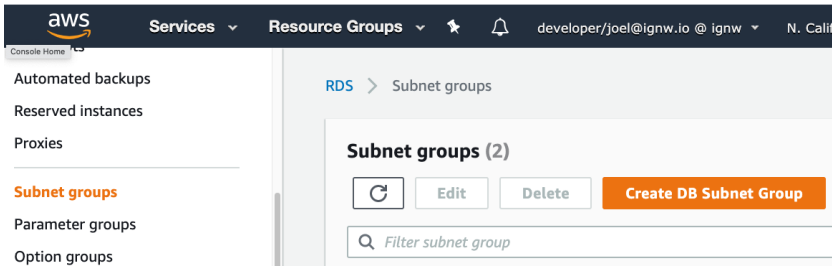
Para obtener más información sobre RDS, visite el siguiente enlace:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

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

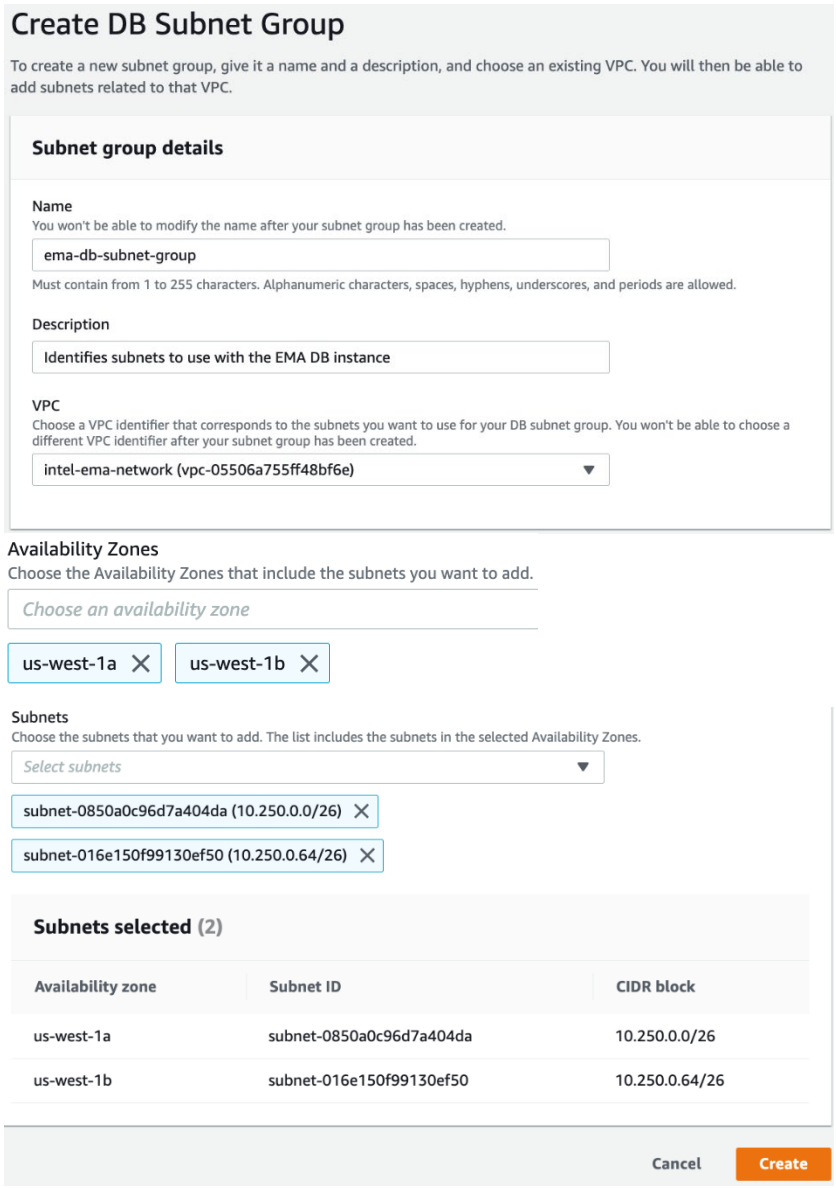
En el menú **Services**, en **Database**, seleccione **RDS**.

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

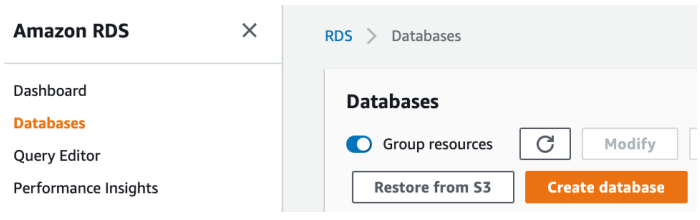


Ingrese los detalles del grupo de subredes de la siguiente manera.

- **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.

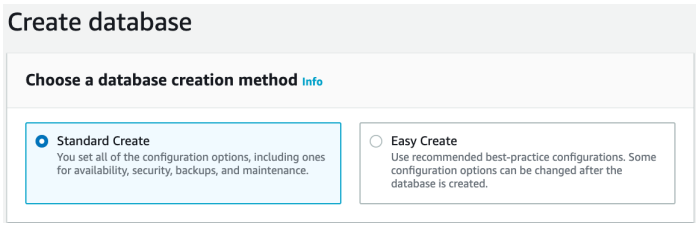
Haga clic en el botón **Create**.

7.3 Crear una base de datos



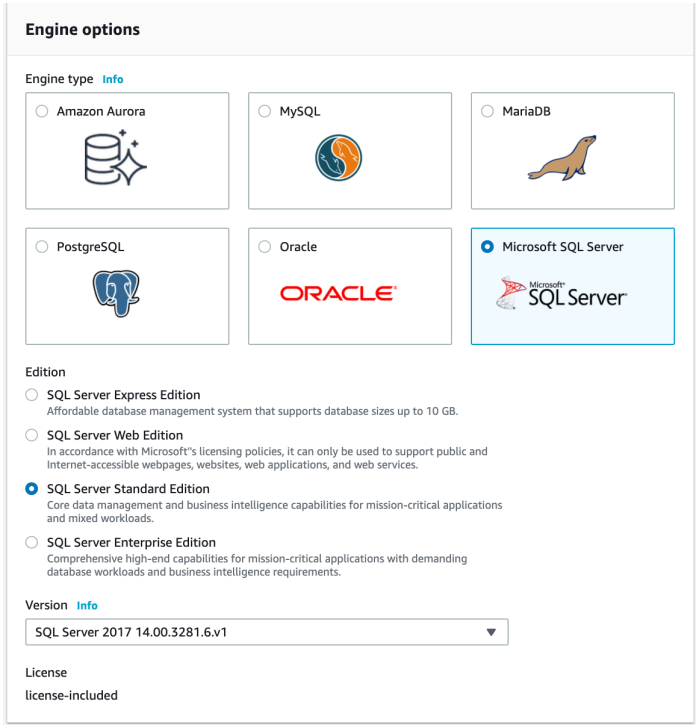
En la barra lateral de RDS, selecciona Databases y, a continuación, haga clic en el botón **Create database**.

7.3.1 Seleccionar el método de creación de la base de datos



Seleccione el método de creación de la base de datos **Standard Create**.

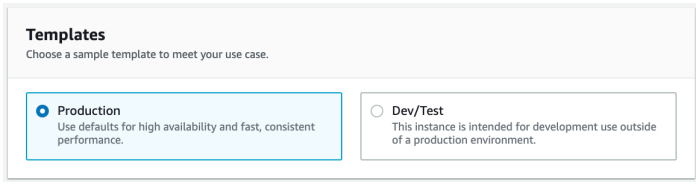
7.3.2 Seleccionar el tipo y la edición del motor



Seleccione el motor **Microsoft SQL Server**.

