



Guía del usuario

# AWS PCS



# AWS PCS: Guía del usuario

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

---

# Table of Contents

¿Qué es AWS PCS? .....	1
Conceptos .....	1
Comience con AWS PCS .....	3
Requisitos previos .....	5
Regístrese AWS y cree un usuario administrativo .....	5
Instale el AWS CLI para AWS PCS .....	7
Permisos de IAM necesarios .....	7
Usando AWS CloudFormation .....	8
Creación de una VPC y de subredes .....	8
Busque el grupo de seguridad predeterminado para la VPC del clúster .....	10
Cree grupos de seguridad .....	10
Creación de grupos de seguridad .....	10
Creación de un clúster .....	11
Cree almacenamiento compartido en Amazon EFS .....	12
Cree almacenamiento compartido en FSx for Lustre .....	13
Cree grupos de nodos de cómputo .....	14
Creación de un perfil de instancia .....	15
Creación de plantillas de lanzamiento .....	16
Cree un grupo de nodos de computación para los nodos de inicio de sesión .....	18
Cree un grupo de nodos de cómputo para los trabajos .....	19
Creación de una cola .....	20
Conéctese a su clúster .....	21
Explore el entorno de clústeres .....	22
Cambiar de usuario .....	23
Trabaje con sistemas de archivos compartidos .....	23
Interactúa con Slurm .....	23
Ejecute un trabajo de un solo nodo .....	24
Ejecute un trabajo de MPI de varios nodos con Slurm .....	26
Elimine sus AWS recursos .....	29
Comience con un AWS CloudFormation AWS PCS .....	32
Se utiliza AWS CloudFormation para crear un clúster .....	32
Conexión a un clúster .....	34
Limpiar un clúster .....	35
Partes de una CloudFormation plantilla para AWS PCS .....	35

Encabezado .....	36
Metadatos .....	36
Parámetros .....	37
Mapeos .....	38
Recursos .....	39
Salidas .....	43
Plantillas para crear un clúster de muestra .....	44
Clústeres .....	46
Creación de un clúster .....	46
Requisitos previos .....	47
Cree un clúster de AWS PCS .....	47
Eliminación de un clúster .....	51
Consideraciones a la hora de eliminar un clúster de AWS PCS .....	51
Elimine el clúster .....	52
Tamaño del clúster .....	52
Secretos de clústeres .....	53
Se usa AWS Secrets Manager para buscar el secreto del clúster .....	54
Utilice AWS PCS para encontrar el secreto del clúster .....	55
Obtén el secreto del cúmulo de Slurm .....	56
Grupos de nodos de cómputo .....	58
Crear un grupo de nodos de cómputo .....	58
Requisitos previos .....	58
Cree un grupo de nodos de cómputo en PCS AWS .....	59
Actualización de un grupo de nodos de cómputo .....	64
Opciones para actualizar un grupo de nodos de cómputo de AWS PCS .....	64
Consideraciones a la hora de actualizar un grupo de nodos de procesamiento de AWS PCS .....	65
Para actualizar un grupo de nodos de cómputo de AWS PCS .....	66
Eliminar un grupo de nodos de cómputo .....	67
Consideraciones a la hora de eliminar un grupo de nodos de cómputo .....	68
Elimine el grupo de nodos de cómputo .....	68
Obtenga detalles del grupo de nodos de cómputo .....	69
Búsqueda de instancias de grupos de nodos de cómputo .....	72
Uso de plantillas de lanzamiento .....	75
Descripción general .....	75
Creación de una plantilla de lanzamiento básica .....	77

Trabajar con datos de EC2 usuario de Amazon .....	79
Ejemplo: instalar software desde un repositorio de paquetes .....	81
Ejemplo: ejecutar scripts desde un bucket de S3 .....	81
Ejemplo: establecer variables de entorno globales .....	83
Ejemplo: utilizar un sistema de archivos EFS como directorio principal compartido .....	83
Reservas de capacidad .....	85
Se utiliza ODCRs con PCS AWS .....	85
Parámetros útiles de la plantilla de lanzamiento .....	87
Active la CloudWatch supervisión detallada .....	87
Instance Metadata Service, versión 2 (IMDS v2) .....	88
Colas .....	89
Creación de una cola .....	89
Requisitos previos .....	89
Para crear una cola en PCS AWS .....	89
Actualización de una cola .....	91
Consideraciones a la hora de actualizar una cola de AWS PCS .....	91
Para actualizar una cola de PCS AWS .....	91
Eliminación de una cola .....	93
Consideraciones a la hora de eliminar una cola .....	93
Eliminación de la cola .....	93
Nodos de inicio de sesión .....	95
Uso de un grupo de nodos de cómputo para iniciar sesión .....	95
Crear un grupo de nodos de cómputo de AWS PCS para los nodos de inicio de sesión .....	95
Actualización de un grupo de nodos de procesamiento de AWS PCS para los nodos de inicio de sesión .....	96
Eliminar un grupo de nodos de cómputo de AWS PCS para los nodos de inicio de sesión .....	97
Uso de instancias independientes como nodos de inicio de sesión .....	97
Paso 1: Recupere la dirección y el secreto del clúster de AWS PCS de destino .....	98
Paso 2: lanzar una EC2 instancia .....	99
Paso 3: Instala Slurm en la instancia .....	100
Paso 4: Recupere y almacene el secreto del clúster .....	100
Paso 5: Configurar la conexión al clúster de PCS AWS .....	101
Paso 6: (opcional) Pruebe la conexión .....	103
Red .....	104
Requisitos de VPC y subred .....	104
Requisitos y consideraciones de la VPC .....	104

Requisitos y consideraciones de la subred .....	105
Creación de una VPC .....	106
Requisitos previos .....	107
Creación de una Amazon VPC .....	107
Grupos de seguridad .....	109
Requisitos del grupo de seguridad .....	109
Múltiples interfaces de red .....	111
Grupos de ubicación .....	112
Uso del Elastic Fabric Adapter (EFA) .....	113
Identifique las instancias habilitadas para EFA EC2 .....	114
Cree un grupo de seguridad para respaldar las comunicaciones de la EFA .....	114
(Opcional) Cree un grupo de ubicación .....	116
Cree o actualice una plantilla de EC2 lanzamiento .....	116
Cree o actualice grupos de nodos de cómputo para EFA .....	117
(Opcional) Pruebe la EFA .....	117
(Opcional) Usa una CloudFormation plantilla para crear una plantilla de lanzamiento compatible con la EFA .....	119
Sistemas de archivos de red .....	122
Consideraciones sobre el uso de sistemas de archivos de red .....	122
Ejemplos de montajes de red .....	123
Imágenes de máquinas de Amazon (AMIs) .....	129
Uso de una muestra AMIs .....	129
Encuentre un ejemplo de AWS PCS actual AMIs .....	129
Obtenga más información sobre el ejemplo de AWS PCS AMIs .....	131
Cree la suya propia AMIs compatible con AWS PCS .....	131
Personalizado AMIs .....	131
Paso 1: Lanzar una instancia temporal .....	132
Paso 2: Instalar el agente AWS PCS .....	133
Paso 3: Instalar Slurm .....	136
Paso 4: (opcional) Instalar controladores, bibliotecas y software de aplicación adicionales ..	138
Paso 5: Crear una AMI compatible con AWS PCS .....	139
Paso 6: Utilice la AMI personalizada con un grupo de nodos de cómputo de AWS PCS .....	140
Paso 7: Finalizar la instancia temporal .....	141
Instaladores para construir AMIs .....	142
AWS Instalador del software PCS Agent .....	142
Instalador de Slurm .....	143

Sistemas operativos compatibles .....	144
Tipos de instancias admitidas .....	144
Versiones de Slurm compatibles .....	144
Verifique los instaladores mediante una suma de verificación .....	145
Notas de lanzamiento para AMIs .....	148
Ejemplo de x86_64 AMIs () AL2 .....	149
Ejemplo AMIs de Arm64 () AL2 .....	151
Sistemas operativos compatibles .....	154
AWS Versiones del agente PCS .....	156
Versiones Slurm .....	158
Versiones de Slurm compatibles en PCS AWS .....	158
Notas de la versión .....	160
Preguntas frecuentes .....	162
Contabilidad Slurm .....	165
Conceptos clave .....	166
Base de datos de contabilidad .....	166
Tiempo de purga predeterminado .....	166
Aplicación de la política contable .....	167
Obtenga la configuración de contabilidad de un clúster de AWS PCS existente .....	168
Seguridad .....	169
Protección de los datos .....	170
Cifrado en reposo .....	171
Cifrado en tránsito .....	171
Administración de claves .....	172
Privacidad del tráfico entre redes .....	172
Cifrar el tráfico de la API .....	173
Cifrado del tráfico de datos .....	173
Política de claves de KMS para volúmenes de EBS cifrados .....	173
Puntos finales de la interfaz VPC ()AWS PrivateLink .....	180
Consideraciones .....	180
Creación de un punto de conexión de interfaz .....	180
Creación de una política de punto de conexión .....	181
Identity and Access Management .....	182
Público .....	183
Autenticación con identidades .....	183
Administración de acceso mediante políticas .....	187

Cómo funciona AWS Parallel Computing Service con IAM .....	190
Ejemplos de políticas basadas en identidades .....	197
AWS políticas gestionadas .....	201
Roles vinculados a servicios .....	207
EC2 Rol de Spot .....	209
Permisos mínimos .....	210
Perfiles de instancias .....	216
Solución de problemas .....	219
Validación de conformidad .....	221
Resiliencia .....	222
Seguridad de infraestructuras .....	222
Análisis y administración de vulnerabilidades .....	223
Prevención de la sustitución confusa entre servicios .....	224
Función de IAM para EC2 instancias de Amazon aprovisionadas como parte de un grupo de nodos de cómputo .....	225
Prácticas recomendadas de seguridad .....	226
Seguridad relacionada con la AMI .....	226
Seguridad de Slurm Workload Manager .....	227
Supervisión y registro .....	227
Seguridad de la red .....	227
Registro y supervisión .....	229
AWS Registros del programador PCS .....	229
Requisitos previos .....	230
Configuración de los registros del programador mediante la AWS consola PCS .....	230
Configurar los registros del programador mediante el AWS CLI .....	231
Rutas y nombres de los flujos de registro del programador .....	233
Ejemplo de registro del programador AWS PCS .....	234
Monitorización con CloudWatch .....	234
Supervisión de métricas .....	235
Monitorización de instancias de .....	236
CloudTrail registros .....	245
AWS Información sobre el PCS en CloudTrail .....	245
Descripción de las entradas de los archivos de CloudTrail registro del AWS PCS .....	246
Puntos de conexión y Service Quotas .....	249
Puntos de conexión de servicio .....	249
Service Quotas .....	250

---

Cuotas internas .....	251
Cuotas relevantes para otros servicios AWS .....	251
Solución de problemas .....	253
EC2 la instancia se termina y se reemplaza después del reinicio .....	253
Historial de documentos .....	255
AWS Glosario .....	266
.....	cclxvii

# ¿Qué es el Servicio de Computación AWS Paralela?

AWS El servicio de computación paralela (AWS PCS) es un servicio gestionado que facilita la ejecución y el escalado de las cargas de trabajo de computación de alto rendimiento (HPC) y la creación de modelos científicos y de ingeniería AWS con Slurm. Utilice AWS PCS para crear clústeres de procesamiento que integren los mejores recursos de AWS computación, almacenamiento, redes y visualización de su clase. Ejecute simulaciones o cree modelos científicos y de ingeniería. Optimice y simplifique las operaciones de sus clústeres mediante las funciones integradas de administración y observabilidad. Permita que sus usuarios se centren en la investigación y la innovación al permitirles ejecutar sus aplicaciones y trabajos en un entorno familiar.

## Temas

- [Conceptos en AWS PCS](#)

## Conceptos en AWS PCS

En AWS PCS, un clúster tiene una o más colas asociadas a al menos un grupo de nodos de cómputo. Los trabajos se envían a colas y se ejecutan en EC2 instancias definidas por grupos de nodos de procesamiento. Puede utilizar estas bases para implementar arquitecturas de HPC sofisticadas.

### Clúster

Un clúster es un recurso para gestionar los recursos y ejecutar las cargas de trabajo. Un clúster es un recurso de AWS PCS que define un conjunto de configuraciones de procesamiento, redes, almacenamiento, identidad y programador de tareas. Para crear un clúster, especifique qué programador de tareas desea usar (actualmente Slurm), qué configuración de programador desea, qué controlador de servicios desea administrar el clúster y en qué VPC desea que se lancen los recursos del clúster. El programador acepta y programa los trabajos, y también lanza los nodos de cómputo (EC2 instancias) que procesan esos trabajos.

### Grupo de nodos de cómputo

Un grupo de nodos de procesamiento es un conjunto de nodos de procesamiento que AWS PCS utiliza para ejecutar trabajos o proporcionar acceso interactivo a un clúster. Al definir un grupo de nodos de cómputo, se especifican características comunes, como los tipos de EC2 instancias de Amazon, el número mínimo y máximo de instancias, las subredes de VPC de destino, la imagen de

máquina de Amazon (AMI), la opción de compra y la configuración de lanzamiento personalizada. AWS PCS usa esta configuración para lanzar, administrar y terminar de manera eficiente los nodos de cómputo de un grupo de nodos de cómputo.

## Cola

Cuando quiere ejecutar un trabajo en un clúster específico, lo envía a una cola determinada (también denominada partición). El trabajo permanece en la cola hasta que AWS PCS lo programe para que se ejecute en un grupo de nodos de procesamiento. Asocia uno o más grupos de nodos de cómputo a cada cola. Se necesita una cola para programar y ejecutar los trabajos en los recursos del grupo de nodos de cómputo subyacentes mediante diversas políticas de programación ofrecidas por el programador de trabajos. Los usuarios no envían los trabajos directamente a un nodo de cómputo o a un grupo de nodos de cómputo.

## Administrador de sistemas

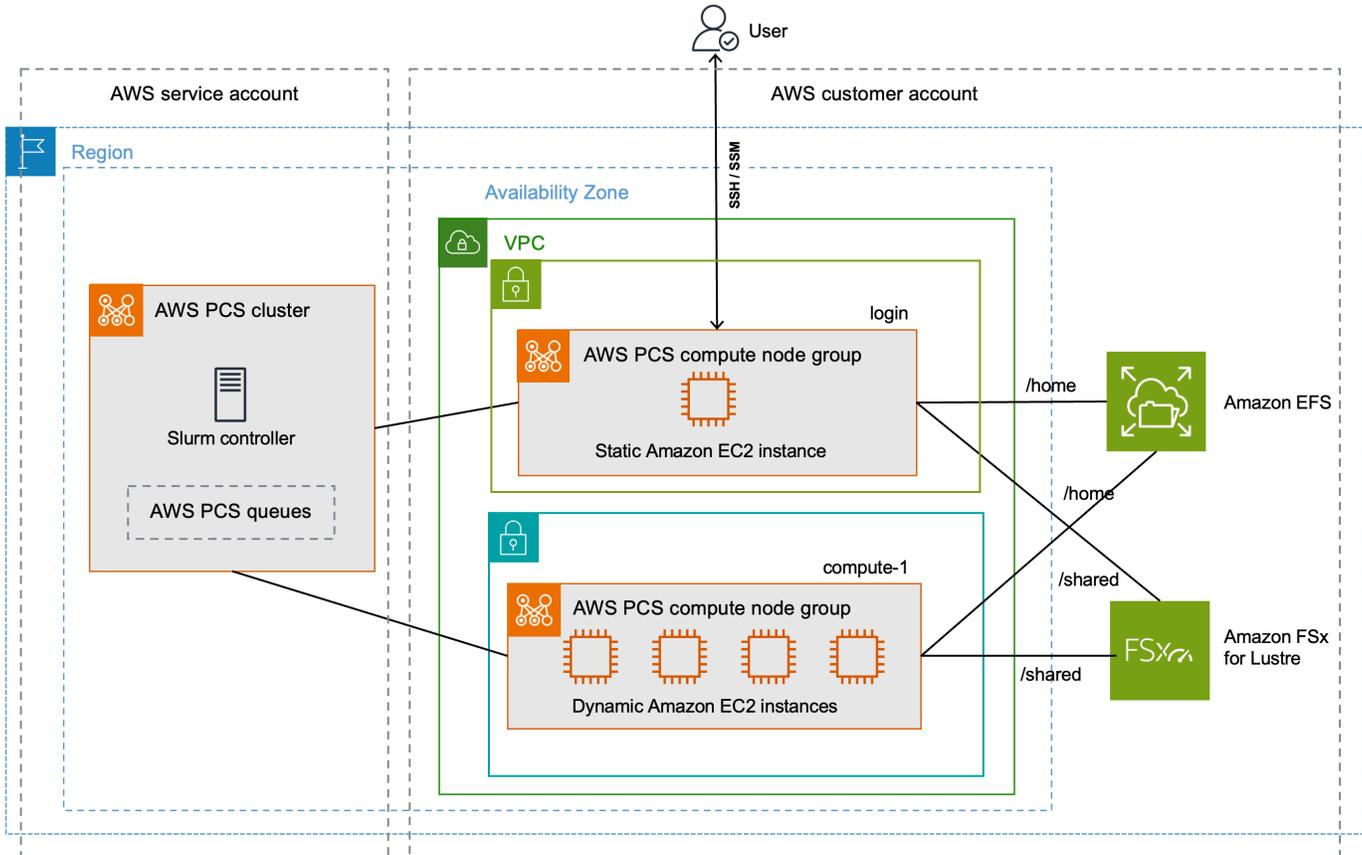
Un administrador del sistema implementa, mantiene y opera un clúster. Pueden acceder a AWS PCS a través de la AWS Management Console API de AWS PCS y el AWS SDK. Tienen acceso a clústeres específicos a través de SSH o AWS Systems Manager, donde pueden ejecutar tareas administrativas, ejecutar trabajos, administrar datos y realizar otras actividades basadas en el shell. Para obtener más información, consulte la Documentación de [AWS Systems Manager](#).

## Usuario final

El usuario final no tiene day-to-day la responsabilidad de implementar u operar un clúster. Utilizan una interfaz de terminal (como SSH) para acceder a los recursos del clúster, ejecutar tareas, administrar datos y realizar otras actividades basadas en el shell.

# Comience con AWS Parallel Computing Service

Este es un tutorial para crear un clúster sencillo que puede utilizar para probar AWS PCS. En la siguiente figura se muestra el diseño del clúster.



El tutorial sobre diseño de clústeres incluye los siguientes componentes clave:

- Una VPC y subredes que cumplan con los requisitos de red de [AWS PCS](#).
- Un sistema de archivos Amazon EFS, que se utilizará como directorio principal compartido.
- Un sistema de archivos Amazon FSx for Lustre, que proporciona un directorio compartido de alto rendimiento.
- Un clúster AWS PCS, que proporciona un controlador Slurm.
- 2 grupos de nodos de cómputo AWS PCS.
  - El grupo de `login` nodos, que proporciona acceso interactivo al sistema basado en una consola.

- El grupo de compute-1 nodos proporciona instancias que se escalan elásticamente para ejecutar trabajos.
- 1 cola que envía los trabajos a las EC2 instancias del grupo de nodos. compute-1

El clúster requiere AWS recursos adicionales, como grupos de seguridad, funciones de IAM y plantillas de EC2 lanzamiento, que no se muestran en el diagrama.

#### Note

Le recomendamos que complete los pasos de la línea de comandos de este tema en un shell de Bash. Si no está utilizando un intérprete de comandos Bash, algunos comandos de script, como los caracteres de continuación de línea y la forma en que se establecen y utilizan las variables, requieren ajustes para su intérprete de comandos. Además, las reglas de entrecorillado y escape de su intérprete de comandos pueden ser diferentes. Para obtener más información, consulte [Comillas y literales con cadenas AWS CLI en la Guía del AWS Command Line Interface usuario de la versión 2](#).

## Temas

- [Requisitos previos para empezar a utilizar el PCS AWS](#)
- [Tutorial de uso AWS CloudFormation con el AWS PCS](#)
- [Crear una VPC y subredes para PCS AWS](#)
- [Crear grupos de seguridad para AWS PCS](#)
- [Crear un clúster en AWS PCS](#)
- [Cree almacenamiento compartido para AWS PCS en Amazon Elastic File System](#)
- [Cree almacenamiento compartido para AWS PCS en Amazon FSx for Lustre](#)
- [Cree grupos de nodos de cómputo en AWS PCS](#)
- [Cree una cola para administrar los trabajos en AWS PCS](#)
- [Conéctese a su clúster AWS PCS](#)
- [Explore el entorno de clústeres en AWS PCS](#)
- [Ejecute un trabajo de un solo nodo en AWS PCS](#)
- [Ejecute un trabajo de MPI de varios nodos con Slurm en PCS AWS](#)

- [Elimine sus AWS recursos para AWS PCS](#)

## Requisitos previos para empezar a utilizar el PCS AWS

Consulte los siguientes temas para preparar su entorno de desarrollo local Cuenta de AWS y el suyo para el AWS PCS.

### Temas

- [Inscríbese AWS y cree un usuario administrativo](#)
- [Instale el AWS CLI para AWS PCS](#)
- [Permisos de IAM necesarios para AWS PCS](#)

## Inscríbese AWS y cree un usuario administrativo

Complete las siguientes tareas para configurar el Servicio de computación AWS paralela (AWS PCS).