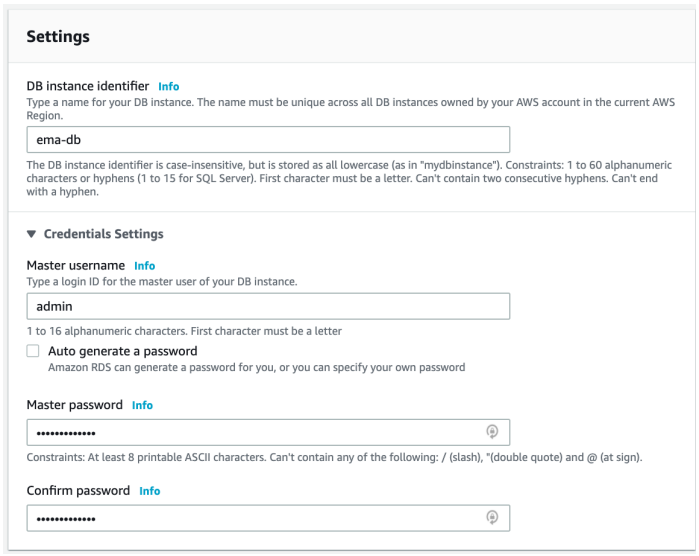
Seleccione la edición apropiada del servidor SQL. En lo que respecta a esta documentación, suponemos una implementación de producción con la edición SQL Server Standard. La edición SQL Server Express podría usarse para las etapas de desarrollo y prueba a fin de reducir costos.

7.3.3 Seleccionar la plantilla de implementación



En Templates, seleccione **Production**.

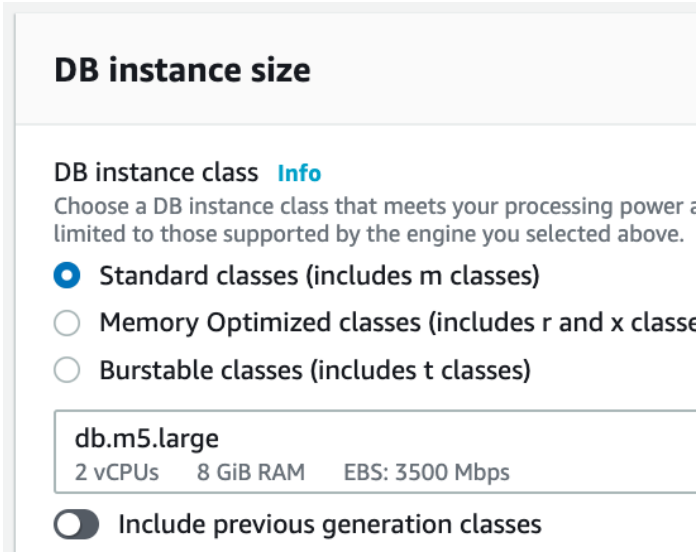
7.3.4 Configurar el nombre de la instancia y las credenciales del usuario maestro



Asigne un nombre único para la base de datos.
Ejemplo: *ema-db*

Cree un nombre de usuario y una contraseña.

7.3.5 Configurar el tamaño de la instancia de DB

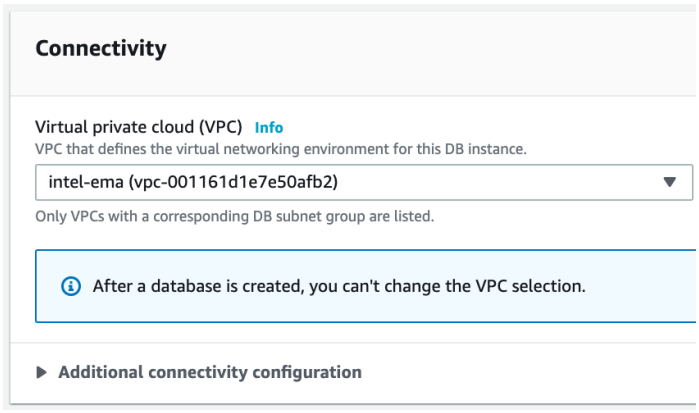


Establezca la clase de instancia de DB para proporcionar los recursos adecuados. Sugerencia: *db.m5.large*

7.3.6 Configurar el almacenamiento (opcional)

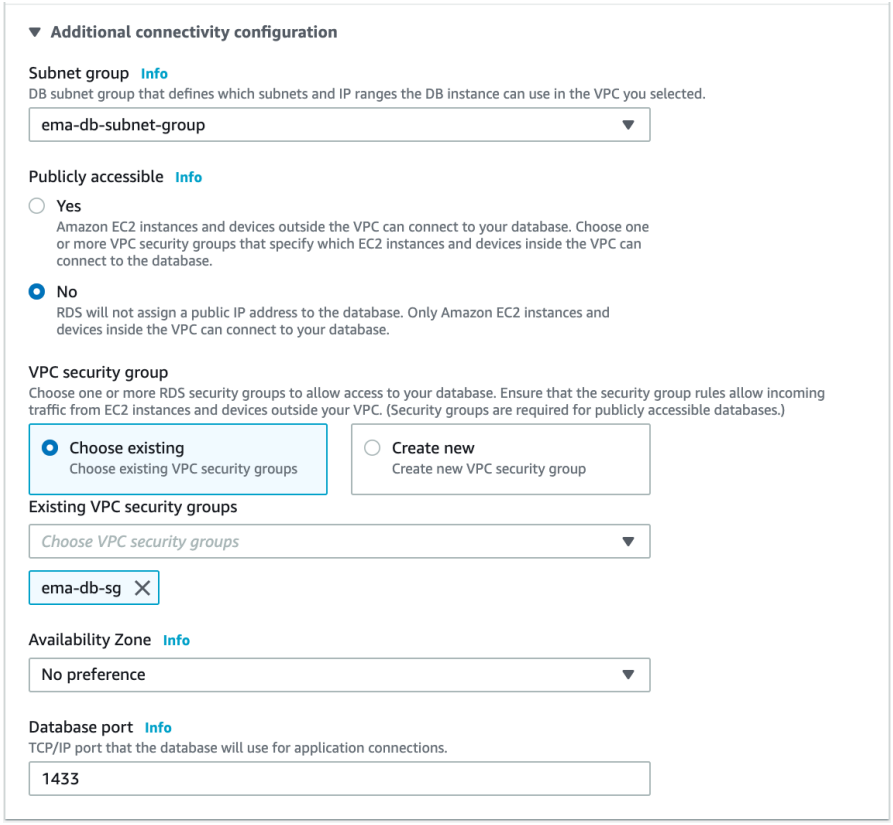
Puede aumentar la cantidad predeterminada del almacenamiento que se asigne según sus necesidades. Ahora, dejaremos el valor predeterminado. Podrá aumentar la capacidad de almacenamiento más adelante.

7.3.7 Configurar la conectividad



En **Connectivity**, seleccione la VPC que creó anteriormente y, a continuación, expanda la sección **Additional connectivity configuration**.

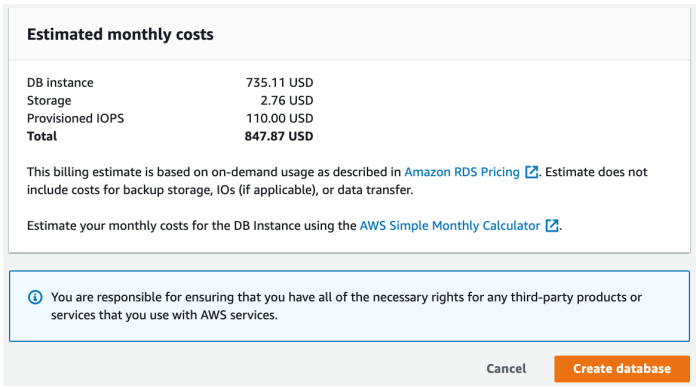
7.3.8 Configurar la conectividad (configuración adicional)



Seleccione el grupo de subredes de base de datos que creó anteriormente.