### Temas

- [Inscríbese en un Cuenta de AWS](#)
- [Creación de un usuario con acceso administrativo](#)

## Inscríbese en un Cuenta de AWS

Si no tiene una Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abrir <https://portal.aws.amazon.com/billing/registro>.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWS se crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar [tareas que requieren acceso de usuario raíz](#).

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a <https://aws.amazon.com/> y seleccionando Mi cuenta.

## Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

### Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión [AWS Management Console](#) como propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte [Iniciar sesión como usuario raíz](#) en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

Para obtener instrucciones, consulte [Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz \(consola\)](#) en la Guía del usuario de IAM.

### Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en [Activar AWS IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte [Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la](#) Guía del AWS IAM Identity Center usuario.

### Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario.

## Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte [Create a permission set](#) en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte [Add groups](#) en la Guía del usuario de AWS IAM Identity Center .

## Instale el AWS CLI para AWS PCS

Debe utilizar la última versión de AWS CLI. Para obtener más información, consulte [Instalar o actualizar a la última versión de AWS CLI en la](#) Guía del AWS Command Line Interface usuario de la versión 2.

Debe configurar el AWS CLI. Para obtener más información, consulte [Configurar el AWS CLI](#) en la Guía del AWS Command Line Interface usuario de la versión 2.

Introduzca el siguiente comando en una línea de comandos para comprobar su AWS CLI estado; debería mostrar información de ayuda.

```
aws pcs help
```

## Permisos de IAM necesarios para AWS PCS

El principal de seguridad de IAM que utilice debe tener permisos para trabajar con las funciones de IAM de AWS PCS, las funciones vinculadas a servicios AWS CloudFormation, una VPC y los recursos relacionados. Para obtener más información [Servicio de Gestión de Identidad y Acceso para Computación AWS Paralela](#), consulte [Crear un rol vinculado a un servicio](#) en la Guía del

usuario.AWS Identity and Access Management Debe completar todos los pasos de esta guía como el mismo usuario. Ejecute el siguiente comando para comprobar el usuario actual:

```
aws sts get-caller-identity
```

## Tutorial de uso AWS CloudFormation con el AWS PCS

El tutorial de AWS PCS consta de muchos pasos y su objetivo es ayudarle a comprender las partes de un clúster de AWS PCS y los procedimientos necesarios para crearlo. Le recomendamos que siga los pasos del tutorial al menos una vez. Una vez que comprenda bien lo que implica, puede utilizarlo AWS CloudFormation para crear el clúster de muestras rápidamente y de forma automática.

AWS CloudFormation es un AWS servicio que le permite crear y aprovisionar despliegues de AWS infraestructura de forma predecible y repetitiva. Puede usar una CloudFormation plantilla para aprovisionar automáticamente los AWS recursos del clúster de muestra como una sola unidad, denominada pila. Puede eliminar la pila cuando haya terminado con ella.

Para obtener más información, consulte [Comience con un AWS CloudFormationAWS PCS](#).

## Crear una VPC y subredes para PCS AWS

Puede crear una VPC y subredes con una plantilla. CloudFormation Utilice la siguiente URL para descargar la CloudFormation plantilla y, a continuación, cárguela en la [AWS CloudFormation consola](#) para crear una pila nueva CloudFormation. Para obtener más información, consulte [Uso de la AWS CloudFormation consola](#) en la Guía del AWS CloudFormation usuario.

```
https://aws-hpc-recipes.s3.amazonaws.com/main/recipes/net/hpc_large_scale/assets/main.yaml
```

Con la plantilla abierta en la AWS CloudFormation consola, introduzca las siguientes opciones. Puede utilizar los valores predeterminados proporcionados en la plantilla.

- En Proporcione un nombre de pila:
  - En Nombre de pila, ingresa:

```
hpc-networking
```

- En Parámetros:

- En VPC:
  - En CidrBlock, introduzca:  
`10.3.0.0/16`
- En las subredes A:
  - En CidrPublicSubnetA, introduzca:  
`10.3.0.0/20`
  - En CidrPrivateSubnetA, introduzca:  
`10.3.128.0/20`
- En las subredes B:
  - En CidrPublicSubnetB, introduzca:  
`10.3.16.0/20`
  - En CidrPrivateSubnetB, introduzca:  
`10.3.144.0/20`
- En Subredes C:
  - Para ProvisionSubnetsC, seleccione True
  - En CidrPublicSubnetC, introduzca:  
`10.3.32.0/20`
  - En CidrPrivateSubnetC, introduzca:  
`10.3.160.0/20`
- En Capacidades:
  - Marque la casilla Reconozco que AWS CloudFormation podría crear recursos de IAM.

Supervisa el estado de la CloudFormation pila. Cuando llegue `CREATE_COMPLETE`, busque el ID del grupo de seguridad predeterminado en la nueva VPC. Utilizará el ID más adelante en el tutorial.

## Busque el grupo de seguridad predeterminado para la VPC del clúster

Para buscar el ID del grupo de seguridad predeterminado en la nueva VPC, siga este procedimiento:

- Navegue hasta la [consola de Amazon VPC](#).
- En el panel de control de VPC, selecciona Filtrar por VPC.
  - Elija la VPC por la que empieza el nombre. hpc-networking
  - En Seguridad, selecciona Grupos de seguridad.
- Busque el ID del grupo de seguridad del grupo denominado default. Tiene la descripción default VPC security group. El ID se utiliza más adelante para configurar las plantillas de EC2 lanzamiento.

## Crear grupos de seguridad para AWS PCS

AWS PCS se basa en los grupos de seguridad para administrar el tráfico de red que entra y sale de un clúster y sus grupos de nodos de cómputo. Para obtener información detallada sobre este tema, consulte [Requisitos y consideraciones sobre los grupos de seguridad](#).

En este paso, utilizará una CloudFormation plantilla para crear dos grupos de seguridad.

- Un grupo de seguridad de clúster, que permite las comunicaciones entre el controlador AWS PCS, los nodos de cómputo y los nodos de inicio de sesión.
- Un grupo de seguridad SSH entrante, que puede añadir de forma opcional a sus nodos de inicio de sesión para admitir el acceso SSH

## Cree los grupos de seguridad para PCS AWS

Puede utilizar una CloudFormation plantilla para crear los grupos de seguridad. Utilice la siguiente URL para descargar la CloudFormation plantilla y, a continuación, cárguela en la [AWS CloudFormation consola](#) para crear una CloudFormation pila nueva. Para obtener más información, consulte [Uso de la AWS CloudFormation consola](#) en la Guía del AWS CloudFormation usuario.

```
https://aws-hpc-recipes.s3.amazonaws.com/main/recipes/pcs/getting_started/assets/pcs-cluster-sg.yaml
```

Con la plantilla abierta en la AWS CloudFormation consola, introduzca las siguientes opciones. Tenga en cuenta que algunas opciones se rellenarán automáticamente en la plantilla; simplemente puede dejarlas como valores predeterminados.

- En Indique un nombre para la pila
  - En Nombre de pila, ingresa:

```
getstarted-sg
```

- En Parámetros
  - En VpcId, elija la VPC por la que empieza el nombre. `hpc-networking`
  - (Opcional) En ClientIpCidr, introduzca un rango de IP más restrictivo para el grupo de seguridad SSH entrante. Le recomendamos que lo restrinja con su propia IP/subred (`x.x.x.x/32` para su propia IP o `x.x.x.x/24` para el rango). Sustituya `x.x.x.x` por su propia IP PÚBLICA. [Puede obtener su IP pública mediante herramientas como https://ifconfig.co/](https://ifconfig.co/)

Supervisa el estado de la CloudFormation pila. Cuando llegue al grupo `CREATE_COMPLETE` de seguridad, los recursos estarán listos.

Se han creado dos grupos de seguridad, con los nombres:

- `cluster-getstarted-sg`— este es el grupo de seguridad del clúster
- `inbound-ssh-getstarted-sg`— se trata de un grupo de seguridad que permite el acceso SSH entrante

## Crear un clúster en AWS PCS

En AWS PCS, un clúster es un recurso persistente para administrar recursos y ejecutar cargas de trabajo. Se crea un clúster para un programador específico (AWS PCS actualmente admite Slurm) en una subred de una VPC nueva o existente. El clúster acepta y programa los trabajos, y también lanza los nodos de cómputo (EC2 instancias) que procesan esos trabajos.

Cómo crear el clúster

1. Abra la [consola AWS PCS](#) y seleccione Crear clúster.
2. En la sección de detalles del clúster, introduzca los siguientes campos:

- Nombre del clúster: introduzca `get-started`
  - Planificador: seleccione la versión 24.11 de Slurm
  - Tamaño del controlador: seleccione Pequeño
3. En la sección Redes, seleccione valores para los siguientes campos:
    - VPC: elija la VPC denominada `hpc-networking:Large-Scale-HPC`
    - Subred: seleccione la subred donde comienza el nombre `hpc-networking:PrivateSubnetA`
    - Grupos de seguridad: seleccione el nombre del grupo de seguridad del clúster `cluster-getstarted-sg`
  4. Elija `Create cluster`.

 Note

El campo Estado muestra la opción `Crear` mientras se aprovisiona el clúster. La creación del clúster puede tardar varios minutos.

## Cree almacenamiento compartido para AWS PCS en Amazon Elastic File System

Amazon Elastic File System (Amazon EFS) es un AWS servicio que proporciona almacenamiento de archivos totalmente elástico y sin servidor para que pueda compartir datos de archivos sin aprovisionar ni administrar la capacidad de almacenamiento y el rendimiento. Para obtener más información, consulte [¿Qué es Amazon Elastic File System?](#) en la Guía del usuario de Amazon Elastic File System.

El clúster de demostración de AWS PCS utiliza un sistema de archivos EFS para proporcionar un directorio principal compartido entre los nodos del clúster. Cree un sistema de archivos EFS en la misma VPC que el clúster.

Cree su sistema de archivos de Amazon EFS

1. Vaya a la [consola de Amazon EFS](#).

2. Asegúrese de que está configurada de la misma manera en la Región de AWS que probará AWS PCS.
3. Seleccione Crear sistema de archivos.
4. En la página Crear sistema de archivos, defina los siguientes parámetros:
  - En Nombre, introduzca `getstarted-efs`.
  - En Virtual Private Cloud (VPC), elige la VPC denominada `hpc-networking:Large-Scale-HPC`
  - Seleccione Crear. De este modo, volverá a la página de sistemas de archivos.
5. Anote el ID del sistema de archivos del sistema de `getstarted-efs` archivos. Usará esta información más tarde.

## Cree almacenamiento compartido para AWS PCS en Amazon FSx for Lustre

Amazon FSx for Lustre hace que sea fácil y rentable lanzar y ejecutar el popular sistema de archivos Lustre de alto rendimiento. Utiliza Lustre para cargas de trabajo en las que la velocidad es importante, como el machine learning, la computación de alto rendimiento (HPC), el procesamiento de vídeo y el modelado financiero. Para obtener más información, consulta [¿Qué es Amazon FSx for Lustre?](#) en la Guía del usuario FSx de Amazon for Lustre.

El clúster de demostración de AWS PCS puede utilizar un sistema de archivos FSx for Lustre para proporcionar un directorio compartido de alto rendimiento entre los nodos del clúster. Cree un sistema de archivos FSx para Lustre en la misma VPC que su clúster.

Para crear su sistema de archivos FSx para Lustre

1. Ve a la [FSx consola de Amazon](#).
2. Asegúrese de que la consola esté configurada para usar lo Región de AWS mismo que su clúster.
3. Seleccione Crear sistema de archivos.
  - En Seleccione el tipo de sistema de archivos, elija Amazon FSx for Lustre y, a continuación, elija Siguiente.
4. En la página Especificar los detalles del sistema de archivos, defina los siguientes parámetros:

- En Detalles del sistema de archivos
    - En Nombre, introduzca `getstarted-fsx`.
    - Para el tipo de implementación y almacenamiento, selecciona Persistente, SSD
    - Para obtener un rendimiento por unidad de almacenamiento, elija 125 MB/s/TiB
    - Para Capacidad de almacenamiento, introduzca 1,2 TiB
    - Para la configuración de metadatos, elija Automática
    - Para el tipo de compresión de datos, elija LZ4
  - En Red y seguridad
    - Para Virtual Private Cloud (VPC), elija la VPC denominada `hpc-networking:Large-Scale-HPC`
    - Para los grupos de seguridad de VPC, deje el grupo de seguridad denominado `default`
    - En Subred, elige la subred en la que comience el nombre `hpc-networking:PrivateSubnetA`
    - Deje las demás opciones con sus valores predeterminados.
    - Elija Next (Siguiente).
5. En la página Revisar y crear, elija Crear sistema de archivos. De este modo, volverá a la página Sistemas de archivos.
  6. Navegue a la página de detalles del sistema de archivos FSx para Lustre que creó.
  7. Anote el ID del sistema de archivos y el nombre del montaje. Usará esta información más tarde.

#### Note

El campo Estado muestra la opción Crear mientras se aprovisiona el sistema de archivos. La creación del sistema de archivos puede tardar varios minutos. Espere a que se complete antes de continuar con el resto del tutorial.

## Cree grupos de nodos de cómputo en AWS PCS

Un grupo de nodos de cómputo es un conjunto virtual de nodos de cómputo (EC2 instancias) que AWS PCS lanza y administra. Al definir un grupo de nodos de procesamiento, se especifican características comunes, como los tipos de EC2 instancias, el número mínimo y máximo de instancias, las subredes de VPC de destino, la opción de compra preferida y la configuración

de lanzamiento personalizada. AWS PCS lanza, administra y termina de manera eficiente los nodos de cómputo de un grupo de nodos de cómputo, de acuerdo con estos ajustes. El clúster de demostración utiliza un grupo de nodos de cálculo para proporcionar nodos de inicio de sesión para el acceso de los usuarios y un grupo de nodos de cálculo independiente para procesar los trabajos. En los temas siguientes se describen los procedimientos para configurar estos grupos de nodos de procesamiento en el clúster.

## Temas

- [Crear un perfil de instancia para AWS PCS](#)
- [Cree plantillas de lanzamiento para AWS PCS](#)
- [Cree un grupo de nodos de cómputo para los nodos de inicio de sesión en AWS PCS](#)
- [Cree un grupo de nodos de cómputo para ejecutar trabajos de cómputo en AWS PCS](#)

## Crear un perfil de instancia para AWS PCS

Los grupos de nodos de cómputo requieren un perfil de instancia cuando se crean. Si utilizas el AWS Management Console para crear un rol para Amazon EC2, la consola crea automáticamente un perfil de instancia y le asigna el mismo nombre que el rol. Para obtener más información, consulte [Uso de perfiles de instancia](#) en la Guía del AWS Identity and Access Management usuario.

En el siguiente procedimiento, se utiliza AWS Management Console para crear un rol para Amazon EC2, que también crea el perfil de instancia para los grupos de nodos de cómputo.

Para crear el perfil de rol y de instancia

- Vaya a la [consola de IAM](#).
- En Access management (Administración de acceso), seleccione Políticas (Políticas).
  - Elija Create Policy.
  - En Especificar permisos, en el editor de políticas, selecciona JSON.
  - Sustituya el contenido del editor de texto por lo siguiente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "pcs:RegisterComputeNodeGroupInstance"
      ]
    }
  ]
}
```

```

        ],
        "Resource": "*",
        "Effect": "Allow"
    }
]
}

```

- Elija Next (Siguiente).
- En Revisar y crear, escriba el nombre de la política `AWSPCS-getstarted-policy`.
- Elija Crear política.
- En Access management (Administración de acceso), elija Roles (Roles).
- Elija Crear rol.
- En Seleccionar entidad de confianza:
  - En el tipo de entidad de confianza, seleccione AWS servicio
  - En Caso de uso, selecciona EC2.
    - A continuación, en Elegir un caso de uso para el servicio especificado, selecciona EC2.
  - Elija Next (Siguiente).
- En Añadir permisos:
  - En Políticas de permisos, busque `AWSPCS-getstarted-policy`.
  - Marque la casilla situada junto a `AWSPCS-getstarted-policy` para añadirla al rol.
  - En Políticas de permisos, busca Amazon `SSMManaged InstanceCore`.
  - Marque la casilla situada junto `SSMManaged InstanceCore` a Amazon para añadirlo al rol.
  - Elija Next (Siguiente).
- En Nombre, revisa y crea:
  - En Detalles del rol:
    - En Role name (Nombre del rol), introduzca `AWSPCS-getstarted-role`.
  - Elija Create role (Crear rol).

## Cree plantillas de lanzamiento para AWS PCS

Al crear un grupo de nodos de cómputo, se proporciona una plantilla de EC2 lanzamiento que AWS PCS utiliza para configurar EC2 las instancias que lanza. Esto incluye ajustes como los grupos de seguridad y los scripts que se ejecutan cuando se lanza la instancia.

En este paso, se utilizará una CloudFormation plantilla para crear dos plantillas de EC2 lanzamiento. Una plantilla se usará para crear nodos de inicio de sesión y la otra se usará para crear nodos de cómputo. La diferencia clave entre ellos es que los nodos de inicio de sesión se pueden configurar para permitir el acceso SSH entrante.

## Accede a la plantilla CloudFormation

Usa la siguiente URL para descargar la CloudFormation plantilla y, a continuación, cárgala en la [AWS CloudFormation consola](#) para crear una CloudFormation pila nueva. Para obtener más información, consulte [Uso de la AWS CloudFormation consola](#) en la Guía del AWS CloudFormation usuario.

```
https://aws-hpc-recipes.s3.amazonaws.com/main/recipes/pcs/getting_started/assets/pcs-1t-efs-fsx1.yaml
```

## Utilice la CloudFormation plantilla para crear plantillas de EC2 lanzamiento

Utilice el siguiente procedimiento para completar la CloudFormation plantilla en la AWS CloudFormation consola

- En Proporcione un nombre de pila:
  - En Nombre de pila, ingresagetstarted-1t.
- En Parámetros:
  - Bajo seguridad
    - Para VpcSecurityGroupId, seleccione el grupo de seguridad nombrado default en la VPC de su clúster.
    - Para ClusterSecurityGroupId, seleccione el grupo denominado cluster-getstarted-sg
    - Para SshSecurityGroupId, seleccione el grupo denominado inbound-ssh-getstarted-sg
    - Para SshKeyName, selecciona tu key pair de claves SSH preferido.
  - En Sistemas de archivos
    - Para EfsFileSystemId, introduzca el ID del sistema de archivos del sistema de archivos EFS que creó anteriormente en el tutorial.
    - Para FSxLustreFileSystemId, introduzca el ID del sistema de archivos del sistema FSx de archivos de Lustre que creó anteriormente en el tutorial.
    - Para FSxLustreFileSystemMountName, introduzca el nombre de montaje correspondiente al mismo sistema FSx de archivos Lustre.

- Seleccione Siguiente y, a continuación, vuelva a seleccionar Siguiente.
- Seleccione Submit (Enviar).

Supervisa el estado de la CloudFormation pila. Cuando llegue a CREATE\_COMPLETE la plantilla de lanzamiento estará lista para ser utilizada.

#### Note

Para ver todos los recursos que creó la CloudFormation plantilla, abre la [AWS CloudFormation consola](#). Elija la pila getstarted-1t y, a continuación, elija la pestaña Resources (Recursos).

## Cree un grupo de nodos de cómputo para los nodos de inicio de sesión en AWS PCS

Un grupo de nodos de cómputo es un conjunto virtual de nodos de cómputo (EC2 instancias) que AWS PCS lanza y administra. Al definir un grupo de nodos de procesamiento, se especifican características comunes, como los tipos de EC2 instancias, el número mínimo y máximo de instancias, las subredes de VPC de destino, la opción de compra preferida y la configuración de lanzamiento personalizada. AWS PCS lanza, administra y termina de manera eficiente los nodos de cómputo de un grupo de nodos de cómputo, de acuerdo con estos ajustes.

En este paso, lanzará un grupo de nodos de computación estáticos que proporciona acceso interactivo al clúster. Puede utilizar SSH o Amazon EC2 Systems Manager (SSM) para iniciar sesión en él y, a continuación, ejecutar comandos de shell y gestionar los trabajos de Slurm.

Para crear el grupo de nodos de cómputo

- Abra la [consola AWS PCS](#) y vaya a Clústeres.
- Seleccione el clúster denominado get-started
- Vaya a Compute nodes groups y elija Crear.
- En la sección de configuración del grupo de nodos de Compute, proporciona lo siguiente:
  - Nombre del grupo de nodos de cómputo: login introdúzcalo.
- En Configuración informática, introduzca o seleccione estos valores:

- EC2 plantilla de lanzamiento: elija la plantilla de lanzamiento donde está el nombre `login-getstarted-1t`
- Perfil de instancia de IAM: elija el nombre del perfil de instancia `AWSPCS-getstarted-role`
- Subredes: seleccione la subred por la que comienza el nombre. `hpc-networking:PublicSubnetA`
- Instancias: seleccione. `c6i.xlarge`
- Configuración de escalado: para el recuento mínimo de instancias, introduzca **1**. Para el recuento máximo de instancias, introduzca. `1`
- En Configuración adicional, especifique lo siguiente:
  - ID de AMI: seleccione la AMI que desee usar y que tenga un nombre con el siguiente formato:

```
aws-pcs-sample_ami-amzn2-platform-slurm-version
```

Para obtener más información sobre el ejemplo AMIs, consulte [Uso de Amazon Machine Images \(AMIs\) de muestra con AWS PCS](#).

- Seleccione Crear grupo de nodos de cómputo.

El campo Estado muestra la opción Crear mientras se aprovisiona el grupo de nodos de cómputo. Puede continuar con el siguiente paso del tutorial mientras está en curso.

## Cree un grupo de nodos de cómputo para ejecutar trabajos de cómputo en AWS PCS

En este paso, lanzará un grupo de nodos de cómputo que se escale de forma elástica para ejecutar los trabajos enviados al clúster.

Para crear el grupo de nodos de cómputo

- Abra la [consola AWS PCS](#) y vaya a Clústeres.
- Seleccione el clúster denominado `get-started`
- Vaya a Compute nodes groups y elija Crear.
- En la sección de configuración del grupo de nodos de Compute, proporcione lo siguiente:
  - Nombre del grupo de nodos de cómputo: `compute-1` introdúzcalo.
- En Configuración informática, introduzca o seleccione estos valores:

- EC2 plantilla de lanzamiento: elija la plantilla de lanzamiento donde está el nombre `compute-getstarted-1t`
- Perfil de instancia de IAM: elija el nombre del perfil de instancia `AWSPCS-getstarted-role`
- Subredes: seleccione la subred por la que comienza el nombre. `hpc-networking:PrivateSubnetA`
- Instancias: seleccione. `c6i.xlarge`
- Configuración de escalado: introduzca `0` el número mínimo de instancias. Para el recuento máximo de instancias, introduzca. `4`
- En Configuración adicional, especifique lo siguiente:
  - ID de AMI: seleccione la AMI que desee usar y que tenga un nombre con el siguiente formato:

```
aws-pcs-sample_ami-amzn2-platform-slurm-version
```

Para obtener más información sobre el ejemplo AMIs, consulte [Uso de Amazon Machine Images \(AMIs\) de muestra con AWS PCS](#).

- Seleccione Crear grupo de nodos de cómputo.

El campo Estado muestra la opción Crear mientras se aprovisiona el grupo de nodos de cómputo.

#### Important

Espere a que el campo Estado muestre Activo antes de continuar con el siguiente paso de este tutorial.

## Cree una cola para administrar los trabajos en AWS PCS

Debe enviar un trabajo a una cola para ejecutarlo. El trabajo permanece en la cola hasta que AWS PCS lo programe para que se ejecute en un grupo de nodos de cómputo. Cada cola está asociada a uno o más grupos de nodos de cómputo, que proporcionan las EC2 instancias necesarias para realizar el procesamiento.

En este paso, creará una cola que utilice el grupo de nodos de procesamiento para procesar los trabajos.

Para crear una cola

- Abra la [consola AWS PCS](#).
- Seleccione el clúster denominado `get-started`.
- Vaya a Compute node groups y asegúrese de que el estado del `compute-1` grupo sea Activo.

 Important

El estado del `compute-1` grupo debe ser Activo antes de continuar con el siguiente paso.

- Navegue hasta Colas y elija Crear cola.
  - En la sección de configuración de colas, proporciona los siguientes valores:
    - Nombre de la cola: introduzca lo siguiente: `demo`
    - Grupos de nodos de cómputo: seleccione el nombre `compute-1` del grupo de nodos de cómputo.
- Elige Crear cola.

El campo Estado muestra la opción Crear mientras se crea la cola.

 Important

Espere a que el campo Estado muestre Activo antes de continuar con el siguiente paso de este tutorial.

## Conéctese a su clúster AWS PCS

Cuando el estado del grupo de nodos de `login` cómputo pase a ser Activo, podrás conectarte a la EC2 instancia que creó.

Para conectarse al nodo de inicio de sesión

- Abra la [consola AWS PCS](#) y vaya a Clusters.
- Seleccione el clúster denominado `get-started`.
- Elija grupos de nodos de cómputo.
- Navegue hasta el grupo de nodos de cómputo denominado `login`.

- Busque el ID del grupo de nodos de cómputo.
- En otra ventana o pestaña del navegador, abra la [EC2 consola de Amazon](#).
  - Elija Instances.
  - Busca EC2 instancias con la siguiente etiqueta. *node-group-id* Sustitúyalo por el valor del ID del grupo de nodos de Compute del paso anterior. Debe haber 1 instancia.

```
aws:pcs:compute-node-group-id=node-group-id
```

- Conéctese a la EC2 instancia. Puedes usar el administrador de sesiones o SSH.

#### Session Manager

- Seleccione la instancia.
- Elija Conectar.
- En Conectar a la instancia, selecciona Administrador de sesiones.
- Elija Conectar.
- Elija Conectar. Se abrirá un terminal interactivo en el navegador.

#### SSH

- Seleccione la instancia.
- Elija Conectar.
- En Conectar a la instancia, selecciona Cliente SSH.
- Sigue las instrucciones que te proporciona la consola.

#### Note

El nombre de usuario de la instancia **ec2-user** no lo es **root**.

## Explore el entorno de clústeres en AWS PCS

Una vez que haya iniciado sesión en el clúster, podrá ejecutar comandos de shell. Por ejemplo, puede cambiar de usuario, trabajar con datos en sistemas de archivos compartidos e interactuar con Slurm.

## Cambiar de usuario

Si ha iniciado sesión en el clúster mediante el Administrador de sesiones, es posible que esté conectado como `ssm-user`. Se trata de un usuario especial que se creó para el Administrador de sesiones. Cambie al usuario predeterminado en Amazon Linux 2 mediante el siguiente comando. No necesitará hacer esto si se conectó mediante SSH.

```
sudo su - ec2-user
```

## Trabaje con sistemas de archivos compartidos

Puede confirmar que el sistema de archivos EFS y los sistemas FSx de archivos Lustre están disponibles con el comando `df -h`. El resultado del clúster debe ser similar al siguiente:

```
[ec2-user@ip-10-3-6-103 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   0  3.8G   0% /dev
tmpfs           3.9G   0  3.9G   0% /dev/shm
tmpfs           3.9G 556K  3.9G   1% /run
tmpfs           3.9G   0  3.9G   0% /sys/fs/cgroup
/dev/nvme0n1p1  24G   18G  6.6G  73% /
127.0.0.1:/     8.0E   0  8.0E   0% /home
10.3.132.79@tcp:/z1shxbev 1.2T 7.5M 1.2T   1% /shared
tmpfs           780M   0  780M   0% /run/user/0
tmpfs           780M   0  780M   0% /run/user/1000
```

El `/home` sistema de archivos monta `127.0.0.1` y tiene una capacidad muy grande. Este es el sistema de archivos EFS que creó anteriormente en el tutorial. Todos los archivos que se escriban aquí estarán disponibles `/home` en todos los nodos del clúster.

El `/shared` sistema de archivos monta una IP privada y tiene una capacidad de 1,2 TB. Este es el sistema de archivos FSx para Lustre que creó anteriormente en el tutorial. Todos los archivos que se escriban aquí estarán disponibles `/shared` en todos los nodos del clúster.

## Interactúa con Slurm

### Temas

- [Enumere las colas y los nodos](#)

- [Mostrar trabajos](#)

## Enumere las colas y los nodos

Puede enumerar las colas y los nodos a los que están asociadas. `sinfo` El resultado del clúster debe ser similar al siguiente:

```
[ec2-user@ip-10-3-6-103 ~]$ sinfo
PARTITION AVAIL  TIMELIMIT  NODES  STATE NODELIST
demo          up    infinite     4  idle~ compute-1-[1-4]
[ec2-user@ip-10-3-6-103 ~]$
```

Anote el nombre de la particióndemo. Su estado es up y tiene un máximo de 4 nodos. Está asociado a los nodos del grupo de compute-1 nodos. Si edita el grupo de nodos de cómputo y aumenta el número máximo de instancias a 8, el número de nodos se leerá 8 y la lista de nodos se leerácompute-1-[1-8]. Si creara un segundo grupo de nodos de cómputo test con un nombre de 4 nodos y lo añadiera a la demo cola, esos nodos también aparecerían en la lista de nodos.

## Mostrar trabajos

Puede enumerar todos los trabajos, en cualquier estado, del sistema consqueue. El resultado del clúster debe ser similar al siguiente:

```
[ec2-user@ip-10-3-6-103 ~]$ squeue
JOBID PARTITION NAME USER ST TIME NODES NODELIST(REASON)
```

Intente squeue volver a ejecutarlo más tarde, cuando tenga un trabajo de Slurm pendiente o en ejecución.

## Ejecute un trabajo de un solo nodo en AWS PCS

Para ejecutar un trabajo con Slurm, debe preparar un script de envío que especifique los requisitos del trabajo y enviarlo a una cola con el comando. `sbatch` Por lo general, esto se hace desde un directorio compartido, de modo que los nodos de inicio de sesión y de procesamiento tengan un espacio común para acceder a los archivos.

Conéctese al nodo de inicio de sesión de su clúster y ejecute los siguientes comandos en su intérprete de comandos.

- Conviértete en el usuario predeterminado. Cambie al directorio compartido.

```
sudo su - ec2-user
cd /shared
```

- Utilice los siguientes comandos para crear un ejemplo de script de trabajo:

```
cat << EOF > job.sh
#!/bin/bash
#SBATCH -J single
#SBATCH -o single.%j.out
#SBATCH -e single.%j.err

echo "This is job \${SLURM_JOB_NAME} [\${SLURM_JOB_ID}] running on \
\${SLURMD_NODENAME}, submitted from \${SLURM_SUBMIT_HOST}" && sleep 60 && echo "Job
complete"
EOF
```

- Envíe el script de trabajo al programador de Slurm:

```
sbatch -p demo job.sh
```

- Cuando se envíe el trabajo, devolverá una ID de trabajo en forma de número. Usa ese identificador para comprobar el estado del trabajo. Sustituya *job-id* el siguiente comando por el número devuelto desde `sbatch`.

```
squeue --job job-id
```

## Example

```
squeue --job 1
```

El `squeue` comando devuelve un resultado similar al siguiente:

```
JOBID PARTITION NAME USER      ST TIME NODES NODELIST(REASON)
1      demo      test ec2-user CF 0:47 1      compute-1
```

- Continúe comprobando el estado del trabajo hasta que alcance el estado R (en ejecución). El trabajo está hecho cuando `squeue` no devuelve nada.
- Inspeccione el contenido del `/shared` directorio.

```
ls -alth /shared
```

El resultado del comando es similar al siguiente:

```
-rw-rw-r- 1 ec2-user ec2-user 107 Mar 19 18:33 single.1.out
-rw-rw-r- 1 ec2-user ec2-user 0 Mar 19 18:32 single.1.err
-rw-rw-r- 1 ec2-user ec2-user 381 Mar 19 18:29 job.sh
```

Uno de los nodos de cómputo del clúster `single.1.err` asignó un nombre `single.1.out` a los archivos y los escribió. Como el trabajo se ejecutó en un directorio compartido (`/shared`), también están disponibles en su nodo de inicio de sesión. Por eso configuró un sistema de archivos FSx para Lustre para este clúster.

- Inspeccione el contenido del `single.1.out` archivo.

```
cat /shared/single.1.out
```

El resultado es similar al siguiente:

```
This is job test [1] running on compute-1, submitted from ip-10-3-13-181
Job complete
```

## Ejecute un trabajo de MPI de varios nodos con Slurm en PCS AWS

Estas instrucciones muestran el uso de Slurm para ejecutar un trabajo de interfaz de paso de mensajes (MPI) en PCS. AWS

Ejecute los siguientes comandos en el intérprete de comandos de su nodo de inicio de sesión.

- Conviértete en el usuario predeterminado. Cambie a su directorio principal.

```
sudo su - ec2-user
cd ~/
```

- Cree el código fuente en el lenguaje de programación C.

```
cat > hello.c << EOF
// * mpi-hello-world - https://www.mpitutorial.com
```

```
// Released under MIT License
//
// Copyright (c) 2014 MPI Tutorial.
//
// Permission is hereby granted, free of charge, to any person obtaining a copy
// of this software and associated documentation files (the "Software"), to
// deal in the Software without restriction, including without limitation the
// rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
// sell copies of the Software, and to permit persons to whom the Software is
// furnished to do so, subject to the following conditions:
// The above copyright notice and this permission notice shall be included in
// all copies or substantial portions of the Software.
//
// THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
// IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
// FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
// AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
// LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
// FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
// DEALINGS IN THE SOFTWARE.

#include <mpi.h>
#include <stdio.h>
#include <stddef.h>

int main(int argc, char** argv) {
    // Initialize the MPI environment. The two arguments to MPI Init are not
    // currently used by MPI implementations, but are there in case future
    // implementations might need the arguments.
    MPI_Init(NULL, NULL);

    // Get the number of processes
    int world_size;
    MPI_Comm_size(MPI_COMM_WORLD, &world_size);

    // Get the rank of the process
    int world_rank;
    MPI_Comm_rank(MPI_COMM_WORLD, &world_rank);

    // Get the name of the processor
    char processor_name[MPI_MAX_PROCESSOR_NAME];
    int name_len;
    MPI_Get_processor_name(processor_name, &name_len);
```

```
// Print off a hello world message
printf("Hello world from processor %s, rank %d out of %d processors\n",
      processor_name, world_rank, world_size);

// Finalize the MPI environment. No more MPI calls can be made after this
MPI_Finalize();
}
EOF
```

- Cargue el módulo OpenMPI.

```
module load openmpi
```

- Compila el programa C.

```
mpicc -o hello hello.c
```

- Escribe un guion de envío de trabajos de Slurm.

```
cat > hello.sh << EOF
#!/bin/bash
#SBATCH -J multi
#SBATCH -o multi.out
#SBATCH -e multi.err
#SBATCH --exclusive
#SBATCH --nodes=4
#SBATCH --ntasks-per-node=1

srun $HOME/hello
EOF
```

- Cambie al directorio compartido.

```
cd /shared
```

- Envíe el script de trabajo.

```
sbatch -p demo ~/hello.sh
```

- squeue Úselo para supervisar el trabajo hasta que esté terminado.
- Compruebe el contenido de `multi.out`:

```
cat multi.out
```

El resultado es similar al siguiente. Tenga en cuenta que cada rango tiene su propia dirección IP porque se ejecutó en un nodo diferente.

```
Hello world from processor ip-10-3-133-204, rank 0 out of 4 processors  
Hello world from processor ip-10-3-128-219, rank 2 out of 4 processors  
Hello world from processor ip-10-3-141-26, rank 3 out of 4 processors  
Hello world from processor ip-10-3-143-52, rank 1 out of 4 processor
```

## Elimine sus AWS recursos para AWS PCS

Una vez que haya terminado con los grupos de clústeres y nodos que creó para este tutorial, debe eliminar los recursos que creó.

### Important

Recibirás cargos de facturación por todos los recursos que estén en funcionamiento en tu Cuenta de AWS

Para eliminar los recursos de AWS PCS que creó para este tutorial

- Abra la [consola AWS PCS](#).
- Navegue hasta el clúster denominado get-started.
- Navegue hasta la sección Colas.
- Seleccione la cola llamada demo.
- Elija Eliminar.

### Important

Espere a que se elimine la cola antes de continuar.

- Navegue hasta la sección Grupos de nodos de cómputo.
- Seleccione el grupo de nodos de cómputo denominado compute-1.

- Elija Eliminar.
- Seleccione el grupo de nodos de cómputo denominado login.
- Elija Eliminar.

 Important

Espere a que se eliminen ambos grupos de nodos de procesamiento antes de continuar.

- En la página de detalles del clúster para empezar, selecciona Eliminar.

 Important

Espere a que se elimine el clúster antes de continuar con los pasos siguientes.

Para eliminar otros AWS recursos que haya creado para este tutorial

- Abra la [consola de IAM](#).
  - Elija Roles.
  - Seleccione el rol denominado AWSPCS-getstarted-role y, a continuación, elija Eliminar.
  - Una vez que se haya eliminado el rol, elija Políticas.
  - Seleccione la política denominada AWSPCS-getstarted-policy y, a continuación, elija Eliminar.
- Abra la [consola de AWS CloudFormation](#).
  - Seleccione la pila denominada getstarted-It.
  - Elija Eliminar.

 Important

Espere a que se elimine la pila antes de continuar.

- Abra la [consola de Amazon EFS](#).
  - Elija Sistemas de archivos.
  - Seleccione el sistema de archivos denominado getstarted-efs.
  - Elija Eliminar.

 Important

Espere a que el sistema de archivos elimine antes de continuar.

- Abra la [FSx consola de Amazon](#).
- Elija Sistemas de archivos.
- Seleccione el sistema de archivos llamado getstarted-fsx.
- Elija Eliminar.

 Important

Espere a que el sistema de archivos elimine antes de continuar.

- Abra la [consola de AWS CloudFormation](#).
- Seleccione la pila denominada getstarted-sg.
- Elija Eliminar.
- Abra la [consola de AWS CloudFormation](#).
- Seleccione la pila denominada hpc-networking.
- Elija Eliminar.

# Comience con un AWS CloudFormationAWS PCS

Se puede utilizar AWS CloudFormation para crear un clúster de AWS PCS. AWS CloudFormation le permite crear y aprovisionar despliegues de AWS infraestructura de forma predecible y repetitiva. Puede utilizarlos AWS CloudFormation para aprovisionar automáticamente los recursos de muchos AWS servicios para crear aplicaciones altamente confiables, escalables y rentables Nube de AWS sin necesidad de crear ni configurar la infraestructura subyacente AWS . AWS CloudFormation le permite utilizar un archivo de plantilla para crear y eliminar un conjunto de recursos juntos como una sola unidad, denominada pila. Para obtener más información al respecto AWS CloudFormation, consulte [¿Qué es AWS CloudFormation?](#) en la Guía AWS CloudFormation del usuario. Para obtener más información sobre los tipos de recursos de AWS PCS AWS CloudFormation, consulte la [referencia de tipos de recursos de AWS PCS](#) en la Guía del AWS CloudFormation usuario.

## Temas

- [Se utiliza AWS CloudFormation para crear un clúster de AWS PCS de muestra](#)
- [Conéctese a un clúster AWS PCS creado con AWS CloudFormation](#)
- [Limpiar un clúster de AWS PCS en AWS CloudFormation](#)
- [Partes de una CloudFormation plantilla para AWS PCS](#)
- [AWS CloudFormation plantillas para crear un clúster de AWS PCS de muestra](#)

## Se utiliza AWS CloudFormation para crear un clúster de AWS PCS de muestra

El siguiente procedimiento utiliza una CloudFormation plantilla en el AWS Management Console para crear un clúster de AWS PCS de muestra. Para obtener más información al respecto AWS CloudFormation, consulte [¿Qué es AWS CloudFormation?](#) en la Guía AWS CloudFormation del usuario. Para obtener más información sobre los tipos de recursos de AWS PCS AWS CloudFormation, consulte la [referencia de tipos de recursos de AWS PCS](#) en la Guía del AWS CloudFormation usuario.

Para crear el clúster de muestra

1. Elija la opción en la Región de AWS que desea crear el clúster (el enlace abre la CloudFormation consola con la plantilla):

- [EE.UU. Este \(Virginia\) \(us-east-1\)](#)
  - [EE.UU. Este \(Ohio\) \(us-east-2\)](#)
  - [EE.UU. Oeste \(Oregón\) \(us-west-2\)](#)
  - [Asia Pacífico \(Singapur\) \(ap-southeast-1\)](#)
  - [Asia Pacífico \(Sídney\) \(ap-southeast-2\)](#)
  - [Asia Pacífico \(Tokio\) \(ap-northeast-1\)](#)
  - [Europa \(Fráncfort\) \(eu-central-1\)](#)
  - [Europa \(Irlanda\) \(eu-west-1\)](#)
  - [Europa \(Estocolmo\) \(eu-north-1\)](#)
2. En Indique un nombre de pila, introduzca un nombre descriptivo. Este es el nombre de la CloudFormation pila. La plantilla usa este valor como nombre para el clúster de AWS PCS.
  3. En Parámetros:
    - a. En SlurmVersion, elige la versión de Slurm que quieres que use tu clúster.
    - b. En NodeArchitecture, elija x86 para implementar un clúster que use instancias compatibles con x86\_64, o elija Graviton para usar instancias Arm64.
    - c. Para KeyName, elija un key pair de claves SSH para acceder a los nodos de inicio de sesión del clúster. Asegúrese de tener el archivo PEM para el key pair que elija.
    - d. Para ello ClientIpCidr, introduzca un rango de IP en formato CIDR para controlar el acceso a los nodos de inicio de sesión.
-  **Warning**

El valor predeterminado de 0.0.0.0/0 permite el acceso desde todas las direcciones IP.
- e. Deje los valores de HpcRecipesS3Bucket y HpcRecipesBranchsus valores predeterminados.
4. En Capacidades y transformaciones:
  - a. Seleccione la casilla de verificación para confirmar que AWS CloudFormation se crearán recursos de IAM.
  - b. Seleccione la casilla de verificación para confirmar que AWS CloudFormation se crearán recursos de IAM con nombres personalizados.

- c. Seleccione la casilla de verificación CAPABILITY\_AUTO\_EXPAND para confirmar la nueva pila. Para obtener más información, consulta [CreateStack](#) en la AWS CloudFormation Referencia de la API de .
5. Seleccione Creación de pila.
6. Supervisa el estado de tu pila. Puede conectarse al clúster una vez que se encuentre el estado de la pila CREATE\_COMPLETE.

## Conéctese a un clúster AWS PCS creado con AWS CloudFormation

Tras crear un clúster de AWS PCS a partir de una AWS CloudFormation plantilla, puede utilizar la consola de AWS PCS (en la AWS Management Console) para administrar el clúster. También puede conectarse a uno de los nodos de inicio de sesión del clúster para administrar el clúster, ejecutar trabajos y gestionar los datos. La AWS CloudFormation pila proporciona enlaces que puede utilizar para conectarse al clúster.

Para conectarse a su clúster

1. Abra la [consola de AWS CloudFormation](#).
2. Elige la pila que has creado.
3. Seleccione la pestaña Salidas de la pila.

La pila proporciona los siguientes enlaces:

- PcsConsoleUrl— Elija este enlace para abrir la consola AWS PCS con el clúster seleccionado. Puede usarlo para explorar las configuraciones del clúster, el grupo de nodos y las colas.
- Ec2 ConsoleUrl: elija este enlace para abrir la EC2 consola de Amazon, filtrada para mostrar las instancias que administra el grupo de nodos de inicio de sesión del clúster.

Desde esta vista, puede seleccionar una instancia y elegir Connect. La instancia del clúster de muestra admite el SSH entrante y AWS Systems Manager las conexiones en un navegador web. Para obtener más información, consulte [Conéctese a su clúster AWS PCS](#).

Después de conectarte a una instancia de inicio de sesión, puedes seguir el tutorial que se encuentra en. [Explore el entorno de clústeres en AWS PCS](#)

# Limpiar un clúster de AWS PCS en AWS CloudFormation

Si AWS CloudFormation solía crear su clúster de AWS PCS, puede abrir la [AWS CloudFormation consola](#) y eliminar la pila para eliminar el clúster y todos sus recursos asociados.

## Important

En el caso del clúster de muestra, si ha creado colas o grupos de nodos de procesamiento adicionales en el clúster (además de `compute-1` los grupos `login` y que creó la CloudFormation plantilla de ejemplo), debe utilizar la [consola AWS PCS](#) o AWS CLI eliminar esos recursos antes de eliminar la CloudFormation pila. Para obtener más información, consulte [Eliminar un clúster en AWS PCS](#).

## Partes de una CloudFormation plantilla para AWS PCS

Una CloudFormation plantilla tiene una o más secciones, cada una de las cuales tiene un propósito específico. AWS CloudFormation define el formato, la sintaxis y el idioma estándar de una plantilla. Para obtener más información, consulte [Trabajar con CloudFormation plantillas](#) en la Guía del AWS CloudFormation usuario.

CloudFormation las plantillas son altamente personalizables y, por lo tanto, sus formatos pueden variar. Para comprender las partes necesarias de una CloudFormation plantilla para crear un clúster de AWS PCS, le recomendamos que examine la plantilla de ejemplo que le proporcionamos para crear un clúster de muestra. En este tema se explican brevemente las secciones de esa plantilla de ejemplo.

## Important

Los ejemplos de código de este tema no están completos. La presencia de puntos suspensivos (`[ . . . ]`) indica que hay código adicional que no se muestra. Para descargar la plantilla completa con formato YAML CloudFormation, consulte [AWS CloudFormation plantillas para crear un clúster de AWS PCS de muestra](#)

## Contenido

- [Encabezado](#)

- [Metadatos](#)
- [Parámetros](#)
- [Mapeos](#)
- [Recursos](#)
- [Salidas](#)

## Encabezado

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: AWS Parallel Computing Service "getting started" cluster
```