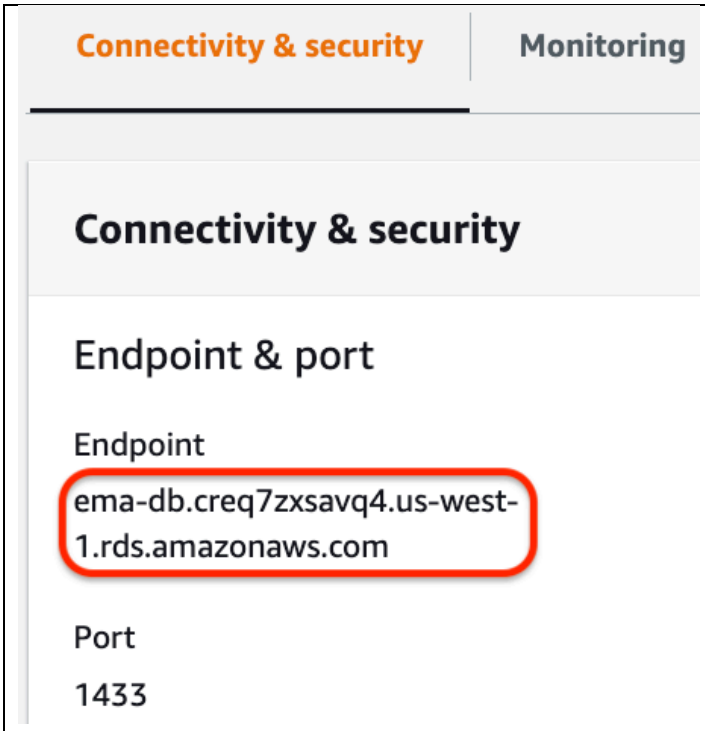
Anule la selección del grupo de seguridad de la VPC predeterminado y elija el que creó anteriormente para la base de datos.

7.3.9 Revisar y crear



Revise el costo estimado y, luego, haga clic en el botón **Create database**.

7.4 Obtener el nombre del host de la base de datos



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.

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.

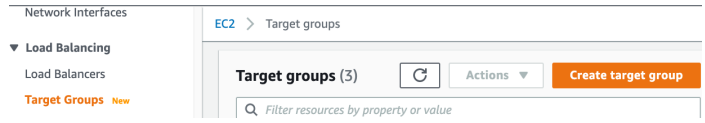
El equilibrador de carga tendrá un nombre de host generado automáticamente que indicará las direcciones de acceso público de los equilibradores de carga relacionados en cada zona de disponibilidad. Se recomienda crear un registro DNS CNAME que cree un alias para ese nombre de host con el fin de usar 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

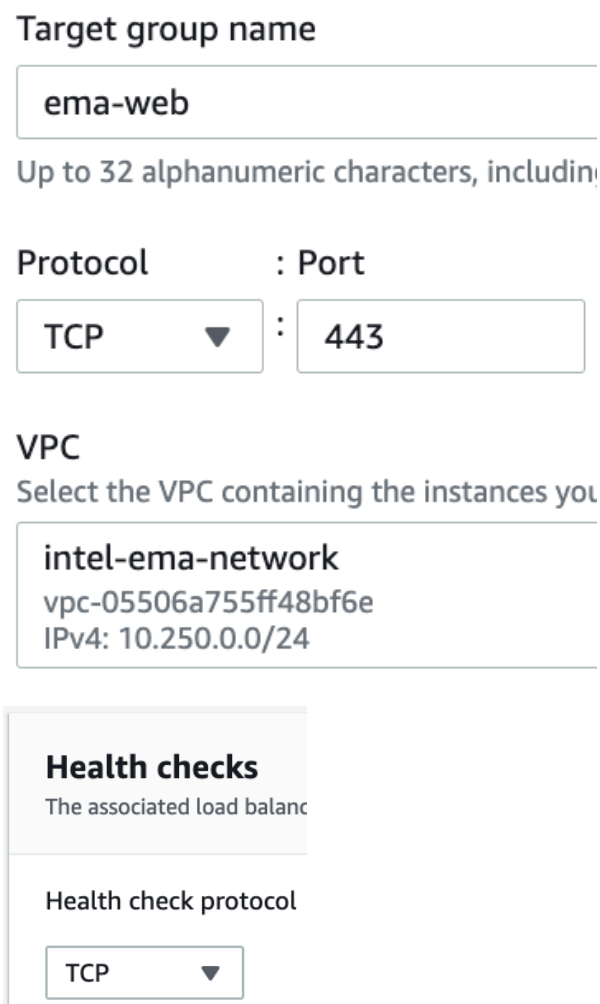
8.2 Crear grupos de destinos

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

	En la barra lateral de **EC2**, en **Load Balancing**, seleccione **Target Groups**. Haga clic en el botón **Create target group**.

8.2.2 Configurar un grupo de destinos para TCP/443

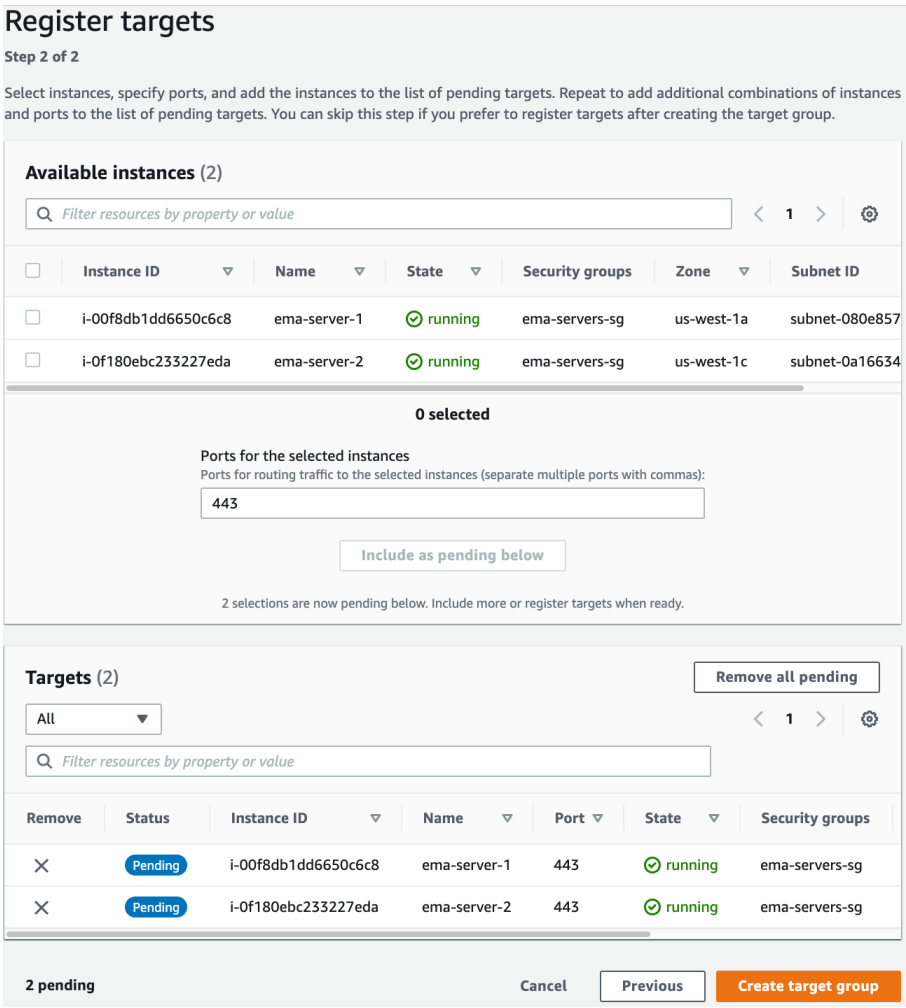


Configure el grupo de destinos de la siguiente manera:

- **Target type**: *Instances*
- **Target group name**: introduzca un nombre único. Ejemplo: *ema-web*
- **Protocol**: *TCP*
- **Port**: *443*
- **VPC**: seleccione la VPC que creó anteriormente.
- **Health check protocol**: *TCP*

Haga clic en **Next** para avanzar a la pantalla **Register targets**.

8.2.2.1 Registre ambas instancias de EC2 como destinos



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

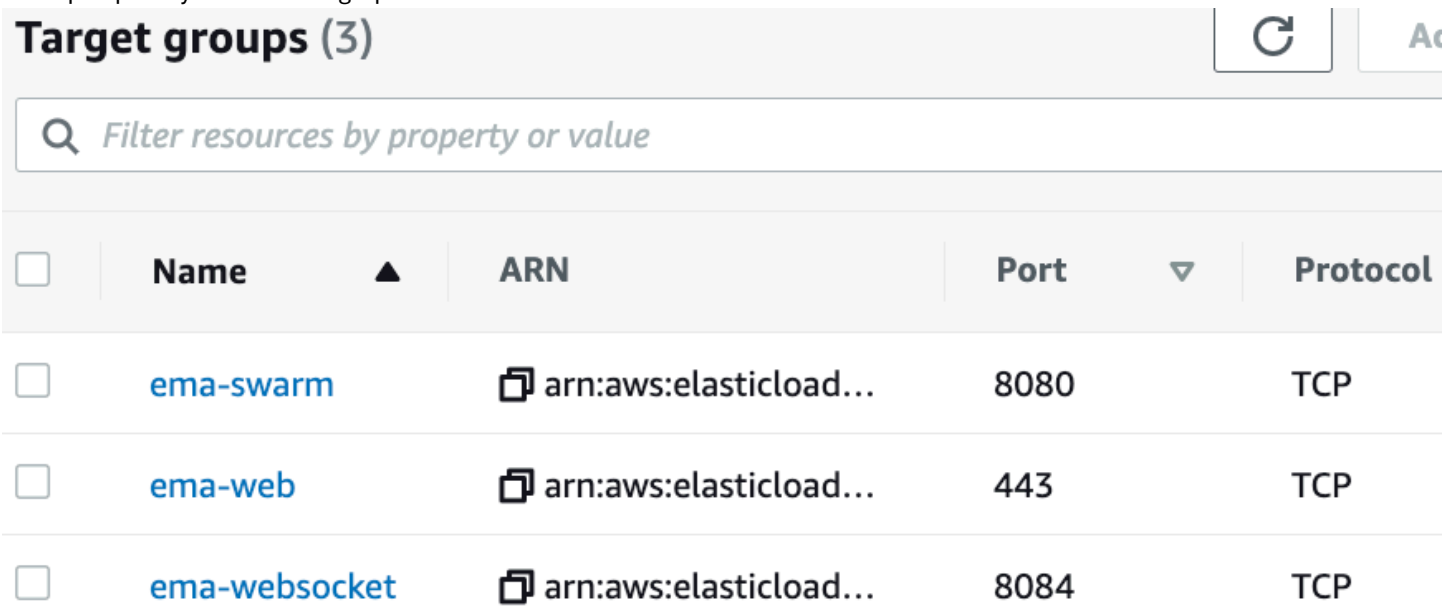
Repita los pasos anteriores en otro grupo de destinos denominado "ema-websocket" para TCP/8084.

8.2.4 Configurar un destino para TCP/8080

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

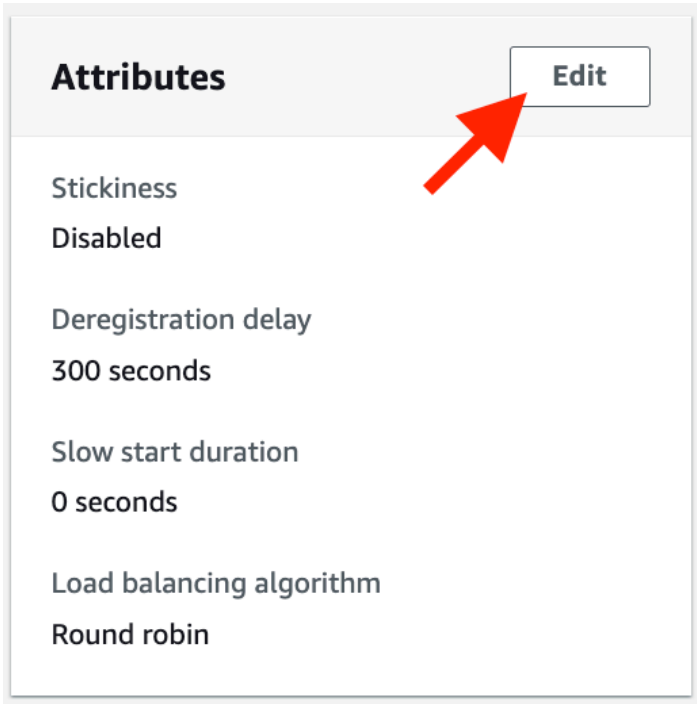
8.2.5 Revisar los grupos de destinos

Verifique que haya creado tres grupos de destinos.

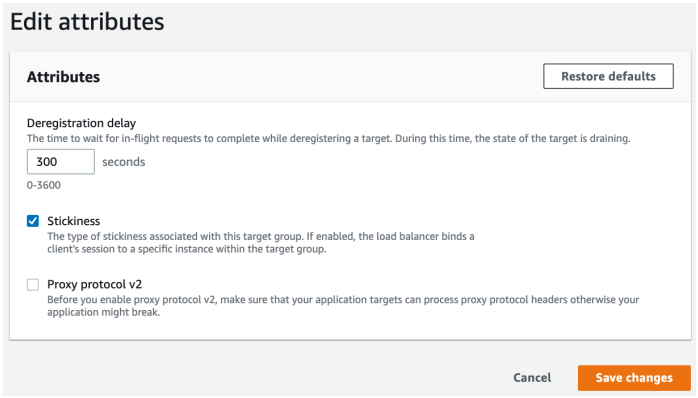


8.2.6 Habilitar la permanencia para el grupo de destinos TCP/443

8.2.6.1 Detalles del grupo de destinos

	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

	Habilite el indicador **Stickiness**. Haga clic en el botón **Save changes**.

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).

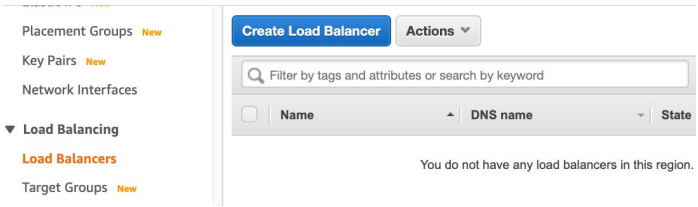
8.2.8 Nota sobre la supervisión del estado del grupo de destinos

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.