`AWSTemplateFormatVersion` identifica la versión del formato de plantilla a la que se ajusta la plantilla. Para obtener más información, consulte la [sintaxis de la versión del formato de CloudFormation plantilla](#) en la Guía del AWS CloudFormation usuario.

`Transform` especifica una macro que se CloudFormation utiliza para procesar la plantilla. Para obtener más información, consulte la [sección Transformación de CloudFormation plantillas](#) en la Guía del AWS CloudFormation usuario. La `AWS::Serverless-2016-10-31` transformación permite AWS CloudFormation procesar una plantilla escrita en la sintaxis AWS Serverless Application Model (AWS SAM). Para obtener más información, consulte la [AWS::Serverless transformación](#) en la Guía AWS CloudFormation del usuario.

## Metadatos

```
### Stack metadata
Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: PCS Cluster configuration
        Parameters:
          - SlurmVersion
      - Label:
          default: PCS ComputeNodeGroups configuration
        Parameters:
          - NodeArchitecture
```

```

    - KeyName
    - ClientIpCidr
- Label:
  default: HPC Recipes configuration
Parameters:
  - HpcRecipesS3Bucket
  - HpcRecipesBranch

```

La metadata sección de una CloudFormation plantilla proporciona información sobre la propia plantilla. La plantilla de ejemplo crea un clúster de computación de alto rendimiento (HPC) completo que utiliza AWS PCS. La sección de metadatos de la plantilla de ejemplo declara los parámetros que controlan la forma en que AWS CloudFormation se lanza (aprovisiona) la pila correspondiente. Hay parámetros que controlan la elección de la arquitectura (NodeArchitecture), la versión de Slurm (SlurmVersion) y los controles de acceso (KeyNameClientIpCidr).

## Parámetros

La Parameters sección define los parámetros personalizados de la plantilla. AWS CloudFormation utiliza estas definiciones de parámetros para construir y validar el formulario con el que se interactúa al lanzar una pila desde esta plantilla.

Parameters:

NodeArchitecture:

Type: String

Default: x86

AllowedValues:

- x86
- Graviton

Description: Architecture of the login and compute node instances

SlurmVersion:

Type: String

Default: 23.11

Description: Version of Slurm to use

AllowedValues:

- 23.11
- 24.05

KeyName:

Description: KeyPair to login to the head node

Type: AWS::EC2::KeyPair::KeyName

AllowedPattern: ".+" # Required

#### ClientIpCidr:

Description: IP(s) allowed to directly access the login nodes. We recommend that you restrict it with your own IP/subnet (x.x.x.x/32 for your own ip or x.x.x.x/24 for range. Replace x.x.x.x with your own PUBLIC IP. You can get your public IP using tools such as <https://ifconfig.co/>)

Default: 127.0.0.1/32

Type: String

AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})/(\d{1,2})

ConstraintDescription: Value must be a valid IP or network range of the form x.x.x.x/x.

#### HpcRecipesS3Bucket:

Type: String

Default: aws-hpc-recipes

Description: HPC Recipes for AWS S3 bucket

AllowedValues:

- aws-hpc-recipes
- aws-hpc-recipes-dev

#### HpcRecipesBranch:

Type: String

Default: main

Description: HPC Recipes for AWS release branch

AllowedPattern: '^(?!.\*\/\.git\$)(?!.\*\/\.)(?!.\*\\.\.)[a-zA-Z0-9-\_\.\.]+\$'

## Mapeos

La Mappings sección define pares clave-valor que especifican valores en función de determinadas condiciones o dependencias.

#### Mappings:

##### Architecture:

AmiArchParameter:

Graviton: arm64

x86: x86\_64

LoginNodeInstances:

Graviton: c7g.xlarge

x86: c6i.xlarge

ComputeNodeInstances:

Graviton: c7g.xlarge

```
x86: c6i.xlarge
```

## Recursos

La Resources sección declara los AWS recursos que se van a aprovisionar y configurar como parte de la pila.

```
Resources:
```

```
[...]
```

La plantilla aprovisiona la infraestructura de clústeres de muestra en capas. Comienza con la Networking configuración de VPC. El almacenamiento lo proporcionan dos sistemas: EfsStorage para almacenamiento compartido y FSxLStorage almacenamiento de alto rendimiento. El clúster principal se establece mediantePCSCluster.

```
Networking:
  Type: AWS::CloudFormation::Stack
  Properties:
    Parameters:
      ProvisionSubnetsC: "False"
      TemplateURL: !Sub 'https://${HpcRecipesS3Bucket}.s3.amazonaws.com/
${HpcRecipesBranch}/recipes/net/hpc_large_scale/assets/main.yaml'

EfsStorage:
  Type: AWS::CloudFormation::Stack
  Properties:
    Parameters:
      SubnetIds: !GetAtt [ Networking, Outputs.DefaultPrivateSubnet ]
      SubnetCount: 1
      VpcId: !GetAtt [ Networking, Outputs.VPC ]
      TemplateURL: !Sub 'https://${HpcRecipesS3Bucket}.s3.amazonaws.com/
${HpcRecipesBranch}/recipes/storage/efs_simple/assets/main.yaml'

FSxLStorage:
  Type: AWS::CloudFormation::Stack
  Properties:
    Parameters:
      PerUnitStorageThroughput: 125
      SubnetId: !GetAtt [ Networking, Outputs.DefaultPrivateSubnet ]
```

```

    VpcId: !GetAtt [ Networking, Outputs.VPC ]
    TemplateURL: !Sub 'https://${HpcRecipesS3Bucket}.s3.amazonaws.com/
${HpcRecipesBranch}/recipes/storage/fsx_lustre/assets/persistent.yaml'

[...]

# Cluster
PCSCluster:
  Type: AWS::PCS::Cluster
  Properties:
    Name: !Sub '${AWS::StackName}'
    Size: SMALL
    Scheduler:
      Type: SLURM
      Version: !Ref SlurmVersion
    Networking:
      SubnetIds:
        - !GetAtt [ Networking, Outputs.DefaultPrivateSubnet ]
      SecurityGroupIds:
        - !GetAtt [ PCSSecurityGroup, Outputs.ClusterSecurityGroupId ]

```

En el caso de los recursos informáticos, la plantilla crea dos grupos de nodos: PCSNodeGroupLogin para un único nodo de inicio de sesión y PCSNodeGroupCompute para un máximo de cuatro nodos informáticos. Estos grupos de nodos son compatibles con los permisos y, PCSInstanceProfile por PCSLaunchTemplate ejemplo, con las configuraciones.

```

# Compute Node groups
PCSInstanceProfile:
  Type: AWS::CloudFormation::Stack
  Properties:
    Parameters:
      # We have to regionalize this in case CX use the template in more than one
region. Otherwise,
      # the create action will fail since instance-role-${AWS::StackName} already
exists!
      RoleName: !Sub '${AWS::StackName}-${AWS::Region}'
      TemplateURL: !Sub 'https://${HpcRecipesS3Bucket}.s3.amazonaws.com/
${HpcRecipesBranch}/recipes/pcs/getting_started/assets/pcs-iip-minimal.yaml'

PCSLaunchTemplate:
  Type: AWS::CloudFormation::Stack
  Properties:

```

```

Parameters:
  VpcDefaultSecurityGroupId: !GetAtt [ Networking, Outputs.SecurityGroup ]
  ClusterSecurityGroupId: !GetAtt [ PCSSecurityGroup,
Outputs.ClusterSecurityGroupId ]
  SshSecurityGroupId: !GetAtt [ PCSSecurityGroup,
Outputs.InboundSshSecurityGroupId ]
  EfsFileSystemSecurityGroupId: !GetAtt [ EfsStorage, Outputs.SecurityGroupId ]
  FSxLustreFileSystemSecurityGroupId: !GetAtt [ FSxLStorage,
Outputs.FSxLustreSecurityGroupId ]
  SshKeyName: !Ref KeyName
  EfsFileSystemId: !GetAtt [ EfsStorage, Outputs.EFSFileSystemId ]
  FSxLustreFileSystemId: !GetAtt [ FSxLStorage, Outputs.FSxLustreFileSystemId ]
  FSxLustreFileSystemMountName: !GetAtt [ FSxLStorage,
Outputs.FSxLustreMountName ]
  TemplateURL: !Sub 'https://${HpcRecipesS3Bucket}.s3.amazonaws.com/
${HpcRecipesBranch}/recipes/pcs/getting_started/assets/cfn-pcs-lt-efs-fsx1.yaml'

# Compute Node groups - Login Nodes
PCSNODEGROUPLOGIN:
  Type: AWS::PCS::ComputeNodeGroup
  Properties:
    ClusterId: !GetAtt [PCSCluster, Id]
    Name: login
    ScalingConfiguration:
      MinInstanceCount: 1
      MaxInstanceCount: 1
    IamInstanceProfileArn: !GetAtt [ PCSInstanceProfile, Outputs.InstanceProfileArn ]
    CustomLaunchTemplate:
      TemplateId: !GetAtt [ PCSLaunchTemplate, Outputs.LoginLaunchTemplateId ]
      Version: 1
    SubnetIds:
      - !GetAtt [ Networking, Outputs.DefaultPublicSubnet ]
    AmiId: !GetAtt [ PcsSampleAmi, AmiId]
    InstanceConfigs:
      - InstanceType: !FindInMap [ Architecture, LoginNodeInstances, !Ref
NodeArchitecture ]

# Compute Node groups - Compute Nodes
PCSNODEGROUPCOMPUTE:
  Type: AWS::PCS::ComputeNodeGroup
  Properties:
    ClusterId: !GetAtt [PCSCluster, Id]
    Name: compute-1
    ScalingConfiguration:

```

```

    MinInstanceCount: 0
    MaxInstanceCount: 4
    IamInstanceProfileArn: !GetAtt [ PCSInstanceProfile, Outputs.InstanceProfileArn ]
    CustomLaunchTemplate:
      TemplateId: !GetAtt [ PCSLaunchTemplate, Outputs.ComputeLaunchTemplateId ]
      Version: 1
    SubnetIds:
      - !GetAtt [ Networking, Outputs.DefaultPrivateSubnet ]
    AmiId: !GetAtt [PcsSampleAmi, AmiId]
    InstanceConfigs:
      - InstanceType: !FindInMap [ Architecture, ComputeNodeInstances, !Ref
        NodeArchitecture ]

```

La programación de trabajos se gestiona mediante PCSQueueCompute.

```

PCSQueueCompute:
  Type: AWS::PCS::Queue
  Properties:
    ClusterId: !GetAtt [PCSCluster, Id]
    Name: demo
    ComputeNodeGroupConfigurations:
      - ComputeNodeGroupId: !GetAtt [PCSNodeGroupCompute, Id]

```

La selección de la AMI se realiza automáticamente a través de la función Pcs AMILookup Fn Lambda y los recursos relacionados.

```

PcsAMILookupRole:
  Type: AWS::IAM::Role
  [...]

PcsAMILookupFn:
  Type: AWS::Lambda::Function
  Properties:
    Runtime: python3.12
    Handler: index.handler
    Role: !GetAtt PcsAMILookupRole.Arn
    Code:
      [...]
    Timeout: 30
    MemorySize: 128

```

```
# Example of using the custom resource to look up an AMI
PcsSampleAmi:
  Type: Custom::AMILookup
  Properties:
    ServiceToken: !GetAtt PcsAMILookupFn.Arn
    OperatingSystem: 'amzn2'
    Architecture: !FindInMap [ Architecture, AmiArchParameter, !Ref
NodeArchitecture ]
    SlurmVersion: !Ref SlurmVersion
```

## Salidas

La plantilla genera la identificación y administración de los clústeres URLs mediante `ClusterIdPcsConsoleUrl`, y `Ec2ConsoleUrl`

### Outputs:

#### ClusterId:

Description: The Id of the PCS cluster  
Value: !GetAtt [ PCSCluster, Id ]

#### PcsConsoleUrl:

Description: URL to access the cluster in the PCS console  
Value: !Sub

- https://\${ConsoleDomain}/pcs/home?region=\${AWS::Region}#/clusters/\${ClusterId}
- { ConsoleDomain: !Sub '\${AWS::Region}.console.aws.amazon.com',  
ClusterId: !GetAtt [ PCSCluster, Id ]  
}

#### Export:

Name: !Sub \${AWS::StackName}-PcsConsoleUrl

#### Ec2ConsoleUrl:

Description: URL to access instance(s) in the login node group  
Value: !Sub

- https://\${ConsoleDomain}/ec2/home?region=\${AWS::Region}#Instances:instanceState=running;tag:aws:pcs:compute-node-group-id=\${NodeGroupLoginId}
- { ConsoleDomain: !Sub '\${AWS::Region}.console.aws.amazon.com',  
NodeGroupLoginId: !GetAtt [ PCSNodeGroupLogin, Id ]  
}

#### Export:

Name: !Sub \${AWS::StackName}-Ec2ConsoleUrl

# AWS CloudFormation plantillas para crear un clúster de AWS PCS de muestra

Región de AWS nombre	Región de AWS	Ver fuente	Ver en AWS Infrastructure Composer	Pila de lanzamiento
Este de EE. UU. (Norte de Virginia)	us-east-1	<a href="#">Descarga YAML</a>	<a href="#">Ver en AWS Infrastructure Composer</a>	<a href="#">Launch Stack</a>
Este de EE. UU. (Ohio)	us-east-2	<a href="#">Descarga YAML</a>	<a href="#">Ver en AWS Infrastructure Composer</a>	<a href="#">Launch Stack</a>
EE. UU. Oeste (Oregon)	us-west-2	<a href="#">Descarga YAML</a>	<a href="#">Ver en AWS Infrastructure Composer</a>	<a href="#">Launch Stack</a>
Asia Pacífico (Singapur)	ap-southeast-1	<a href="#">Descarga YAML</a>	<a href="#">Ver en AWS Infrastructure Composer</a>	<a href="#">Launch Stack</a>
Asia Pacífico (Sídney)	ap-southeast-2	<a href="#">Descarga YAML</a>	<a href="#">Ver en AWS Infrastructure Composer</a>	<a href="#">Launch Stack</a>
Asia Pacífico (Tokio)	ap-northeast-1	<a href="#">Descarga YAML</a>	<a href="#">Ver en AWS Infrastructure Composer</a>	<a href="#">Launch Stack</a>
Europa (Fráncfort)	eu-central-1	<a href="#">Descarga YAML</a>	<a href="#">Ver en AWS Infrastructure Composer</a>	<a href="#">Launch Stack</a>

Región de AWS nombre	Región de AWS	Ver fuente	Ver en AWS Infrastructure Composer	Pila de lanzamiento
Europa (Irlanda)	eu-west-1	<a href="#">Descarga YAML</a>	<a href="#">Ver en AWS Infrastructure Composer</a>	
Europa (Estocolmo)	eu-north-1	<a href="#">Descarga YAML</a>	<a href="#">Ver en AWS Infrastructure Composer</a>	

# AWS Clústeres PCS

Un clúster AWS PCS consta de los siguientes componentes:

- Instancias gestionadas del software programador del sistema HPC, como el daemon de control Slurm (`slurmctld`)
- Componentes que se integran con el programador del sistema HPC para aprovisionar y gestionar las instancias de Amazon EC2.
- Componentes que se integran con el programador del sistema HPC para transmitir registros y métricas a Amazon. CloudWatch

Estos componentes se ejecutan en una cuenta gestionada por AWS. Trabajan juntos para gestionar las EC2 instancias de Amazon en tu cuenta de cliente. AWS PCS proporciona interfaces de red elásticas en su subred de Amazon VPC para proporcionar conectividad desde el software del programador a las EC2 instancias de Amazon (por ejemplo, para permitir la programación de trabajos por lotes en ellas y permitir a los usuarios ejecutar comandos del programador para enumerar y administrar esos trabajos).

## Temas

- [Creación de un clúster en AWS Parallel Computing Service](#)
- [Eliminar un clúster en AWS PCS](#)
- [Tamaño del clúster en AWS PCS](#)
- [Trabajar con secretos de clústeres en AWS PCS](#)

## Creación de un clúster en AWS Parallel Computing Service

En este tema se proporciona una descripción general de las opciones disponibles y se describe lo que se debe tener en cuenta al crear un clúster en AWS Parallel Computing Service (AWS PCS). Si es la primera vez que crea un clúster de AWS PCS, le recomendamos que haga lo siguiente [Comience con AWS Parallel Computing Service](#). El tutorial puede ayudarle a crear un sistema HPC que funcione sin tener que ampliar todas las opciones y arquitecturas de sistema disponibles.

## Requisitos previos

- Una VPC y una subred existentes que cumplen los requisitos. [AWS Redes PCS](#) Antes de implementar un clúster para su uso en producción, le recomendamos que conozca a fondo los requisitos de VPC y subred. Para crear una VPC y una subred, consulte. [Creación de una VPC para su AWS clúster de PCS](#)
- Un [director de IAM](#) con permisos para crear y administrar AWS los recursos de PCS. Para obtener más información, consulte [Servicio de Gestión de Identidad y Acceso para Computación AWS Paralela](#).

## Cree un clúster de AWS PCS

Puede usar AWS Management Console o AWS CLI para crear un clúster.

### AWS Management Console

Para crear un clúster

1. Abra la consola AWS PCS en [https://console.aws.amazon.com/pcs/home#/clusters\\_y seleccione Crear clúster](https://console.aws.amazon.com/pcs/home#/clusters_y_seleccione_Crear_clúster).
2. En la sección Configuración del clúster, introduzca los siguientes campos:
  - Nombre del clúster: un nombre para el clúster. El nombre solo puede contener caracteres alfanuméricos (con distinción de mayúsculas y minúsculas) y guiones. Debe empezar por un carácter alfabético y no puede tener más de 40 caracteres. El nombre debe ser único dentro del grupo Región de AWS y en el Cuenta de AWS que se va a crear el clúster.
  - Planificador: elige un programador y una versión. Para obtener más información, consulte [Versiones Slurm en PCS AWS](#).
  - Tamaño del mando: elige un tamaño para el mando. Esto determina cuántos trabajos y nodos de cómputo simultáneos puede administrar el clúster de AWS PCS. Solo puede establecer el tamaño de la controladora cuando se crea el clúster. Para obtener más información sobre el tamaño, consulte [Tamaño del clúster en AWS PCS](#).
3. En la sección Redes, seleccione valores para los siguientes campos:
  - VPC: elija una VPC existente que cumpla con los requisitos de PCS. AWS Para obtener más información, consulte [AWS Requisitos y consideraciones de PCS, VPC y subred](#).