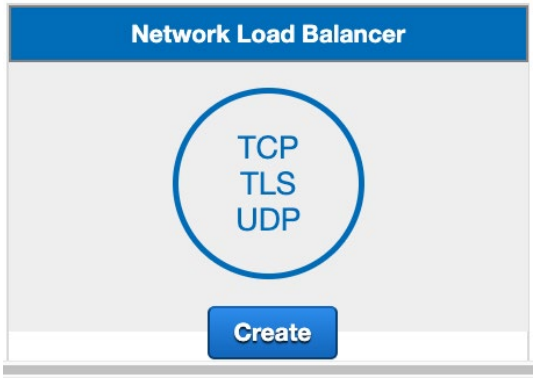
8.3 Crear un equilibrador de carga de red para el tráfico web

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

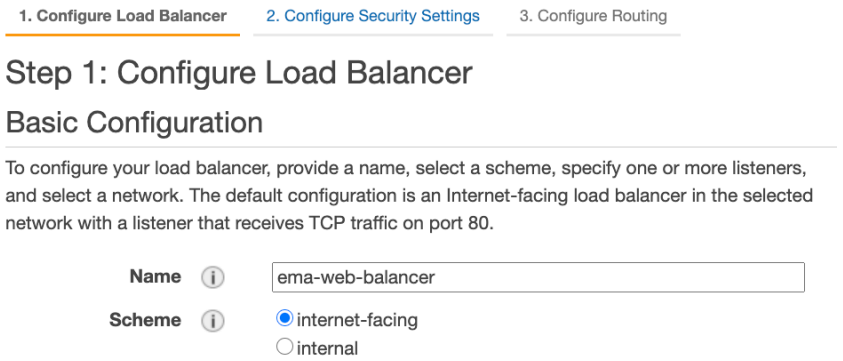
	En la barra lateral de **EC2**, en **Load Balancing**, seleccione **Load Balancers** y haga clic en **Create Load Balancer**.

8.3.2 Seleccionar el tipo de equilibrador de carga

	Haga clic en el botón **Create** en el encabezado **Network Load Balancer**.

8.3.3 Configurar el equilibrador de carga

8.3.3.1 Configuración básica



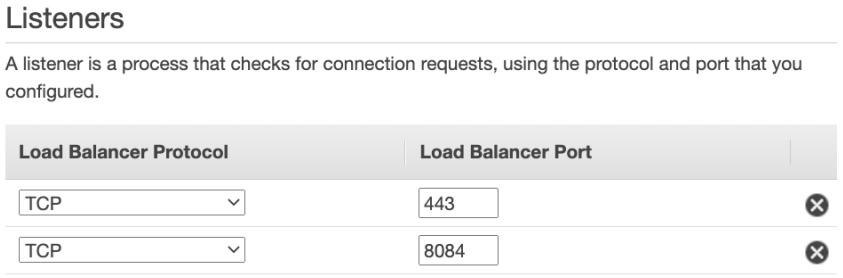
Ingrese la configuración básica.

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.

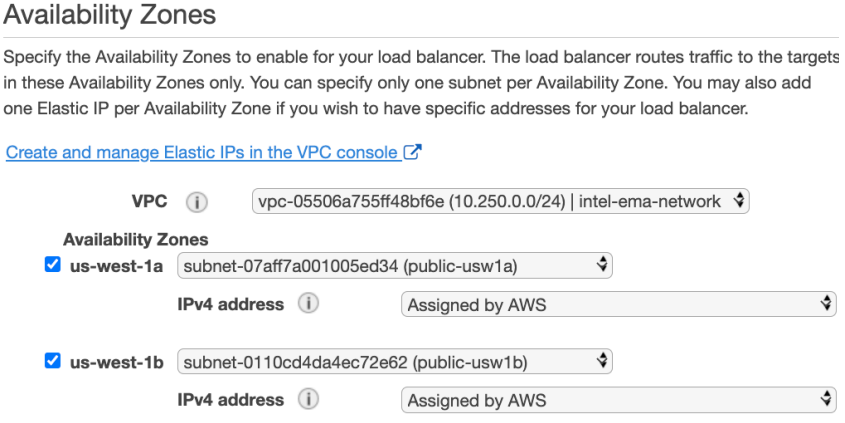
8.3.3.2 Objetos de escucha



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



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

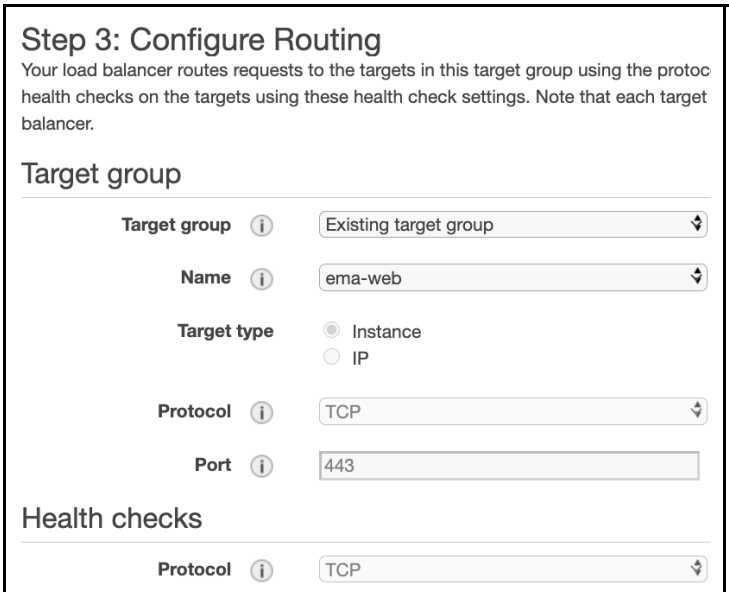
- **VPC**: seleccione la VPC que creó anteriormente.
- **Availability Zones**: habilite ambas zonas de disponibilidad y seleccione ambas subredes públicas. La dirección IPv4 debería establecerse en *Assigned by AWS*.

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

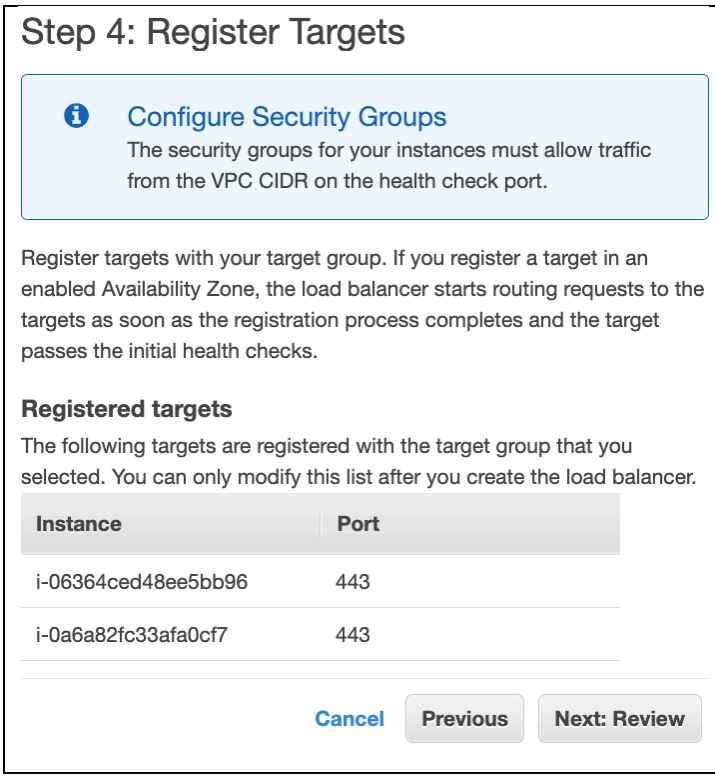


En el **Step 3: Configure Routing**, configure el grupo de destinos de la siguiente manera.

- **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

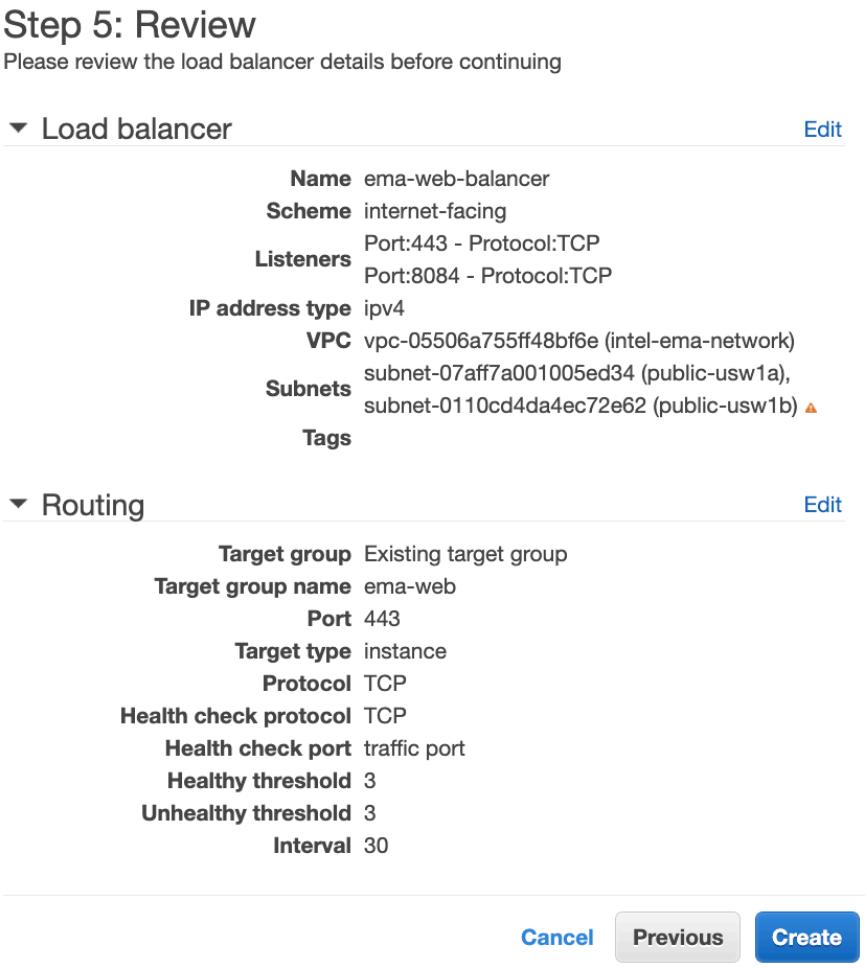


Verifique que vea dos instancias en la lista como destinos registrados.

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

8.3.3.7 Revisar

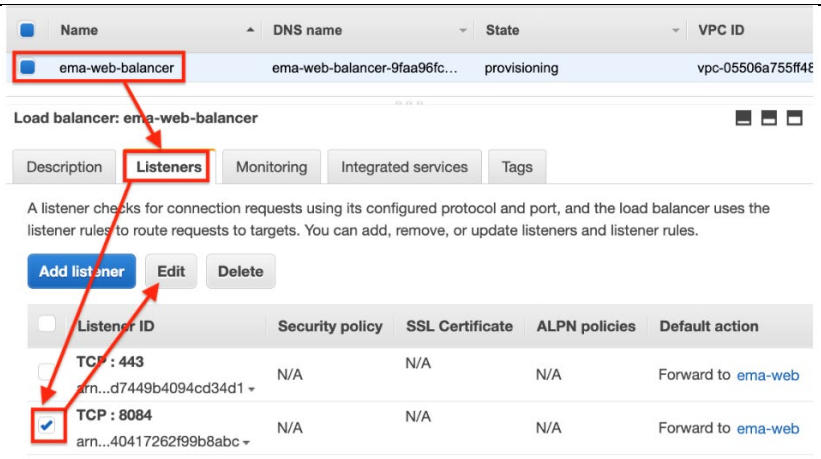
En el **Step 5: Review**, verifique que la configuración se vea similar al ejemplo proporcionado aquí y, luego, haga clic en el botón **Create**.



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



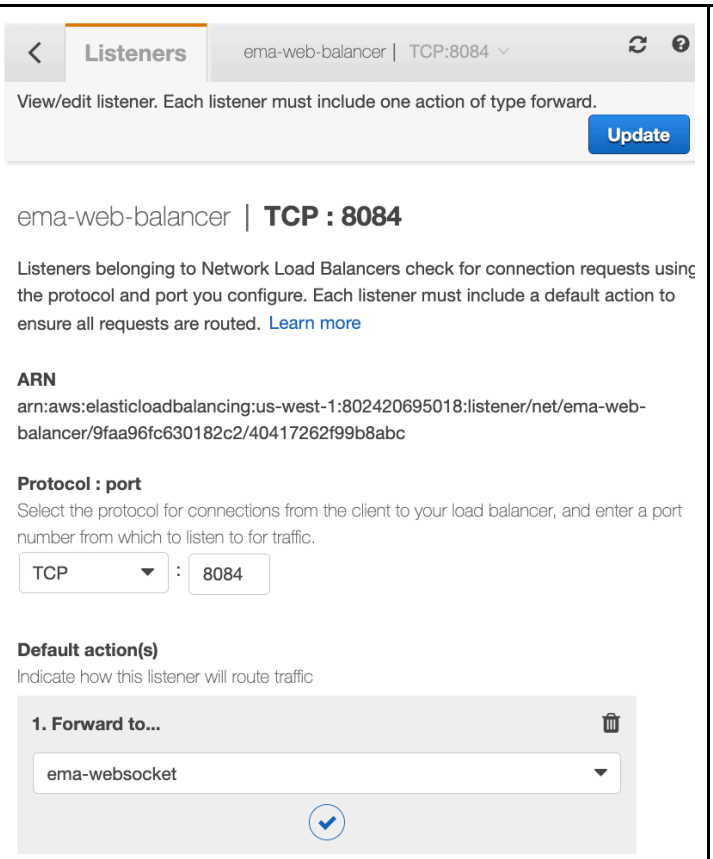
Seleccione el equilibrador de carga que creó.

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

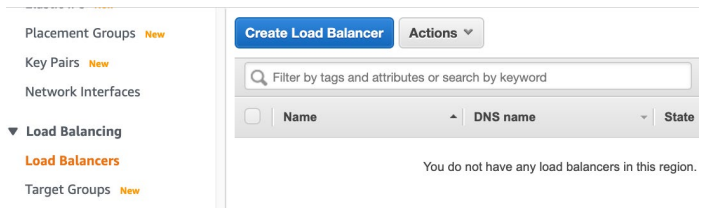


Cambie la acción predeterminada de reenvío al objeto de escucha de WebSocket.

Haga clic en el botón **Update**.

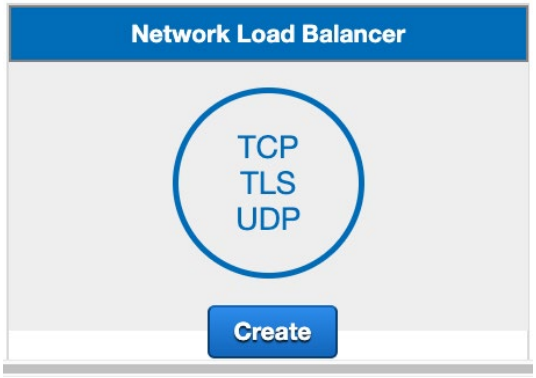
8.4 Crear un equilibrador de carga de red para el tráfico Swarm

8.4.1 Crear el equilibrador de carga



En la barra lateral de **EC2**, en **Load Balancing**, seleccione **Load Balancers** y haga clic en **Create Load Balancer**.