Después de crear el clúster, no puede cambiar su VPC. VPCs Si no aparece ninguna, primero debe crear una.

- Subred: se muestran todas las subredes disponibles en la VPC seleccionada. Elija una subred que cumpla con los requisitos de subred del PCS AWS . Para obtener más información, consulte [AWS Requisitos y consideraciones de PCS, VPC y subred](#). Le recomendamos que seleccione una subred privada para evitar exponer los puntos finales de su programador a la Internet pública.
  - Grupos de seguridad: especifique los grupos de seguridad que desea que AWS PCS asocie a las interfaces de red que crea para su clúster. Debe seleccionar al menos un grupo de seguridad que permita la comunicación entre el clúster y sus nodos de procesamiento. Para obtener más información, consulte [Requisitos y consideraciones sobre los grupos de seguridad](#).
4. (Opcional) En la sección de configuración de la contabilidad de Slurm, puede activar la contabilidad de Slurm y establecer los parámetros de la contabilidad. Para obtener más información, consulte [Contabilidad de barrios bajos en PCS AWS](#).
  5. (Opcional) En la sección de configuración de Slurm, puede especificar las opciones de configuración de Slurm que anulan los valores predeterminados establecidos por el PCS: AWS
    - Reduzca el tiempo de inactividad: esto controla cuánto tiempo permanecen activos los nodos de cómputo provisionados dinámicamente una vez finalizados o terminados los trabajos que se les asignan. Si se establece en un valor más largo, es más probable que se ejecute un trabajo posterior en el nodo, pero puede aumentar los costes. Un valor más bajo reducirá los costes, pero puede aumentar la proporción de tiempo que el sistema HPC dedica a provisionar nodos en lugar de a ejecutar tareas en ellos.
    - Prolog: se trata de una ruta totalmente cualificada para acceder a un directorio de scripts de prolog en las instancias de su grupo de nodos de cómputo. Esto corresponde a la configuración de [Prolog en Slurm](#). Tenga en cuenta que debe ser un directorio, no una ruta a un ejecutable específico.
    - Epilog: esta es una ruta totalmente cualificada para acceder a un directorio de scripts de epilog en las instancias de su grupo de nodos de cómputo. Esto corresponde a la configuración de [Epilog](#) en Slurm. Tenga en cuenta que debe ser un directorio, no una ruta a un ejecutable específico.
    - Seleccione los parámetros de tipo: esto ayuda a controlar el algoritmo de selección de recursos utilizado por Slurm. Si se establece este valor en, CR\_CPU\_Memory se

activará la programación basada en la memoria, mientras que si se establece en, se CR\_CPU activará la programación solo para la CPU. Este parámetro corresponde a la [SelectTypeParameters](#) configuración de Slurm, en la que PCS establece. `SelectType select/cons_tres AWS`

6. (Opcional) En Etiquetas, añada cualquier etiqueta a su clúster de AWS PCS.
7. Elija Create cluster. El campo Estado se muestra `Creating` mientras el AWS PCS crea el clúster. Este proceso puede tardar varios minutos.

#### Important

Solo puede haber 1 clúster en un `Creating` estado Región de AWS por cada uno Cuenta de AWS. AWS Cuando intenta crear un clúster, PCS devuelve un error si ya existe un clúster en ese `Creating` estado.

## AWS CLI

Para crear un clúster

1. Creación del clúster con el siguiente comando. Antes de ejecutar el comando, realice los siguientes reemplazos:
  - Sustitúyalo por el ID *region* con el Región de AWS que desea crear el clúster, por `ejemplous-east-1`.
  - Reemplace *my-cluster* por el nombre del clúster. El nombre solo puede contener caracteres alfanuméricos (con distinción de mayúsculas y minúsculas) y guiones. Debe empezar por un carácter alfabético y no puede tener más de 40 caracteres. El nombre debe ser único dentro del clúster Región de AWS y en el Cuenta de AWS lugar en el que vaya a crearlo.
  - **24.11** Sustitúyalo por cualquier versión compatible de Slurm.

#### Note

AWS Actualmente, PCS es compatible con Slurm 24.11, 24.05 y 23.11.

- Sustitúyalo por cualquier tamaño de *SMALL* clúster compatible. Esto determina cuántos trabajos y nodos de cómputo simultáneos puede administrar el clúster de AWS PCS. Solo

se puede configurar cuando se crea el clúster. Para obtener más información sobre el tamaño, consulte [Tamaño del clúster en AWS PCS](#).

- Sustituya el valor de `subnetIds` el suyo propio. Le recomendamos que seleccione una subred privada para evitar exponer los puntos finales de su programador a la Internet pública.
- Especifique los `securityGroupIds` que desea que el AWS PCS asocie a las interfaces de red que crea para el clúster. Los grupos de seguridad deben estar en la misma VPC que el clúster. Debe seleccionar al menos un grupo de seguridad que permita la comunicación entre el clúster y sus nodos de procesamiento. Para obtener más información, consulte [Requisitos y consideraciones sobre los grupos de seguridad](#).
- Si lo desea, puede proporcionar una clave KMS personalizada para cifrar los datos del controlador mediante `--kms-key-id kms-key` ella. `kms-key` Sustitúyalo por un ARN, un identificador de clave o un alias de KMS existentes. Tenga en cuenta que la cuenta utilizada para crear el clúster debe tener `kms:Decrypt` privilegios en la clave KMS personalizada.

```
aws pcs create-cluster --region region \  
  --cluster-name my-cluster \  
  --scheduler type=SLURM,version=24.11 \  
  --size SMALL \  
  --networking subnetIds=subnet-ExampleId1,securityGroupIds=sg-ExampleId1
```

- Si lo desea, puede añadir la `--slurm-configuration` opción de personalizar el comportamiento de Slurm y especificar las opciones de configuración de Slurm. El siguiente ejemplo establece el tiempo de inactividad reducido en 60 minutos (3600 segundos), habilita la contabilidad de Slurm y especifica la configuración como valor para `slurm.conf` `slurmCustomSettings` Para obtener más información, consulte [Contabilidad de barrios bajos en PCS AWS](#).

 Note

Se admite la contabilidad en Slurm 24.11 o versiones posteriores.

```
aws pcs create-cluster --region region \  
  --cluster-name my-cluster \  
  --slurm-configuration slurmCustomSettings
```

```
--scheduler type=SLURM,version=24.11 \  
--size SMALL \  
--networking subnetIds=subnet-ExampleId1,securityGroupIds=sg-ExampleId1  
--slurm-configuration  
scaleDownIdleTimeInSeconds=3600,accounting='{mode=STANDARD}',slurmCustomSettings='{p
```

2. El aprovisionamiento del clúster puede tardar varios minutos. Puede consultar el estado del clúster con el siguiente comando. No proceda a crear colas ni a calcular grupos de nodos hasta que aparezca el campo de estado del clúster. ACTIVE

```
aws pcs get-cluster --region region --cluster-identifier my-cluster
```

### Important

Solo puede haber 1 clúster en un Creating estado Región de AWS por cada uno. Cuenta de AWS AWS Cuando intenta crear un clúster, PCS devuelve un error si ya existe un clúster en ese Creating estado.

Próximos pasos recomendados para su clúster

- Agregue grupos de nodos de cómputo.
- Añada colas.
- Habilitar el registro.

## Eliminar un clúster en AWS PCS

En este tema se proporciona información general sobre cómo eliminar un clúster de AWS PCS.

### Consideraciones a la hora de eliminar un clúster de AWS PCS

- Se deben eliminar todas las colas asociadas al clúster antes de poder eliminar el clúster. Para obtener más información, consulte [Eliminar una cola en PCS AWS](#).
- Todos los grupos de nodos de procesamiento asociados al clúster deben eliminarse antes de poder eliminar el clúster. Para obtener más información, consulte [Eliminar un grupo de nodos de cómputo en AWS PCS](#).

## Elimine el clúster

Puede usar AWS Management Console o AWS CLI para eliminar un clúster.

### AWS Management Console

Para eliminar un clúster

1. Abra la [consola AWS PCS](#).
2. Seleccione el clúster que desee eliminar.
3. Elija Eliminar.
4. Aparece el campo Estado del clúster `Deleting`. Puede tardar varios minutos en completarse.

### AWS CLI

Para eliminar un clúster

1. Use el siguiente comando para eliminar un clúster, con estas sustituciones:
  - *region-code* Reemplácelo por el Región de AWS que contiene su clúster.
  - *my-cluster* Sustitúyalo por el nombre o el ID de tu clúster.

```
aws pcs delete-cluster --region region-code --cluster-identifier my-cluster
```

2. Eliminar el clúster puede tardar varios minutos. Puede comprobar el estado del clúster con el siguiente comando.

```
aws pcs get-cluster --region region-code --cluster-identifier my-cluster
```

## Tamaño del clúster en AWS PCS

AWS El PCS proporciona clústeres seguros y de alta disponibilidad, a la vez que automatiza tareas clave como la aplicación de parches, el aprovisionamiento de nodos y las actualizaciones.

Al crear un clúster, se selecciona su tamaño en función de dos factores:

- La cantidad de nodos de cómputo que administrará
- La cantidad de trabajos activos y en cola que espera ejecutar en el clúster

### Important

No puede cambiar el tamaño del clúster después de crearlo. Si necesita cambiar el tamaño, debe crear un clúster nuevo.

Tamaño del clúster de Slurm	Número de instancias administradas	Número de trabajos activos y en cola
Pequeña	Hasta 32	Hasta 256
Medio	Hasta 512	Hasta 8192
Grande	Hasta 2048	Hasta 16384

### Ejemplos

- Si su clúster tendrá hasta 24 instancias administradas y ejecutará hasta 100 trabajos, elija Small.
- Si el clúster tendrá hasta 24 instancias administradas y ejecutará hasta 1000 trabajos, elija Medium.
- Si su clúster tendrá hasta 1000 instancias administradas y ejecutará hasta 100 trabajos, elija Grande.
- Si el clúster tendrá hasta 1000 instancias administradas y ejecutará hasta 10 000 trabajos, elija Grande.

## Trabajar con secretos de clústeres en AWS PCS

Como parte de la creación de un clúster, AWS PCS crea un secreto de clúster que es necesario para conectarse al programador de tareas del clúster. También se crean grupos de nodos de cómputo de AWS PCS, que definen conjuntos de instancias que se van a lanzar en respuesta a eventos de escalado. AWS PCS configura las instancias lanzadas por esos grupos de nodos de cómputo con el secreto del clúster para que puedan conectarse al programador de tareas. Hay casos en los que es

posible que desee configurar los clientes de Slurm manualmente. Los ejemplos incluyen la creación de un nodo de inicio de sesión persistente o la configuración de un administrador de flujo de trabajo con capacidades de administración de trabajos.

AWS PCS almacena el secreto del clúster como un [secreto gestionado](#) con el prefijo `pcs!`. AWS Secrets Manager El coste del secreto está incluido en el coste del uso del AWS PCS.

#### Warning

No modifique el secreto de su clúster. AWS El PCS no podrá comunicarse con el clúster si modificas el secreto del clúster. AWS PCS no admite la rotación del secreto del clúster. Debe crear un clúster nuevo si necesita modificar su secreto de clúster.

## Contenido

- [Se usa AWS Secrets Manager para buscar el secreto del clúster](#)
- [Utilice AWS PCS para encontrar el secreto del clúster](#)
- [Obtén el secreto del cúmulo de Slurm](#)

## Se usa AWS Secrets Manager para buscar el secreto del clúster

### AWS Management Console

1. Vaya a la [consola del administrador de secretos](#).
2. Selecciona Secretos y, a continuación, busca el `pcs!` prefijo.

#### Note

El secreto de un clúster de AWS PCS tiene un nombre en el formato `pcs!slurm-secret-cluster-id` donde *cluster-id* está el ID del clúster de AWS PCS.

### AWS CLI

Cada secreto de clúster de AWS PCS también está etiquetado con `aws:pcs:cluster-id`. Puede obtener el identificador secreto de un clúster con el siguiente comando. Realice estas sustituciones antes de ejecutar el comando:

- *region* Región de AWS Sustitúyalo por el para crear el clúster, por ejemplo `us-east-1`.
- *cluster-id* Sustitúyalo por el ID del clúster de AWS PCS para encontrar el secreto del clúster.

```
aws secretsmanager list-secrets \  
  --region region \  
  --filters Key=tag-key,Values=aws:pcs:cluster-id \  
           Key=tag-value,Values=cluster-id
```

## Utilice AWS PCS para encontrar el secreto del clúster

Puede utilizar el AWS CLI para encontrar el ARN de un secreto de clúster de AWS PCS. Introduzca el comando siguiente y realice las siguientes sustituciones:

- *region* Región de AWS Sustitúyalo por el para crear el clúster, por ejemplo `us-east-1`.
- *my-cluster* Sustitúyalo por el nombre o identificador del clúster.

```
aws pcs get-cluster --region region --cluster-identifier my-cluster
```

El siguiente ejemplo de salida proviene del `get-cluster` comando. Puedes usar `secretArn` y `secretVersion` juntos para obtener el secreto.

```
{  
  "cluster": {  
    "name": "get-started",  
    "id": "pcs_123456abcd",  
    "arn": "arn:aws:pcs:us-east-1:111122223333:cluster/pcs_123456abcd",  
    "status": "ACTIVE",  
    "createdAt": "2024-12-17T21:03:52+00:00",  
    "modifiedAt": "2024-12-17T21:03:52+00:00",  
    "scheduler": {  
      "type": "SLURM",  
      "version": "24.05"  
    },  
    "size": "SMALL",  
    "slurmConfiguration": {  
      "authKey": {
```

```

        "secretArn": "arn:aws:secretsmanager:us-east-1:111122223333:secret:pcs!
slurm-secret-pcs_123456abcd-a12ABC",
        "secretVersion": "ef232370-d3e7-434c-9a87-ec35c1987f75"
    }
},
"networking": {
    "subnetIds": [
        "subnet-0123456789abcdef0"
    ],
    "securityGroupIds": [
        "sg-0123456789abcdef0"
    ]
},
"endpoints": [
    {
        "type": "SLURMCTLD",
        "privateIpAddress": "10.3.149.220",
        "port": "6817"
    }
]
}
}

```

## Obtén el secreto del cúmulo de Slurm

Puede usar Secrets Manager para obtener la versión actual codificada en base64 de un secreto de clúster de Slurm. El siguiente ejemplo usa el AWS CLI Realice las siguientes sustituciones antes de ejecutar el comando.

- *region* Región de AWS Sustitúyala por la para crear el clúster, por ejemplo `us-east-1`.
- *secret-arn* Sustitúyalo `secretArn` por el de un clúster de AWS PCS.

```

aws secretsmanager get-secret-value \
  --region region \
  --secret-id 'secret-arn' \
  --version-stage AWSCURRENT \
  --query 'SecretString' \
  --output text

```

Para obtener información sobre cómo utilizar el secreto del clúster de Slurm, consulte [Uso de instancias independientes como nodos de inicio de sesión de AWS PCS](#)

## Permisos

Utiliza un principal de IAM para obtener el secreto del clúster de Slurm. El director de IAM debe tener permiso para leer el secreto. Para obtener más información, consulte [los términos y conceptos de las funciones](#) en la Guía del AWS Identity and Access Management usuario.

El siguiente ejemplo de política de IAM permite el acceso a un ejemplo de secreto de clúster.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretValueRetrievalAndVersionListing",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource": "arn:aws:secretsmanager:us-east-1:012345678901:secret:pcs!
slurm-secret-s3431v9rx2-FN7tJF"
    }
  ]
}
```

# AWS Grupos de nodos de cómputo PCS

Un grupo de nodos de cómputo de AWS PCS es un conjunto lógico de nodos ( EC2 instancias de Amazon). Estos nodos se pueden usar para ejecutar tareas informáticas, así como para proporcionar acceso interactivo y basado en shell a un sistema HPC. Un grupo de nodos de cómputo consta de reglas para crear nodos, que incluyen qué tipos de instancias de Amazon EC2 usar, cuántas instancias ejecutar, si usar instancias puntuales o instancias bajo demanda, qué subredes y grupos de seguridad usar y cómo configurar cada instancia cuando se lanza. Cuando se actualizan esas reglas, AWS PCS actualiza los recursos asociados al grupo de nodos de cómputo para que coincidan.

## Temas

- [Creación de un grupo de nodos de cómputo en AWS PCS](#)
- [Actualización de un grupo de nodos de cómputo AWS PCS](#)
- [Eliminar un grupo de nodos de cómputo en AWS PCS](#)
- [Obtenga detalles del grupo de nodos de cómputo en AWS PCS](#)
- [Búsqueda de instancias de grupos de nodos de cómputo en AWS PCS](#)

## Creación de un grupo de nodos de cómputo en AWS PCS

En este tema se proporciona una descripción general de las opciones disponibles y se describe lo que se debe tener en cuenta al crear un grupo de nodos de procesamiento en AWS Parallel Computing Service (AWS PCS). Si es la primera vez que crea un grupo de nodos de cómputo en AWS PCS, le recomendamos que siga el tutorial que aparece en [Comience con AWS Parallel Computing Service](#). El tutorial puede ayudarle a crear un sistema HPC que funcione sin tener que ampliar todas las opciones y arquitecturas de sistema disponibles.

## Requisitos previos

- Cuotas de servicio suficientes para lanzar el número deseado de EC2 instancias en su. Región de AWS Puede utilizarlas [AWS Management Console](#) para comprobar y solicitar aumentos en sus cuotas de servicio.
- Una VPC y subredes existentes que cumplen con los requisitos de red de AWS PCS. Le recomendamos que comprenda detenidamente estos requisitos antes de implementar un clúster para su uso en producción. Para obtener más información, consulte [AWS Requisitos y](#)

[consideraciones de PCS, VPC y subred](#). También puede usar una CloudFormation plantilla para crear una VPC y subredes. AWS proporciona una receta de HPC para la plantilla. CloudFormation Para obtener más información, consulte [aws-hpc-recipes](#) en GitHub.

- Un perfil de instancia de IAM con permisos para activar la acción de la `RegisterComputeNodeGroupInstance` API de AWS PCS y acceder a cualquier otro AWS recurso necesario para las instancias de su grupo de nodos. Para obtener más información, consulte [Perfiles de instancia de IAM para AWS Parallel Computing Service](#).
- Una plantilla de lanzamiento para las instancias de tu grupo de nodos. Para obtener más información, consulte [Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS](#).
- Para crear un grupo de nodos de cómputo que utilice instancias de Amazon EC2 Spot, debe tener el rol vinculado al servicio de `AWSServiceRoleForEC2Spot` en su. Cuenta de AWS Para obtener más información, consulte [Función de Amazon EC2 Spot para AWS PCS](#).

## Cree un grupo de nodos de cómputo en PCS AWS

Puede crear un grupo de nodos de cómputo mediante el AWS Management Console o el AWS CLI.

### AWS Management Console

Para crear su grupo de nodos de cómputo mediante la consola

1. Abra la [consola AWS PCS](#).
2. Seleccione el clúster en el que desee crear un grupo de nodos de cómputo. Diríjase a los grupos de nodos de cómputo y elija Crear.
3. En la sección de configuración del grupo de nodos de Compute, proporciona un nombre para el grupo de nodos. El nombre solo puede contener caracteres alfanuméricos y guiones que distingan mayúsculas de minúsculas. Debe empezar por un carácter alfabético y no puede tener más de 25 caracteres. El nombre debe ser único en el clúster.
4. En Configuración informática, introduzca o seleccione estos valores:
  - a. EC2 Plantilla de lanzamiento: seleccione una plantilla de lanzamiento personalizada para utilizarla en este grupo de nodos. Las plantillas de lanzamiento se pueden utilizar para personalizar la configuración de la red, como la subred y los grupos de seguridad, la configuración de supervisión y el almacenamiento a nivel de instancia. Si no tienes una plantilla de lanzamiento preparada, consulta [Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS](#) para aprender a crear una.

**⚠ Important**

AWS PCS crea una plantilla de lanzamiento gestionada para cada grupo de nodos de cómputo. Estos se denominan `pcs-identifier-do-not-delete`. No los seleccione cuando cree o actualice un grupo de nodos de procesamiento, o el grupo de nodos no funcionará correctamente.

- b. EC2 versión de la plantilla de lanzamiento: debe seleccionar una versión de su plantilla de lanzamiento personalizada. Si cambia la versión más adelante, debe actualizar el grupo de nodos de procesamiento para detectar cambios en la plantilla de lanzamiento. Para obtener más información, consulte [Actualización de un grupo de nodos de cómputo AWS PCS](#).
- c. ID de AMI: si tu plantilla de lanzamiento no incluye un ID de AMI o si quieres anular el valor de la plantilla de lanzamiento, proporciona un ID de AMI aquí. Tenga en cuenta que la AMI utilizada para el grupo de nodos debe ser compatible con el AWS PCS. También puede seleccionar un ejemplo de AMI proporcionado por AWS. Para obtener más información sobre este tema, consulte [Amazon Machine Images \(AMIs\) para AWS PCS](#).
- d. Perfil de instancia de IAM: elija un perfil de instancia para el grupo de nodos. Un perfil de instancia otorga a la instancia permisos para acceder a los AWS recursos y servicios de forma segura. Si no tiene uno preparado, consulte [Perfiles de instancia de IAM para AWS Parallel Computing Service](#) para obtener información sobre cómo crear uno.
- e. Subredes: elija una o más subredes en la VPC en la que se implementa el clúster de AWS PCS. Si seleccionas varias subredes, las comunicaciones EFA no estarán disponibles entre los nodos y es posible que la comunicación entre los nodos de distintas subredes tenga una mayor latencia. Asegúrese de que las subredes que especifique aquí coincidan con las que haya definido en la plantilla de lanzamiento. EC2
- f. Instancias: elija uno o más tipos de instancias para cumplir con las solicitudes de escalado del grupo de nodos. Todos los tipos de instancias deben tener la misma arquitectura de procesador (x86\_64 o arm64) y el mismo número de v. CPUs Si las instancias lo tienen GPUs, todos los tipos de instancias deben tener el mismo número de GPUs
- g. Configuración de escalado: especifique la cantidad mínima y máxima de instancias para el grupo de nodos. Puede definir una configuración estática, en la que hay un número fijo de nodos en ejecución, o una configuración dinámica, en la que se pueden ejecutar

hasta el número máximo de nodos. Para una configuración estática, defina el mínimo y el máximo en el mismo número, superior a cero. Para una configuración dinámica, establece el número mínimo de instancias en cero y el máximo en un número superior a cero. AWS PCS no admite grupos de nodos de cómputo con una combinación de instancias estáticas y dinámicas.

5. (Opcional) En Configuración adicional, especifique lo siguiente:
  - a. Opción de compra: seleccione entre instancias puntuales y bajo demanda.
  - b. Estrategia de asignación: si ha seleccionado la opción de compra puntual, puede especificar cómo se eligen los grupos de capacidad puntuales al lanzar instancias en el grupo de nodos. Para obtener más información, consulte [Estrategias de asignación para instancias puntuales](#) en la Guía del usuario de Amazon Elastic Compute Cloud. Esta opción no tiene efecto si ha seleccionado la opción de compra bajo demanda.
6. (Opcional) En el Slurm en la sección de configuración personalizada, proporcione estos valores:
  - a. Peso: este valor establece la prioridad de los nodos del grupo para fines de programación. Los nodos con pesos más bajos tienen mayor prioridad y las unidades son arbitrarias. Para obtener más información, consulte [Peso](#) en Slurm .
  - b. Memoria real: este valor establece el tamaño (en GB) de la memoria real en los nodos del grupo de nodos. Está pensado para usarse junto con la CR\_CPU\_Memory opción del clúster Slurm configuración en AWS PCS. Para obtener más información, consulte [RealMemory](#) en la Slurm .
7. (Opcional) En Etiquetas, agrega cualquier etiqueta a tu grupo de nodos de cómputo.
8. Selecciona Crear grupo de nodos de cómputo. El campo Estado se muestra Creating mientras AWS PCS aprovisiona el grupo de nodos. Esto puede tardar varios minutos.

#### Siguiente paso recomendado

- Agregue su grupo de nodos a una cola en AWS PCS para que pueda procesar los trabajos.

## AWS CLI

Para crear su grupo de nodos de cómputo mediante AWS CLI

Cree su cola con el siguiente comando. Antes de ejecutar el comando, realice los siguientes reemplazos:

1. *region* Sustitúyalo por el ID en el Región de AWS que se va a crear el clúster, por ejemplo. `us-east-1`
2. *my-cluster* Sustitúyalo por el nombre o `clusterId` el de tu clúster.
3. *my-node-group* Sustitúyalo por el nombre de tu grupo de nodos de procesamiento. El nombre solo puede contener caracteres alfanuméricos (con distinción de mayúsculas y minúsculas) y guiones. Debe empezar por un carácter alfabético y no puede tener más de 25 caracteres. El nombre debe ser único en el clúster.
4. *subnet-ExampleID1* Sustitúyala por una o más subredes IDs de la VPC del clúster.
5. *lt-ExampleID1* Sustitúyalo por el ID de la plantilla de lanzamiento personalizada. Si no tienes una preparada, consulta [Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS](#) para aprender a crearla.

### Important

AWS PCS crea una plantilla de lanzamiento gestionado para cada grupo de nodos de cómputo. Estos se denominan `pcs-identifier-do-not-delete`. No los seleccione cuando cree o actualice un grupo de nodos de procesamiento, o el grupo de nodos no funcionará correctamente.

6. *launch-template-version* Sustitúyala por una versión de plantilla de lanzamiento específica. AWS PCS asocia su grupo de nodos a esa versión específica de la plantilla de lanzamiento.
7. *arn:InstanceProfile* Sustitúyalo por el ARN de tu perfil de instancia de IAM. Si no tiene uno preparado, consulte [Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS](#) para obtener orientación.
8. Sustituya *min-instances* y *max-instances* por valores enteros. Puede definir una configuración estática, en la que hay un número fijo de nodos en ejecución, o una configuración dinámica, en la que se puede ejecutar hasta el número máximo de nodos. Para una configuración estática, defina el mínimo y el máximo en el mismo número, superior a cero. Para una configuración dinámica, establece el número mínimo de instancias en cero y

el máximo en un número superior a cero. AWS PCS no admite grupos de nodos de cómputo con una combinación de instancias estáticas y dinámicas.

9. *t3.large* Sustitúyala por otro tipo de instancia. Puede añadir más tipos de instancias especificando una lista de `instanceType` ajustes. Por ejemplo, `--instance-configs instanceType=c6i.16xlarge instanceType=c6a.16xlarge`. Todos los tipos de instancias deben tener la misma arquitectura de procesador (x86\_64 o arm64) y el mismo número de v. CPUs Si las instancias lo tienen GPUs, todos los tipos de instancias deben tener el mismo número de. GPUs

```
aws pcs create-compute-node-group --region region \
  --cluster-identifier my-cluster \
  --compute-node-group-name my-node-group \
  --subnet-ids subnet-ExampleID1 \
  --custom-launch-template id=lt-ExampleID1,version='launch-template-version' \
  --iam-instance-profile-arn=arn:InstanceProfile \
  --scaling-config minInstanceCount=min-instances,maxInstanceCount=max-instance \
  --instance-configs instanceType=t3.large
```

Hay varios ajustes de configuración opcionales que puedes añadir al `create-compute-node-group` comando.

- Puede especificar `--amiId` si su plantilla de lanzamiento personalizada no incluye una referencia a una AMI o si desea anular ese valor. Tenga en cuenta que la AMI utilizada para el grupo de nodos debe ser compatible con el AWS PCS. También puede seleccionar un ejemplo de AMI proporcionado por AWS. Para obtener más información sobre este tema, consulte [Amazon Machine Images \(AMIs\) para AWS PCS](#).
- Puede seleccionar entre instancias bajo demanda (ONDEMAND) y Spot (SPOT) utilizando `--purchase-option`. Bajo demanda es la opción predeterminada. Si elige instancias puntuales, también puede utilizarlas `--allocation-strategy` para definir cómo AWS PCS elige los grupos de capacidad puntuales cuando lanza instancias en el grupo de nodos. Para obtener más información, consulte [Estrategias de asignación para instancias puntuales](#) en la Guía del usuario de Amazon Elastic Compute Cloud.
- Es posible proporcionar Slurm opciones de configuración para los nodos del grupo de nodos mediante `--slurm-configuration`. Puede establecer el peso (prioridad de programación) y la memoria real. Los nodos con pesos más bajos tienen mayor prioridad y las unidades son arbitrarias. Para obtener más información, consulte [Peso](#) en Slurm . La memoria real establece el tamaño (en GB) de la memoria real en los nodos del grupo de nodos. Está

diseñado para usarse junto con la `CR_CPU_Memory` opción de clúster de AWS PCS de su Slurm configuración. Para obtener más información, consulte [RealMemory](#) en la Slurm .

 Important

La creación del grupo de nodos de procesamiento puede tardar varios minutos.

Puede consultar el estado de su grupo de nodos con el siguiente comando. No podrás asociar el grupo de nodos a una cola hasta que se alcance `ACTIVE` su estado.

```
aws pcs get-compute-node-group --region region \  
  --cluster-identifier my-cluster \  
  --compute-node-group-identifier my-node-group
```

## Actualización de un grupo de nodos de cómputo AWS PCS

En este tema se proporciona información general sobre las opciones disponibles y se describe lo que se debe tener en cuenta al actualizar un grupo de nodos de cómputo de AWS PCS.

### Opciones para actualizar un grupo de nodos de cómputo de AWS PCS

La actualización de un grupo de nodos de procesamiento de AWS PCS le permite cambiar las propiedades de las instancias lanzadas por AWS PCS, así como las reglas de lanzamiento de esas instancias. Por ejemplo, puede reemplazar la AMI de las instancias del grupo de nodos por otra que tenga instalado un software diferente. O bien, puede actualizar los grupos de seguridad para cambiar la conectividad de red entrante o saliente. También puede cambiar la configuración de escalado o incluso cambiar la opción de compra preferida hacia o desde las instancias Spot.

La siguiente configuración del grupo de nodos no se puede modificar después de su creación:

- Nombre
- instancias

## Consideraciones a la hora de actualizar un grupo de nodos de procesamiento de AWS PCS

Los grupos de nodos de cómputo definen las EC2 instancias que se utilizan para procesar trabajos, proporcionar acceso interactivo al shell y otras tareas. Suelen estar asociados a una o más colas de AWS PCS. Al actualizar el grupo de nodos de cómputo para cambiar su comportamiento (o el de sus nodos), tenga en cuenta lo siguiente:

- Los cambios en las propiedades del grupo de nodos de cómputo se hacen efectivos cuando el estado del grupo de nodos de cómputo cambia de Actualizado a Activo. Se lanzan nuevas instancias con las propiedades actualizadas.
- Las actualizaciones que no afectan a la configuración de nodos específicos no afectan a los nodos en ejecución. Por ejemplo, añadir una subred y cambiar la estrategia de asignación.
- Si actualiza la plantilla de lanzamiento de un grupo de nodos de cómputo, debe actualizar el grupo de nodos de cómputo para usar la nueva versión.
- Para añadir o eliminar un grupo de seguridad de los nodos de un grupo de nodos de procesamiento, edite su plantilla de lanzamiento y actualice el grupo de nodos de procesamiento. Se lanzan nuevas instancias con el conjunto actualizado de grupos de seguridad.
- Si editas directamente un grupo de seguridad utilizado por un grupo de nodos de procesamiento, esto tendrá efecto inmediato en las instancias en ejecución y en las futuras.
- Si agregas o eliminas permisos del perfil de instancias de IAM utilizado por un grupo de nodos de procesamiento, esto tendrá efecto inmediato en las instancias en ejecución y en las futuras.
- Para cambiar la AMI utilizada por las instancias de un grupo de nodos de cómputo, actualice el grupo de nodos de cómputo (o su plantilla de lanzamiento) para usar la nueva AMI y espere a que AWS PCS sustituya las instancias.
- AWS El PCS reemplaza las instancias existentes en el grupo de nodos tras una operación de actualización del grupo de nodos. Si hay trabajos en ejecución en un nodo, se permite que dichos trabajos se completen antes de que AWS PCS sustituya el nodo. Los procesos de usuario interactivos (por ejemplo, en las instancias de nodos de inicio de sesión) finalizan. El estado del grupo de nodos vuelve `Active` al que el AWS PCS marca las instancias para su reemplazo, pero el reemplazo real se produce cuando las instancias están inactivas.
- Si reduces el número máximo de instancias permitido en un grupo de nodos de cómputo, AWS PCS eliminará los nodos de Slurm para cumplir con el nuevo máximo. AWS El PCS finaliza las instancias en ejecución asociadas a los nodos de Slurm eliminados. Los trabajos en ejecución en los nodos eliminados fallan y vuelven a sus colas.

- AWS PCS crea una plantilla de lanzamiento gestionada para cada grupo de nodos de cómputo. Se nombran pcs-*identifier*-do-not-delete. No los seleccione al crear o actualizar un grupo de nodos de procesamiento, o el grupo de nodos no funcionará correctamente.
- Si actualiza un grupo de nodos de cómputo para usar Spot como opción de compra, debe tener el rol vinculado al servicio de AWSServiceRoleForEC2Spot en su cuenta. Para obtener más información, consulte [Función de Amazon EC2 Spot para AWS PCS](#).

## Para actualizar un grupo de nodos de cómputo de AWS PCS

Puede actualizar un grupo de nodos mediante la consola de administración de AWS o la CLI de AWS.

### AWS Management Console

Para actualizar un grupo de nodos de cómputo

1. Abra la consola PCS de AWS en `https://console.aws.amazon.com/pcs/home#/clusters`
2. Seleccione el clúster en el que desea actualizar un grupo de nodos de cómputo.
3. Vaya a Grupos de nodos de cómputo, vaya al grupo de nodos que desee actualizar y, a continuación, seleccione Editar.
4. En la configuración informática, en los ajustes adicionales y Slurm en las secciones de ajustes de personalización, actualice todos los valores excepto:
  - Instancias: no puedes cambiar las instancias de un grupo de nodos de cómputo.
5. Elija Actualizar. El campo Estado mostrará la actualización mientras se aplican los cambios.

#### Important

Las actualizaciones de los grupos de nodos de cómputo pueden tardar varios minutos.

## AWS CLI

Para actualizar un grupo de nodos de cómputo

1. Actualice su grupo de nodos de cómputo con el siguiente comando. Antes de ejecutar el comando, realice los siguientes reemplazos:
  - a. *region-code* Sustitúyala por la región de AWS en la que deseas crear tu clúster.
  - b. *my-node-group* Sustitúyalo por el nombre o computeNodeGroupId por el grupo de nodos de cómputo.
  - c. *my-cluster* Sustitúyalo por el nombre o clusterId el de tu clúster.

```
aws pcs update-compute-node-group --region region-code \  
  --cluster-identifier my-cluster \  
  --compute-node-group-identifier my-node-group
```

2. Actualice todos los parámetros del grupo de nodos, excepto `--instance-configs`: Por ejemplo, para configurar un nuevo ID de AMI, pass `--amiId my-custom-ami-id` where *my-custom-ami-id* se sustituye por la AMI que prefiera.

### Important

La actualización del grupo de nodos de cómputo puede tardar varios minutos.

Puedes consultar el estado de tu grupo de nodos con el siguiente comando.

```
aws pcs get-compute-node-group --region region-code \  
  --cluster-identifier my-cluster \  
  --compute-node-group-identifier my-node-group
```

## Eliminar un grupo de nodos de cómputo en AWS PCS

En este tema se proporciona una descripción general de las opciones disponibles y se describe lo que se debe tener en cuenta al eliminar un grupo de nodos de procesamiento en AWS PCS.

## Consideraciones a la hora de eliminar un grupo de nodos de cómputo

Los grupos de nodos de cómputo definen las EC2 instancias que se utilizan para procesar trabajos, proporcionar acceso interactivo al shell y otras tareas. Suelen estar asociados a una o más colas de AWS PCS. Antes de eliminar un grupo de nodos de procesamiento, tenga en cuenta lo siguiente:

- Se cancelará cualquier EC2 instancia lanzada por el grupo de nodos de cómputo. Esto cancelará los trabajos que se estén ejecutando en estas instancias y pondrá fin a la ejecución de los procesos interactivos.
- Debe desasociar el grupo de nodos de cómputo de todas las colas antes de poder eliminarlo. Para obtener más información, consulte [Actualización de una cola de AWS PCS](#).

## Elimine el grupo de nodos de cómputo

Puede usar AWS Management Console o AWS CLI para eliminar un grupo de nodos de procesamiento.

### AWS Management Console

Para eliminar un grupo de nodos de cómputo

1. Abra la [consola AWS PCS](#).
2. Seleccione el clúster del grupo de nodos de cómputo.
3. Vaya a Grupos de nodos de cómputo y seleccione el grupo de nodos de cómputo que desee eliminar.
4. Elija Eliminar.
5. Aparece el campo `EstadoDeleting`. Puede tardar varios minutos en completarse.

#### Note

Puede usar los comandos nativos de su programador para confirmar que se ha eliminado el grupo de nodos de procesamiento. Por ejemplo, usa `sinfo` o `squeue` para Slurm.

## AWS CLI

Para eliminar un grupo de nodos de cómputo

- Usa el siguiente comando para eliminar un grupo de nodos de cómputo, con estos reemplazos:
  - *region-code* Sustitúyalo por el que se encuentra Región de AWS tu clúster.
  - *my-node-group* Sustitúyalo por el nombre o el ID de tu grupo de nodos de procesamiento.
  - *my-cluster* Sustitúyalo por el nombre o el ID de tu clúster.

```
aws pcs delete-compute-node-group --region region-code \  
  --compute-node-group-identifier my-node-group \  
  --cluster-identifier my-cluster
```

Eliminar el grupo de nodos de procesamiento puede tardar varios minutos.

### Note

Puede usar los comandos nativos de su programador para confirmar que se ha eliminado el grupo de nodos de procesamiento. Por ejemplo, usa `sinfo` o `squeue` para Slurm.

## Obtenga detalles del grupo de nodos de cómputo en AWS PCS

Puede usar AWS Management Console o AWS CLI para obtener detalles sobre un grupo de nodos de cómputo, como su ID de grupo de nodos de cómputo, el nombre de recurso de Amazon (ARN) y el ID de Amazon Machine Image (AMI). Estos detalles suelen ser valores obligatorios para las acciones y configuraciones de la API de AWS PCS.

### AWS Management Console

Para obtener los detalles del grupo de nodos de cómputo

1. Abra la [consola AWS PCS](#).
2. Seleccione el clúster.

3. Elija grupos de nodos de cómputo.
4. Elija un grupo de nodos de procesamiento en el panel de lista.

## AWS CLI

Para obtener los detalles del grupo de nodos de cómputo

1. Usa la acción [ListClusters](#) de la API para buscar el nombre o el ID del clúster.

```
aws pcs list-clusters
```

Ejemplo de salida:

```
{
  "clusters": [
    {
      "name": "get-started-cfn",
      "id": "pcs_abc1234567",
      "arn": "arn:aws:pcs:us-east-1:111122223333:cluster/pcs_abc1234567",
      "createdAt": "2025-04-01T20:11:22+00:00",
      "modifiedAt": "2025-04-01T20:11:22+00:00",
      "status": "ACTIVE"
    }
  ]
}
```

2. Usa la acción de la [ListComputeNodeGroups](#) API para enumerar los grupos de nodos de procesamiento de un clúster.

```
aws pcs list-compute-node-groups --cluster-identifier cluster-name-or-id
```

Ejemplo de llamada:

```
aws pcs list-compute-node-groups --cluster-identifier get-started-cfn
```

Ejemplo de salida:

```
{
  "computeNodeGroups": [
```

```

    {
      "name": "compute-1",
      "id": "pcs_abc123abc1",
      "arn": "arn:aws:pcs:us-east-1:111122223333:cluster/pcs_abc1234567/
computenodegroup/pcs_abc123abc1",
      "clusterId": "pcs_abc1234567",
      "createdAt": "2025-04-01T20:19:25+00:00",
      "modifiedAt": "2025-04-01T20:19:25+00:00",
      "status": "ACTIVE"
    },
    {
      "name": "login",
      "id": "pcs_abc456abc7",
      "arn": "arn:aws:pcs:us-east-1:111122223333:cluster/pcs_abc1234567/
computenodegroup/pcs_abc456abc7",
      "clusterId": "pcs_abc1234567",
      "createdAt": "2025-04-01T20:19:31+00:00",
      "modifiedAt": "2025-04-01T20:19:31+00:00",
      "status": "ACTIVE"
    }
  ]
}

```

3. Usa la acción de la [GetComputeNodeGroup](#) API para obtener detalles adicionales de un grupo de nodos de cómputo.

```
aws pcs get-compute-node-group --cluster-identifier cluster-name-or-id --
compute-node-group-identifier compute-node-group-name-or-id
```

Ejemplo de llamada:

```
aws pcs get-compute-node-group --cluster-identifier get-started-cfn --compute-
node-group-identifier compute-1
```

Ejemplo de salida:

```

{
  "computeNodeGroup": {
    "name": "compute-1",
    "id": "pcs_abc123abc1",
    "arn": "arn:aws:pcs:us-east-1:111122223333:cluster/pcs_abc1234567/
computenodegroup/pcs_abc123abc1",

```

```
"clusterId": "pcs_abc1234567",
"createdAt": "2025-04-01T20:19:25+00:00",
"modifiedAt": "2025-04-01T20:19:25+00:00",
"status": "ACTIVE",
"amiId": "ami-0123456789abcdef0",
"subnetIds": [
  "subnet-abc012345789abc12"
],
"purchaseOption": "ONDEMAND",
"customLaunchTemplate": {
  "id": "lt-012345abcdef01234",
  "version": "1"
},
"iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-profile/
AWSPCS-get-started-cfn-us-east-1",
"scalingConfiguration": {
  "minInstanceCount": 0,
  "maxInstanceCount": 4
},
"instanceConfigs": [
  {
    "instanceType": "c6i.xlarge"
  }
]
}
}
```

## Búsqueda de instancias de grupos de nodos de cómputo en AWS PCS

Cada grupo de nodos de cómputo de AWS PCS puede lanzar EC2 instancias con configuraciones compartidas. Puede usar EC2 etiquetas para buscar instancias en un grupo de nodos de cómputo en AWS Management Console o con AWS CLI.

### AWS Management Console

Para encontrar las instancias de tu grupo de nodos de cómputo

1. Abre la [consola AWS PCS](#).
2. Seleccione el clúster.

3. Elija grupos de nodos de cómputo.
4. Busca el ID del grupo de nodos de inicio de sesión que creaste.
5. Navegue hasta la [EC2 consola](#) y elija Instancias.
6. Busque las instancias con la siguiente etiqueta. *node-group-id* Sustitúyala por el ID (no el nombre) de tu grupo de nodos de cómputo.