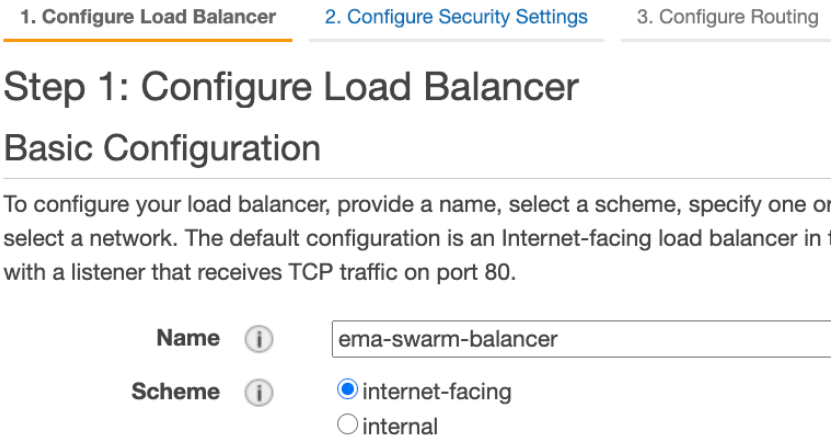
8.4.2 Seleccionar el tipo de equilibrador de carga



Haga clic en el botón **Create** en el encabezado **Network Load Balancer**.

8.4.3 Configurar el equilibrador de carga

8.4.3.1 Configuración básica

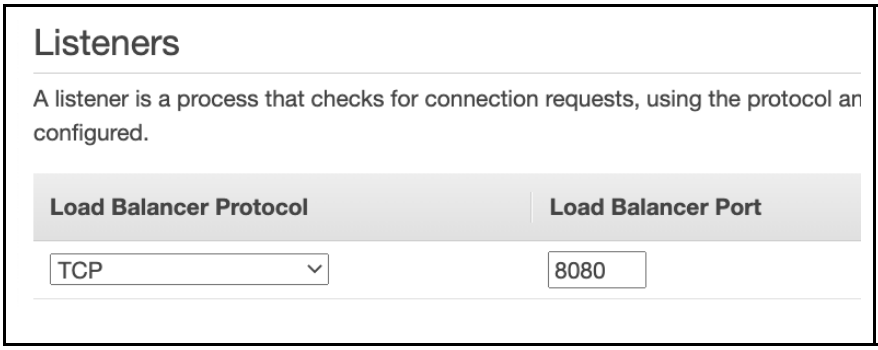


Ingrese la configuración básica.

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

Scheme: internet-facing.

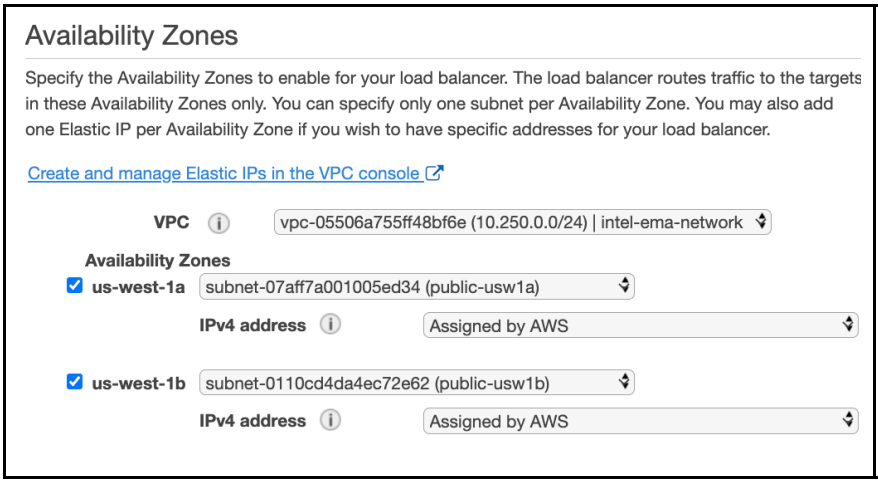
8.4.3.2 Objetos de escucha



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

- *TCP 8080*

8.4.3.3 Zonas de disponibilidad



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

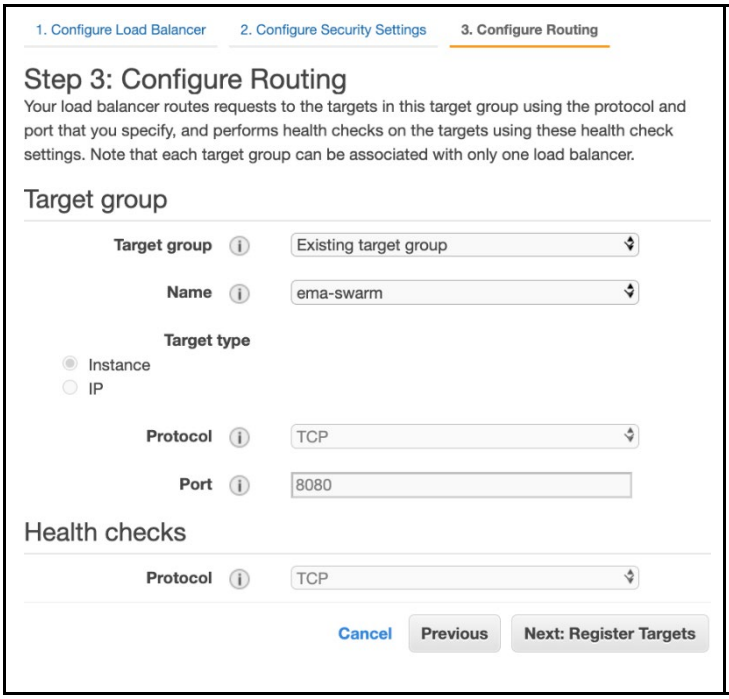
- **VPC**: seleccione la VPC que creó anteriormente.
- **Availability Zones**: habilite ambas zonas de disponibilidad y seleccione ambas subredes públicas. La dirección IPv4 debería establecerse en *Assigned by AWS*.

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

8.4.3.4 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



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/8080 que creó anteriormente.
  Ejemplo: *ema-swarm*

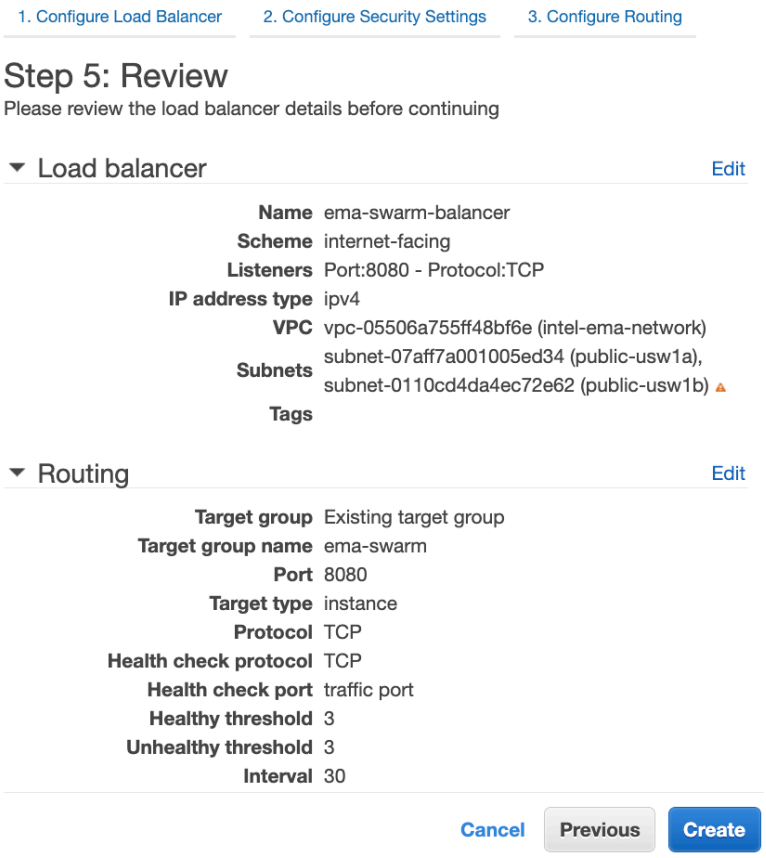
Haga clic en el botón **Next: Register Targets**.