```
aws:pcs:compute-node-group-id=node-group-id
```

7. (Opcional) Puede cambiar el valor del estado de la instancia en el campo de búsqueda para buscar las instancias que se estén configurando o que se hayan cancelado recientemente.
8. Busca el ID de instancia y la dirección IP de cada instancia en la lista de instancias etiquetadas.

## AWS CLI

Para encontrar las instancias de tu grupo de nodos, usa los siguientes comandos. Antes de ejecutar los comandos, realiza las siguientes sustituciones:

- *region-code* Sustitúyalo por el Región de AWS de su clúster. Ejemplo: us-east-1
- *node-group-id* Sustitúyalo por el ID (no el nombre) de tu grupo de nodos de procesamiento. Para encontrar el ID de un grupo de nodos de cómputo, consulte [Obtenga detalles del grupo de nodos de cómputo en AWS PCS](#).
- *running* Sustitúyalo por otros estados de instancia, como *pending* o *terminated* para buscar EC2 instancias en otros estados.

```
aws ec2 describe-instances \
  --region region-code --filters \
  "Name=tag:aws:pcs:compute-node-group-id,Values=node-group-id" \
  "Name=instance-state-name,Values=running" \
  --query 'Reservations[*].Instances[*]'.
{InstanceID:InstanceId,State:State.Name,PublicIP:PublicIpAddress,PrivateIP:PrivateIpAddress}
```

El comando devuelve un resultado similar al siguiente. El valor de `PublicIP` es `null` si la instancia está en una subred privada.

```
[
  [
```

```
[
  {
    "InstanceID": "i-0123456789abcdefa",
    "State": "running",
    "PublicIP": "18.189.32.188",
    "PrivateIP": "10.0.0.1"
  }
]
```

 Note

Si espera `describe-instances` devolver una gran cantidad de instancias, debe usar las opciones para varias páginas. Para obtener más información, consulte la referencia [DescribeInstances](#) de la API de Amazon Elastic Compute Cloud.

# Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS

En Amazon EC2, una plantilla de lanzamiento puede almacenar un conjunto de preferencias para que no tengas que especificarlas de forma individual al lanzar instancias. AWS El PCS incorpora plantillas de lanzamiento como una forma flexible de configurar grupos de nodos de cómputo. Al crear un grupo de nodos, se proporciona una plantilla de lanzamiento. AWS PCS crea una plantilla de lanzamiento derivada a partir de ella que incluye transformaciones para garantizar que funcione con el servicio.

Entender cuáles son las opciones y las consideraciones a tener en cuenta a la hora de escribir una plantilla de lanzamiento personalizada puede ayudarle a crear una para utilizarla con AWS PCS. Para obtener más información sobre las plantillas de lanzamiento, consulte [Lanzar una instancia desde una plantilla de lanzamiento](#) en la Guía del EC2 usuario de Amazon.

## Temas

- [Descripción general de las plantillas de lanzamiento en AWS PCS](#)
- [Creación de una plantilla de lanzamiento básica](#)
- [Trabajar con datos de EC2 usuario de Amazon para AWS PCS](#)
- [Reservas de capacidad en AWS PCS](#)
- [Parámetros útiles de la plantilla de lanzamiento](#)

## Descripción general de las plantillas de lanzamiento en AWS PCS

Hay [más de 30 parámetros disponibles](#) que puede incluir en una plantilla de EC2 lanzamiento y controlar muchos aspectos de la configuración de las instancias. La mayoría son totalmente compatibles con el AWS PCS, pero hay algunas excepciones.

El AWS PCS ignorará los siguientes parámetros de la plantilla de EC2 lanzamiento, ya que el servicio debe administrar directamente estas propiedades:

- Tipo de instancia/especifique los atributos del tipo de instancia (InstanceRequirements): AWS PCS no admite la selección de instancias basada en atributos.
- Tipo de instancia (InstanceType): especifique los tipos de instancias al crear un grupo de nodos.

- Detalles avanzados/perfil de instancia de IAM (IamInstanceProfile): los proporcionas al crear o actualizar el grupo de nodos.
- Detalles avanzados/Desactivar la terminación de la API (DisableApiTermination): AWS PCS debe controlar el ciclo de vida de las instancias del grupo de nodos que lanza.
- Detalles avanzados/Desactivar la parada de la API (DisableApiStop): AWS PCS debe controlar el ciclo de vida de las instancias de grupos de nodos que lanza.
- Detalles avanzados/Comportamiento de parada e hibernación (HibernationOptions): AWS PCS no admite la hibernación de instancias.
- Detalles avanzados/Elastic GPU (ElasticGpuSpecifications): Amazon Elastic Graphics finalizó su vida útil el 8 de enero de 2024.
- Detalles avanzados/Inferencia elástica (ElasticInferenceAccelerators): Amazon Elastic Inference ya no está disponible para clientes nuevos.
- AAdvanced details/Specify CPU options/Threadsper core (ThreadsPerCore): AWS PCS establece el número de hilos por núcleo en 1.

Estos parámetros tienen requisitos especiales que respaldan la compatibilidad con el AWS PCS:

- Datos de usuario (UserData): deben estar codificados en varias partes. Consulte [Trabajar con datos de EC2 usuario de Amazon para AWS PCS](#).
- Imágenes de la aplicación y del sistema operativo (ImageId): puede incluirlas. Sin embargo, si especifica un ID de AMI al crear o actualizar el grupo de nodos, este anulará el valor de la plantilla de lanzamiento. La AMI que proporcione debe ser compatible con AWS PCS. Para obtener más información, consulte "[Amazon Machine Images \(AMIs\) para AWS PCS](#)".
- Configuración de red/Firewall (grupos de seguridad) (**SecurityGroups**): no se puede configurar una lista de nombres de grupos de seguridad en una plantilla de lanzamiento de AWS PCS. Puede configurar una lista de grupos de seguridad IDs (SecurityGroupIds), a menos que defina las interfaces de red en la plantilla de lanzamiento. A continuación, debe especificar el grupo de seguridad IDs para cada interfaz. Para obtener más información, consulte [Grupos de seguridad en AWS PCS](#).
- Configuración de red/Configuración de red avanzada (NetworkInterfaces): si utiliza EC2 instancias con una sola tarjeta de red y no necesita ninguna configuración de red especializada, AWS PCS puede configurar la red de instancias por usted. Para configurar varias tarjetas de red o habilitar el adaptador Elastic Fabric en sus instancias, utilice NetworkInterfaces Cada interfaz de red debe tener una lista de grupos de seguridad IDs debajoGroups. Para obtener más información, consulte [Múltiples interfaces de red en AWS PCS](#).

- Detalles avanzados/reserva de capacidad (CapacityReservationSpecification): se puede configurar, pero no puede hacer referencia a un dato específico CapacityReservationId cuando se trabaja con AWS PCS. Sin embargo, puede hacer referencia a un grupo de reservas de capacidad, si ese grupo contiene una o más reservas de capacidad. Para obtener más información, consulte [Reservas de capacidad en AWS PCS](#).

## Creación de una plantilla de lanzamiento básica

Puede crear una plantilla de lanzamiento mediante el AWS Management Console o el AWS CLI.

### AWS Management Console

Para crear una plantilla de lanzamiento

1. Abre la [EC2consola de Amazon](#) y selecciona Launch templates.
2. Elija Crear plantilla de inicialización.
3. En Nombre y descripción de la plantilla de lanzamiento, introduce un nombre único y distintivo para el nombre de la plantilla de lanzamiento
4. En Par de claves (inicio de sesión) en Nombre del par de claves, seleccione el par de claves SSH que se usará para iniciar sesión en EC2 las instancias administradas por AWS PCS. Esto es opcional, pero recomendable.
5. En Configuración de red y, a continuación, en Firewall (grupos de seguridad), elija los grupos de seguridad que desee conectar a la interfaz de red. Todos los grupos de seguridad de la plantilla de lanzamiento deben pertenecer a la VPC del clúster de AWS PCS. Como mínimo, elija:
  - Un grupo de seguridad que permite la comunicación con el clúster de AWS PCS
  - Un grupo de seguridad que permite la comunicación entre EC2 instancias lanzadas por AWS PCS
  - (Opcional) Un grupo de seguridad que permite el acceso SSH entrante a instancias interactivas
  - (Opcional) Un grupo de seguridad que permite a los nodos de cómputo establecer conexiones salientes a Internet
  - (Opcional) Grupos de seguridad que permiten el acceso a los recursos de la red, como los sistemas de archivos compartidos o un servidor de bases de datos.

6. Podrás acceder a tu nueva ID de plantilla de lanzamiento en la EC2 consola de Amazon, en Plantillas de lanzamiento. El identificador de la plantilla de lanzamiento incluirá el formulario1t-0123456789abcdef01.

### Siguiente paso recomendado

- Utilice la nueva plantilla de lanzamiento para crear o actualizar un grupo de nodos de cómputo de AWS PCS.

## AWS CLI

### Para crear una plantilla de lanzamiento

Cree su plantilla de lanzamiento con el siguiente comando.

- Antes de ejecutar el comando, realice los siguientes reemplazos:
  - a. *region-code* Sustitúyala por la Región de AWS que estás trabajando con AWS PCS
  - b. *my-launch-template-name* Sustitúyala por un nombre para la plantilla. Debe ser exclusivo del Cuenta de AWS y Región de AWS que está utilizando.
  - c. *my-ssh-key-name* Sustitúyala por el nombre de tu clave SSH preferida.
  - d. Reemplace *sg-ExampleID1* y *sg-ExampleID2* por un grupo de seguridad IDs que permita la comunicación entre sus EC2 instancias y el programador y la comunicación entre EC2 instancias. Si solo tiene un grupo de seguridad que permite todo este tráfico, puede eliminarlo *sg-ExampleID2* y el carácter de coma que lo precede. También puede añadir más grupos IDs de seguridad. Todos los grupos de seguridad que incluya en la plantilla de lanzamiento deben provenir de la VPC de su clúster de AWS PCS.

```
aws ec2 create-launch-template --region region-code \  
  --launch-template-name my-template-name \  
  --launch-template-data '{"KeyName":"my-ssh-key-name","SecurityGroupIds":  
  ["sg-ExampleID1","sg-ExampleID2"]}'
```

El resultado AWS CLI será un texto parecido al siguiente. El identificador de la plantilla de lanzamiento se encuentra en `LaunchTemplateId`.

```
{
  "LaunchTemplate": {
    "LatestVersionNumber": 1,
    "LaunchTemplateId": "lt-0123456789abcdef01",
    "LaunchTemplateName": "my-launch-template-name",
    "DefaultVersionNumber": 1,
    "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
    "CreateTime": "2019-04-30T18:16:06.000Z"
  }
}
```

### Siguiente paso recomendado

- Utilice la nueva plantilla de lanzamiento para crear o actualizar un grupo de nodos de cómputo de AWS PCS.

## Trabajar con datos de EC2 usuario de Amazon para AWS PCS

Puede proporcionar datos de EC2 usuario en la plantilla de lanzamiento que `cloud-init` se ejecuta cuando se lanzan las instancias. Los bloques de datos de usuario con ese tipo de contenido se `cloud-config` ejecutan antes de que la instancia se registre en la API de AWS PCS, mientras que los bloques de datos de usuario con ese tipo de contenido se `text/x-shellscript` ejecutan una vez finalizado el registro, pero antes de que se inicie el daemon de Slurm. Para obtener más información sobre los tipos de contenido, consulte la [documentación de cloud-init](#).

nuestros datos de usuario pueden realizar escenarios de configuración comunes, incluidos, entre otros, los siguientes:

- [Incluidos usuarios o grupos](#)
- [Instalación de paquetes](#)
- [Creación de particiones y sistemas de archivos](#)
- Montaje de sistemas de archivos de red

Los datos de usuario de las plantillas de lanzamiento deben estar en formato de [archivo MIME de varias partes](#). Esto se debe a que sus datos de usuario se combinan con otros datos de usuario de AWS PCS necesarios para configurar los nodos de su grupo de nodos. Puede combinar varios bloques de datos de usuario en un único archivo multiparte MIME.

Un archivo multiparte MIME consta de los siguientes componentes:

- El tipo de contenido y declaración de límite de partes: `Content-Type: multipart/mixed; boundary="==BOUNDARY=="`
- La declaración de versión de MIME: `MIME-Version: 1.0`
- Uno o más bloques de datos de usuario, que contienen los siguientes componentes:
  - El límite de apertura, que señala el inicio de un bloque de datos de usuario: `--==BOUNDARY==`. Debe dejar en blanco la línea anterior a este límite.
  - La declaración del tipo de contenido del bloque: `Content-Type: text/cloud-config; charset="us-ascii"` o `Content-Type: text/x-shellscript; charset="us-ascii"`. Debe dejar en blanco la línea que sigue a la declaración de tipo de contenido.
  - El contenido de los datos de usuario, por ejemplo, una lista de intérprete de comandos o políticas de `cloud-config`.
- El límite de cierre, que señala el final del archivo multiparte MIME: `--==BOUNDARY==--`. Debe dejar en blanco la línea anterior al límite de cierre.

#### Note

Si añades datos de usuario a una plantilla de lanzamiento en la EC2 consola de Amazon, puedes pegarlos como texto sin formato. O bien, puede cargarlos desde un archivo. Si utilizas el SDK AWS CLI o un AWS SDK, primero debes codificar en base64 los datos del usuario y enviar esa cadena como el valor del `UserData` parámetro cuando llames [CreateLaunchTemplate](#), tal y como se muestra en este archivo JSON.

```
{
  "LaunchTemplateName": "base64-user-data",
  "LaunchTemplateData": {
    "UserData":
"ewogICAgIkxhdW5jaFR1bXBsYXR1TmFtZSI6ICJpbmNyZWZzZS1jb250YWluZXItZm9sdW..."
  }
}
```

## Ejemplos

- [Ejemplo: instalar software desde un repositorio de paquetes](#)

- [Ejemplo: ejecutar scripts desde un bucket de S3](#)
- [Ejemplo: establecer variables de entorno globales](#)
- [Uso de sistemas de archivos de red con AWS PCS](#)
- [Ejemplo: utilizar un sistema de archivos EFS como directorio principal compartido](#)

## Ejemplo: instalar software para AWS PCS desde un repositorio de paquetes

Proporcione este script como el valor de "userData" en su plantilla de lanzamiento. Para obtener más información, consulte [Trabajar con datos de EC2 usuario de Amazon para AWS PCS](#).

Este script usa cloud-config para instalar paquetes de software en instancias de grupos de nodos en el momento del lanzamiento. Para obtener más información, consulta los [formatos de datos de usuario](#) en la documentación de cloud-init. En este ejemplo, se instala curl y llvm

### Note

Sus instancias deben poder conectarse a sus repositorios de paquetes configurados.

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=="MYBOUNDARY=="

--MYBOUNDARY--
Content-Type: text/cloud-config; charset="us-ascii"

packages:
- python3-devel
- rust
- golang

--MYBOUNDARY--
```

## Ejemplo: ejecutar scripts adicionales para AWS PCS desde un bucket de S3

Proporcione este script como el valor de "userData" en su plantilla de lanzamiento. Para obtener más información, consulte [Trabajar con datos de EC2 usuario de Amazon para AWS PCS](#).

El siguiente script de datos de usuario usa cloud-config para importar un script de un bucket de S3 y ejecutarlo en instancias de grupos de nodos en el momento del lanzamiento. Para obtener más información, consulta los [formatos de datos de usuario](#) en la documentación de cloud-init.

Sustituya los siguientes valores por sus propios detalles:

- *amzn-s3-demo-bucket*— El nombre de un bucket de S3 desde el que puede leer tu cuenta.
- *object-key*— La clave de objeto S3 del script que se va a importar. Incluye el nombre del script y su ubicación en la estructura de carpetas del depósito. Por ejemplo, `scripts/script.sh`. Para obtener más información, consulte [Organizar objetos en la consola de Amazon S3 mediante carpetas](#) en la Guía del usuario de Amazon Simple Storage Service.
- *shell*— El shell de Linux que se utilizará para ejecutar el script, por ejemplo `bash`.

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=="MYBOUNDARY=="

--MYBOUNDARY==
Content-Type: text/cloud-config; charset="us-ascii"

runcmd:
- aws s3 cp s3://amzn-s3-demo-bucket/object-key /tmp/script.sh
- /usr/bin/shell /tmp/script.sh

--MYBOUNDARY==
```

El perfil de instancia de IAM del grupo de nodos debe tener acceso al bucket. La siguiente política de IAM es un ejemplo del depósito del script de datos de usuario anterior.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}
```

```

    ]
  }
]
}

```

## Ejemplo: establecer variables de entorno globales para AWS PCS

Proporcione este script como el valor de "userData" en su plantilla de lanzamiento. Para obtener más información, consulte [Trabajar con datos de EC2 usuario de Amazon para AWS PCS](#).

El siguiente ejemplo se utiliza /etc/profile.d para establecer variables globales en instancias de grupos de nodos.

```

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="==MYBOUNDARY=="

--==MYBOUNDARY==
Content-Type: text/x-shellscript; charset="us-ascii"

#!/bin/bash
touch /etc/profile.d/awspcs-userdata-vars.sh
echo MY_GLOBAL_VAR1=100 >> /etc/profile.d/awspcs-userdata-vars.sh
echo MY_GLOBAL_VAR2=abc >> /etc/profile.d/awspcs-userdata-vars.sh

--==MYBOUNDARY==--

```

## Ejemplo: utilizar un sistema de archivos EFS como directorio principal compartido para AWS PCS

Proporcione este script como valor de "userData" en su plantilla de lanzamiento. Para obtener más información, consulte [Trabajar con datos de EC2 usuario de Amazon para AWS PCS](#).

Este ejemplo amplía el ejemplo de montaje de EFS [Uso de sistemas de archivos de red con AWS PCS](#) para implementar un directorio principal compartido. Se hace una copia de seguridad del contenido de /home antes de montar el sistema de archivos EFS. A continuación, el contenido se copia rápidamente en su lugar en el almacenamiento compartido una vez finalizado el montaje.

Sustituya los siguientes valores de este script por sus propios detalles:

- */mount-point-directory*— La ruta de una instancia en la que desea montar el sistema de archivos EFS.

- *filesystem-id*— El ID del sistema de archivos del sistema de archivos EFS.

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="==MYBOUNDARY=="

--==MYBOUNDARY==
Content-Type: text/cloud-config; charset="us-ascii"

packages:
  - amazon-efs-utils

runcmd:
  - mkdir -p /tmp/home
  - rsync -a /home/ /tmp/home
  - echo "filesystem-id:/ mount-point-directory efs tls,_netdev" >> /etc/fstab
  - mount -a -t efs defaults
  - rsync -a --ignore-existing /tmp/home/ /home
  - rm -rf /tmp/home/

--==MYBOUNDARY==--
```

## Ejemplo: habilitar SSH sin contraseña

Puedes basarte en el ejemplo del directorio principal compartido para implementar conexiones SSH entre instancias del clúster mediante claves SSH. Para cada usuario que utilice el sistema de archivos de inicio compartido, ejecute un script similar al siguiente:

```
#!/bin/bash

mkdir -p $HOME/.ssh && chmod 700 $HOME/.ssh
touch $HOME/.ssh/authorized_keys
chmod 600 $HOME/.ssh/authorized_keys

if [ ! -f "$HOME/.ssh/id_rsa" ]; then
  ssh-keygen -t rsa -b 4096 -f $HOME/.ssh/id_rsa -N ""
  cat ~/.ssh/id_rsa.pub >> $HOME/.ssh/authorized_keys
fi
```

**Note**

Las instancias deben usar un grupo de seguridad que permita las conexiones SSH entre los nodos del clúster.

## Reservas de capacidad en AWS PCS

Puedes reservar la EC2 capacidad de Amazon en una zona de disponibilidad específica y durante un período específico mediante reservas de capacidad bajo demanda o bloques de EC2 capacidad para asegurarte de que tienes la capacidad informática necesaria disponible cuando la necesites.

**Note**

AWS PCS admite las reservas de capacidad bajo demanda (ODCR), pero actualmente no admite bloques de capacidad para el aprendizaje automático.

## Se utiliza ODCRs con PCS AWS

Puede elegir la forma en que AWS PCS consume sus instancias reservadas. Si crea una ODCR abierta, cualquier instancia coincidente lanzada por AWS PCS u otros procesos de su cuenta se descontará de la reserva. Con una ODCR segmentada, solo las instancias lanzadas con el identificador de reserva específico se tienen en cuenta para la reserva. En el caso de las cargas de trabajo urgentes, las segmentadas ODCRs son más habituales.

Puede configurar un grupo de nodos de cómputo de AWS PCS para que utilice un ODCR de destino agregándolo a una plantilla de lanzamiento. Estos son los pasos para hacerlo:

1. Cree una reserva de capacidad a pedido (ODCR) específica.
2. Agregue la ODCR a un grupo de reserva de capacidad.
3. Asocie el grupo de reserva de capacidad a una plantilla de lanzamiento.
4. Cree o actualice un grupo de nodos de cómputo de AWS PCS para usar la plantilla de lanzamiento.

## Ejemplo: reserve y utilice instancias hpc6a.48xlarge con un ODCR de destino

Este comando de ejemplo crea un ODCR de destino para 32 instancias de hpc6a.48xlarge. Para lanzar las instancias reservadas en un grupo de ubicación, agréguelas al comando. `--placement-group-arn` Puede definir una fecha de finalización con `--end-date` y `--end-date-type`, de lo contrario, la reserva continuará hasta que se finalice manualmente.