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**.

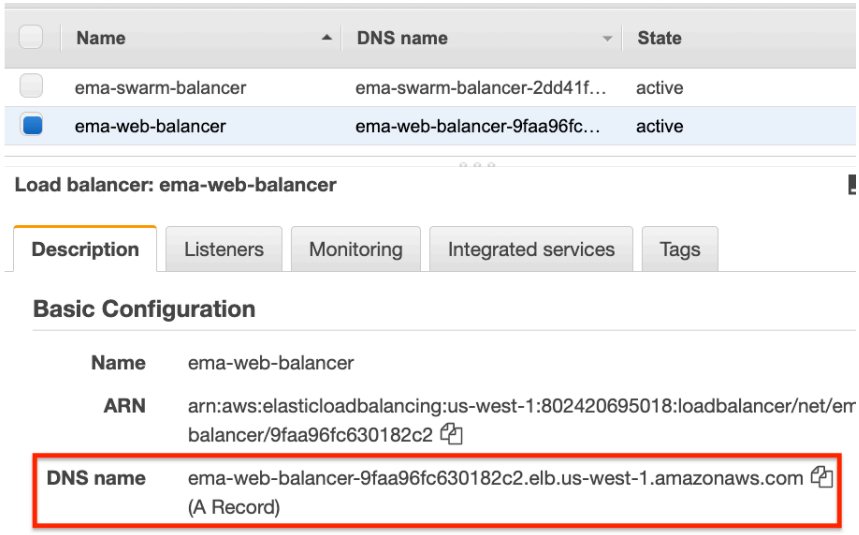
8.4.3.7 Revisar

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



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.


Name
DNS name
State
ema-swarm-balancer
ema-swarm-balancer-2dd41f…
active
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/em
balancer/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*

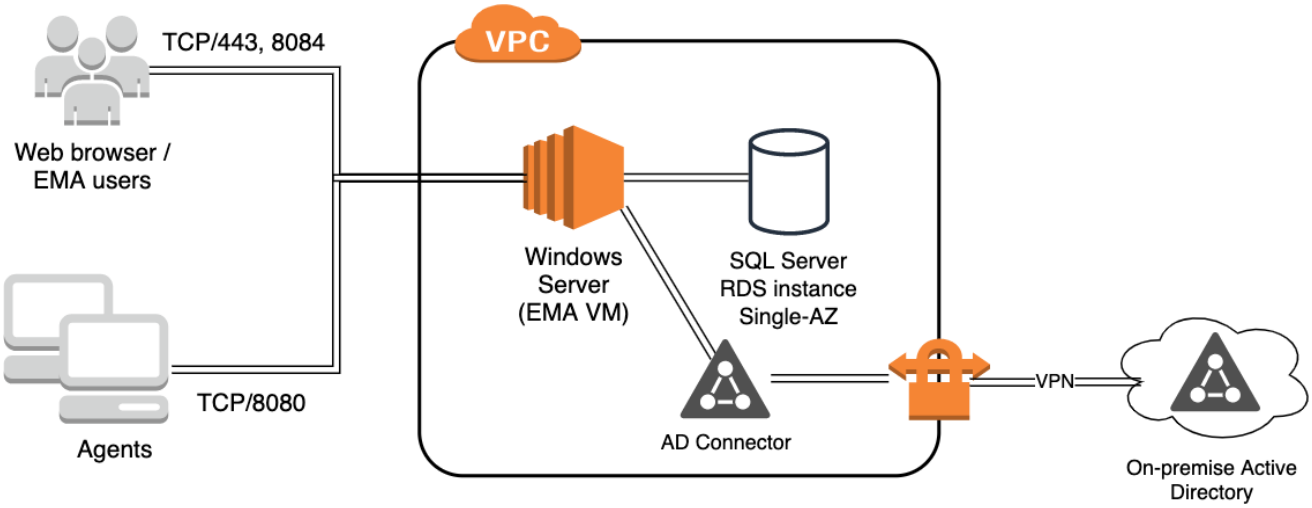
Existen varias maneras de integrar Active Directory* (AD) con AWS para poder conectar sus máquinas virtuales a un dominio y usar la autenticación de AD. Debido a que las necesidades de las organizaciones pueden ser bien diferentes, este apéndice solo proporciona algunos indicadores breves sobre como 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:

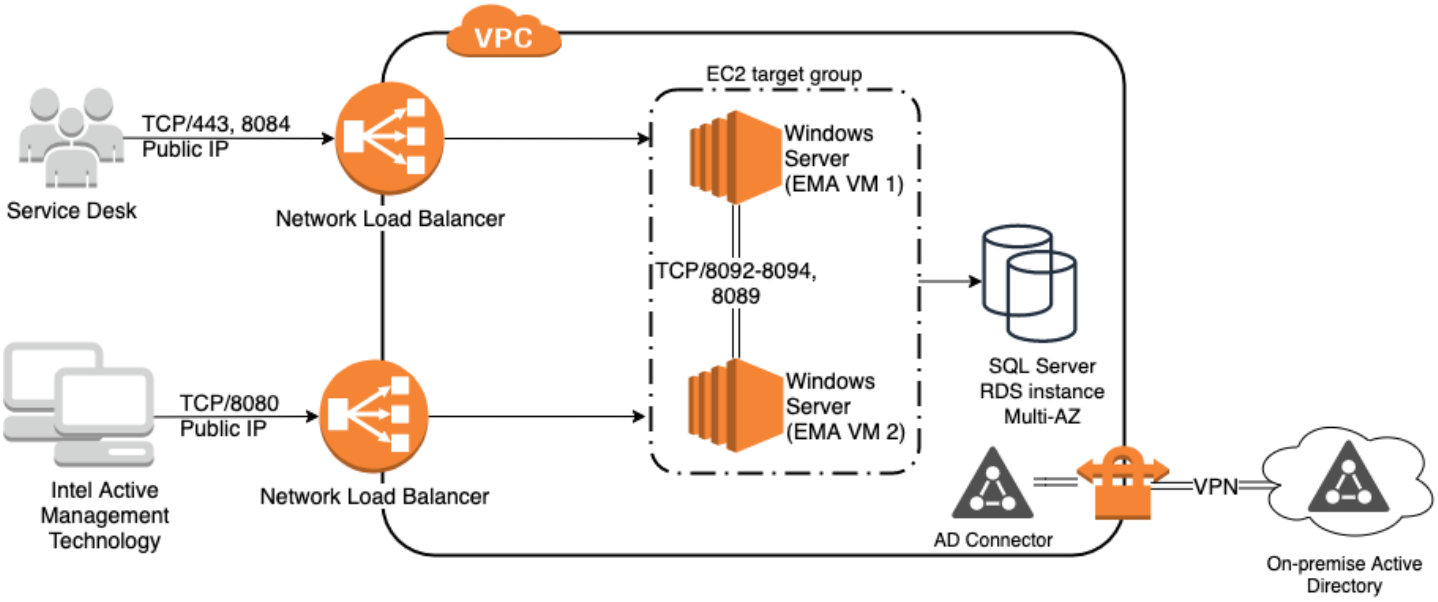
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html
https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq_connector.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.