```
aws ec2 create-capacity-reservation \  
  --instance-type hpc6a.48xlarge \  
  --instance-platform Linux/UNIX \  
  --availability-zone us-east-2a \  
  --instance-count 32 \  
  --instance-match-criteria targeted
```

El resultado de este comando será un ARN para el nuevo ODCR. Para usar el ODCR con el AWS PCS, debe agregarse a un grupo de reserva de capacidad. Esto se debe a que AWS PCS no admite personas. ODCRs Para obtener más información, consulte [Grupos de reserva de capacidad](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

A continuación, se explica cómo añadir el ODCR a un grupo de reserva de capacidad denominado `EXAMPLE-CR-GROUP`.

```
aws resource-groups group-resources --group EXAMPLE-CR-GROUP \  
  --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/  
cr-1234567890abcdef1
```

Con el ODCR creado y agregado a un grupo de reserva de capacidad, ahora se puede conectar a un grupo de nodos de cómputo del AWS PCS agregándolo a una plantilla de lanzamiento. A continuación, se muestra un ejemplo de plantilla de lanzamiento que hace referencia al grupo de reserva de capacidad.

```
{  
  "CapacityReservationSpecification": {  
    "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-  
east-2:123456789012:group/EXAMPLE-CR-GROUP"  
  }  
}
```

Por último, cree o actualice un grupo de nodos de cómputo de AWS PCS para usar instancias hpc6a.48xlarge y use la plantilla de lanzamiento que hace referencia al ODCR en su grupo de

reserva de capacidad. Para un grupo de nodos estático, defina las instancias mínimas y máximas según el tamaño de la reserva (32). Para un grupo de nodos dinámico, establece el número mínimo de instancias en 0 y el máximo en el tamaño de la reserva.

Este ejemplo es una implementación simple de un ODCR único que se aprovisiona para un grupo de nodos de cómputo. Sin embargo, AWS PCS admite muchos otros diseños. Por ejemplo, puede subdividir un grupo grande de ODCR o de reserva de capacidad entre varios grupos de nodos de cómputo. O bien, puede usar la ODCRs que otra cuenta de AWS haya creado y compartido con la suya. La principal limitación es que ODCRs siempre debe estar incluida en un grupo de reserva de capacidad.

Para obtener más información, consulte [Reservas de capacidad bajo demanda y bloques de capacidad para aprendizaje automático](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

## Parámetros útiles de la plantilla de lanzamiento

En esta sección se describen algunos parámetros de la plantilla de lanzamiento que pueden resultar muy útiles con el AWS PCS.

### Active la CloudWatch supervisión detallada

Puede habilitar la recopilación de CloudWatch métricas en un intervalo más corto mediante un parámetro de plantilla de lanzamiento.

#### AWS Management Console

En las páginas de la consola para crear o editar plantillas de lanzamiento, esta opción se encuentra en la sección de detalles avanzados. Configure la CloudWatch supervisión detallada en Activar.

#### YAML

```
Monitoring:
  Enabled: True
```

#### JSON

```
{"Monitoring": {"Enabled": "True"}}
```

Para obtener más información, consulte [Habilitar o desactivar la supervisión detallada de sus instancias](#) en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

## Instance Metadata Service, versión 2 (IMDS v2)

El uso del IMDS v2 con EC2 las instancias ofrece importantes mejoras de seguridad y ayuda a mitigar los posibles riesgos asociados al acceso a los metadatos de las instancias en AWS los entornos.

### AWS Management Console

En las páginas de la consola para crear o editar plantillas de lanzamiento, esta opción se encuentra en la sección de detalles avanzados. Configura los metadatos accesibles en Habilitados, la versión de metadatos en V2 únicamente (se requiere un token) y el límite de saltos de respuesta de los metadatos en 4.

### YAML

```
MetadataOptions:
  HttpEndpoint: enabled
  HttpTokens: required
  HttpPutResponseHopLimit: 4
```

### JSON

```
{
  "MetadataOptions": {
    "HttpEndpoint": "enabled",
    "HttpPutResponseHopLimit": 4,
    "HttpTokens": "required"
  }
}
```

# AWS Colas PCS

Una cola de AWS PCS es una abstracción ligera de la implementación nativa de una cola de trabajos por parte del programador. En el caso de Slurm, una cola AWS PCS equivale a una partición Slurm.

Los usuarios envían los trabajos a una cola en la que residen hasta que puedan programarse para que se ejecuten en los nodos proporcionados por uno o más grupos de nodos de procesamiento. Un clúster de AWS PCS puede tener varias colas de trabajos. Por ejemplo, puede crear una cola que utilice Amazon EC2 On-Demand Instances para los trabajos de alta prioridad y otra cola que utilice Amazon EC2 Spot Instances para los trabajos de baja prioridad.

## Temas

- [Creación de una cola en PCS AWS](#)
- [Actualización de una cola de AWS PCS](#)
- [Eliminar una cola en PCS AWS](#)

## Creación de una cola en PCS AWS

En este tema se proporciona una visión general de las opciones disponibles y se describe lo que se debe tener en cuenta al crear una cola en AWS PCS.

## Requisitos previos

- Un clúster de AWS PCS: las colas solo se pueden crear en asociación con un clúster de AWS PCS específico.
- Uno o más grupos de nodos de cómputo de AWS PCS: una cola debe estar asociada a al menos un grupo de nodos de cómputo de AWS PCS.

## Para crear una cola en PCS AWS

Puede crear una cola utilizando el AWS Management Console o el AWS CLI

### AWS Management Console

Para crear una cola mediante la consola

1. Abra la [consola AWS PCS](#).

2. Seleccione el clúster para la cola. Navegue hasta Colas y elija Crear cola.
3. En la sección de configuración de colas, proporciona los siguientes valores:
  - a. Nombre de la cola: un nombre para la cola. El nombre solo puede contener caracteres alfanuméricos (con distinción de mayúsculas y minúsculas) y guiones. Debe empezar por un carácter alfabético y no puede tener más de 25 caracteres. El nombre debe ser único en el clúster.
  - b. Grupos de nodos de cómputo: seleccione uno o más grupos de nodos de cómputo para dar servicio a esta cola. Un grupo de nodos de cómputo se puede asociar a más de una cola.
4. (Opcional) En Etiquetas, añada cualquier etiqueta a la cola de AWS PCS
5. Elige Crear cola. El campo Estado mostrará la opción Crear mientras AWS PCS crea la cola. La creación de la cola puede tardar varios minutos.

#### Siguiente paso recomendado

- Envía un trabajo a tu nueva lista.

## AWS CLI

Para crear una cola mediante AWS CLI

Utilice el siguiente comando para crear la cola. Realice las siguientes sustituciones:

1. Reemplace *region-code* por la AWS región del clúster. Por ejemplo, `us-east-1`.
2. *my-queue* Sustitúyalo por el nombre de la cola. El nombre solo puede contener caracteres alfanuméricos (con distinción de mayúsculas y minúsculas) y guiones. Debe empezar por un carácter alfabético y no puede tener más de 25 caracteres. El nombre debe ser único en el clúster.
3. *my-cluster* Sustitúyalo por el nombre o el ID del clúster.
4. *compute-node-group-id* Sustitúyalo por el ID del grupo de nodos de procesamiento para dar servicio a la cola. Por ejemplo, `pcs_abcdef12345`.

**Note**

Al crear una cola, debe proporcionar el ID del grupo de nodos de procesamiento y no su nombre.

```
aws pcs create-queue --region region-code \  
  --queue-name my-queue \  
  --cluster-identifier my-cluster \  
  --compute-node-group-configurations \  
  computeNodeGroupId=compute-node-group-id
```

La creación de la cola puede tardar varios minutos. Puede consultar el estado de la cola con el siguiente comando. No podrá enviar trabajos a la cola hasta que alcance su estado. ACTIVE

```
aws pcs get-queue --region region-code \  
  --cluster-identifier my-cluster \  
  --queue-identifier my-queue
```

Siguiente paso recomendado

- Envía un trabajo a tu nueva lista

## Actualización de una cola de AWS PCS

En este tema se proporciona una visión general de las opciones disponibles y se describe lo que se debe tener en cuenta al actualizar una cola de AWS PCS.

### Consideraciones a la hora de actualizar una cola de AWS PCS

Las actualizaciones de las colas no afectarán a los trabajos en ejecución, pero es posible que el clúster no pueda aceptar nuevos trabajos mientras se actualiza la cola.

### Para actualizar una cola de PCS AWS

Puede usar AWS Management Console o AWS CLI para actualizar una cola.

## AWS Management Console

Para actualizar una cola

1. Abra la consola AWS PCS en <https://console.aws.amazon.com/pcs/home#/clusters>
2. Seleccione el clúster en el que desee actualizar una cola.
3. Ve a Colas, ve a la cola que deseas actualizar y, a continuación, selecciona Editar.
4. En la sección de configuración de colas, actualiza cualquiera de los siguientes valores:
  - Grupos de nodos: agregue o elimine grupos de nodos de cómputo de la asociación con la cola.
  - Etiquetas: añada o elimine etiquetas para la cola.
5. Elija Actualizar. El campo Estado mostrará la actualización mientras se aplican los cambios.

 Important

Las actualizaciones de las colas pueden tardar varios minutos.

## AWS CLI

Para actualizar una cola

1. Actualice la cola con el siguiente comando. Antes de ejecutar el comando, realice los siguientes reemplazos:
  - a. *region-code* Sustitúyala por la Región de AWS que deseas crear tu clúster.
  - b. *my-queue* Sustitúyalo por el nombre o `computeNodeGroupId` por el de tu cola.
  - c. *my-cluster* Sustitúyalo por el nombre o `clusterId` el de tu clúster.
  - d. Para cambiar las asociaciones de grupos de nodos de cómputo, proporciona una lista actualizada de `--compute-node-group-configurations`.
    - Por ejemplo, para añadir un segundo grupo de nodos de cómputo `computeNodeGroupExampleID2`:

```
--compute-node-group-configurations
computeNodeId=computeNodeGroupExampleID1, computeNodeId=computeNodeGro
```

```
aws pcs update-queue --region region-code \
  --queue-identifier my-queue \
  --cluster-identifier my-cluster \
  --compute-node-group-configurations \
  computeNodeId=computeNodeGroupExampleID1
```

2. La actualización de la cola puede tardar varios minutos. Puede consultar el estado de la cola con el siguiente comando. No podrá enviar trabajos a la cola hasta que alcance su estado. ACTIVE

```
aws pcs get-queue --region region-code \
  --cluster-identifier my-cluster \
  --queue-identifier my-queue
```

### Próximos pasos recomendados

- Envía un trabajo a tu lista de espera actualizada.

## Eliminar una cola en PCS AWS

En este tema se proporciona una descripción general de cómo eliminar una cola en AWS PCS.

### Consideraciones a la hora de eliminar una cola

- Si hay trabajos en ejecución en la cola, el programador los finalizará cuando se elimine la cola. Los trabajos pendientes de la cola se cancelarán. Considere la posibilidad de esperar a que terminen los trabajos de la cola o detenerlos o cancelarlos manualmente mediante los comandos nativos del programador (como los de Slurm). `scancel`

### Eliminación de la cola

Puede usar o para eliminar una cola. AWS Management Console AWS CLI

## AWS Management Console

Para eliminar una cola

1. Abra la [consola AWS PCS](#).
2. Seleccione el grupo de la cola.
3. Navegue hasta Colas y seleccione la cola que desee eliminar.
4. Elija Eliminar.
5. Aparece el campo Estado. Deleting Puede tardar varios minutos en completarse.

### Note

Puede usar los comandos nativos de su programador para confirmar que la cola se ha eliminado. Por ejemplo, usa `sinfo` o `squeue` para Slurm.

## AWS CLI

Para eliminar una cola

- Utilice el siguiente comando para eliminar una cola, con estas sustituciones:
  - *region-code* Sustitúyala por la que se encuentra Región de AWS tu clúster.
  - *my-queue* Sustitúyalo por el nombre o el ID de la cola.
  - *my-cluster* Sustitúyalo por el nombre o el ID de tu clúster.

```
aws pcs delete-queue --region region-code \  
  --queue-identifier my-queue \  
  --cluster-identifier my-cluster
```

Eliminar la cola puede tardar varios minutos.

### Note

Puede usar los comandos nativos de su programador para confirmar que la cola se ha eliminado. Por ejemplo, usa `sinfo` o `squeue` para Slurm.

# AWS nodos de inicio de sesión PCS

Por lo general, un clúster de AWS PCS necesita al menos un nodo de inicio de sesión para admitir el acceso interactivo y la administración de tareas. Una forma de lograrlo es con un grupo de nodos de cómputo AWS PCS estáticos configurado para funcionar con nodos de inicio de sesión. También puede configurar una EC2 instancia independiente para que actúe como nodo de inicio de sesión.

## Temas

- [Uso de un grupo de nodos de cómputo de AWS PCS para proporcionar nodos de inicio de sesión](#)
- [Uso de instancias independientes como nodos de inicio de sesión de AWS PCS](#)

## Uso de un grupo de nodos de cómputo de AWS PCS para proporcionar nodos de inicio de sesión

En este tema se proporciona una descripción general de las opciones de configuración sugeridas y se describe qué se debe tener en cuenta al utilizar un grupo de nodos de cómputo de AWS PCS para proporcionar un acceso persistente e interactivo a su clúster.

## Crear un grupo de nodos de cómputo de AWS PCS para los nodos de inicio de sesión

Desde el punto de vista operativo, esto no es muy diferente de crear un grupo de nodos de cómputo normal. Sin embargo, hay que tomar algunas decisiones de configuración clave:

- Establezca una configuración de escalado estático de al menos una EC2 instancia del grupo de nodos de procesamiento.
- Elija la opción de compra bajo demanda para evitar que se recuperen sus instancias.
- Elija un nombre informativo para el grupo de nodos de cómputo, como el inicio de sesión.
- Si desea que se pueda acceder a las instancias del nodo de inicio de sesión desde fuera de su VPC, considere la posibilidad de utilizar una subred pública.
- Si pretende permitir el acceso a SSH, la plantilla de lanzamiento necesitará tener un grupo de seguridad que exponga el puerto SSH a las direcciones IP que elija.

- El perfil de instancia de IAM debe tener solo los permisos de AWS que desee que tengan sus usuarios finales. Para obtener más información, consulte [Perfiles de instancia de IAM para AWS Parallel Computing Service](#).
- Considere la posibilidad de permitir que AWS Systems Manager Session Manager administre sus instancias de inicio de sesión.
- Considere restringir el acceso a las credenciales de AWS de la instancia solo a los usuarios administrativos
- Seleccione tipos de instancias menos costosos que los de los grupos de nodos de cómputo normales, ya que los nodos de inicio de sesión se ejecutarán de forma continua.
- Use la misma AMI (o una derivada) que para sus otros grupos de nodos de cómputo para garantizar que todas las instancias tengan instalado el mismo software. Para obtener más información sobre la personalización AMIs, consulte [Amazon Machine Images \(AMIs\) para AWS PCS](#)
- Configure el mismo sistema de archivos de red (Amazon EFS, Amazon FSx for Lustre, etc.) para montarlo en los nodos de inicio de sesión que en las instancias informáticas. Para obtener más información, consulte [Uso de sistemas de archivos de red con AWS PCS](#).

Acceda a sus nodos de inicio de sesión

Cuando su nuevo grupo de nodos de cómputo alcance el estado ACTIVO, podrá encontrar las EC2 instancias que ha creado e iniciar sesión en ellas. Para obtener más información, consulte [Búsqueda de instancias de grupos de nodos de cómputo en AWS PCS](#).

## Actualización de un grupo de nodos de procesamiento de AWS PCS para los nodos de inicio de sesión

Puede actualizar un grupo de nodos de inicio de sesión mediante UpdateComputeNodeGroup. Como parte del proceso de actualización del grupo de nodos, se sustituirán las instancias en ejecución. Ten en cuenta que esto interrumpirá cualquier sesión de usuario o proceso activo en la instancia. Los trabajos de Slurm en ejecución o en cola no se verán afectados. Para obtener más información, consulte [Actualización de un grupo de nodos de cómputo AWS PCS](#).

También puede editar la plantilla de lanzamiento utilizada por su grupo de nodos de cómputo. Debe utilizarla UpdateComputeNodeGroup para aplicar la plantilla de lanzamiento actualizada al grupo de nodos de procesamiento. EC2 Las nuevas instancias lanzadas en el grupo de nodos

de procesamiento utilizan la plantilla de lanzamiento actualizada. Para obtener más información, consulte [Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS](#).

## Eliminar un grupo de nodos de cómputo de AWS PCS para los nodos de inicio de sesión

Puede actualizar un grupo de nodos de inicio de sesión mediante el mecanismo de eliminación del grupo de nodos de cálculo de AWS PCS. Las instancias en ejecución se cancelarán como parte de la eliminación del grupo de nodos. Ten en cuenta que esto interrumpirá cualquier sesión de usuario o proceso activo en la instancia. Los trabajos de Slurm en ejecución o en cola no se verán afectados. Para obtener más información, consulte [Eliminar un grupo de nodos de cómputo en AWS PCS](#).

## Uso de instancias independientes como nodos de inicio de sesión de AWS PCS

Puede configurar EC2 instancias independientes para que interactúen con el programador Slurm de un clúster de AWS PCS. Esto resulta útil para crear nodos de inicio de sesión, estaciones de trabajo o hosts de administración de flujos de trabajo dedicados que funcionen con clústeres de PCS pero que operen fuera de la administración de AWS PCS. Para ello, cada instancia independiente debe:

1. Tener instalada una versión de software Slurm compatible.
2. Podrá conectarse al punto final Slurmctld del clúster AWS PCS.
3. Configure correctamente el Slurm Auth and Cred Kiosk Daemon (sackd) con el punto final y el secreto del clúster de PCS. Para obtener más información, consulte [sackd en la documentación de Slurm](#).

Este tutorial le ayuda a configurar una instancia independiente que se conecta a un clúster de PCS.  
AWS

### Contenido

- [Paso 1: Recupere la dirección y el secreto del clúster de AWS PCS de destino](#)
- [Paso 2: lanzar una EC2 instancia](#)
- [Paso 3: Instala Slurm en la instancia](#)
- [Paso 4: Recupere y almacene el secreto del clúster](#)

- [Paso 5: Configurar la conexión al clúster de PCS AWS](#)
- [Paso 6: \(opcional\) Pruebe la conexión](#)

## Paso 1: Recupere la dirección y el secreto del clúster de AWS PCS de destino

Recupere los detalles sobre el clúster AWS PCS AWS CLI de destino mediante el comando siguiente. Antes de ejecutar el comando, realice los siguientes reemplazos:

- *region-code* Sustitúyalo por el Región de AWS lugar en el que se ejecuta el clúster de destino.
- *cluster-ident* Sustitúyalo por el nombre o identificador del clúster de destino

```
aws pcs get-cluster --region region-code --cluster-identifier cluster-ident
```

El comando devolverá un resultado similar al de este ejemplo.

```
{
  "cluster": {
    "name": "get-started",
    "id": "pcs_123456abcd",
    "arn": "arn:aws:pcs:us-east-1:111122223333:cluster/pcs_123456abcd",
    "status": "ACTIVE",
    "createdAt": "2024-12-17T21:03:52+00:00",
    "modifiedAt": "2024-12-17T21:03:52+00:00",
    "scheduler": {
      "type": "SLURM",
      "version": "24.05"
    },
    "size": "SMALL",
    "slurmConfiguration": {
      "authKey": {
        "secretArn": "arn:aws:secretsmanager:us-east-1:111122223333:secret:pcs!slurm-secret-pcs_123456abcd-a12ABC",
        "secretVersion": "ef232370-d3e7-434c-9a87-ec35c1987f75"
      }
    },
    "networking": {
      "subnetIds": [
        "subnet-0123456789abcdef0"
      ]
    }
  }
}
```

```
    ],
    "securityGroupIds": [
      "sg-0123456789abcdef0"
    ]
  },
  "endpoints": [
    {
      "type": "SLURMCTLD",
      "privateIpAddress": "10.3.149.220",
      "port": "6817"
    }
  ]
}
```

En este ejemplo, el punto final del controlador Slurm del clúster tiene una dirección IP de 10.3.149.220 y se ejecuta en el puerto. 6817 Se `secretArn` usará en pasos posteriores para recuperar el secreto del clúster. La dirección IP y el puerto se utilizarán en pasos posteriores para configurar el `sackd` servicio.

## Paso 2: lanzar una EC2 instancia

Para lanzar una EC2 instancia

1. Abra la [EC2 consola de Amazon](#).
2. En el panel de navegación, elija Instancias y, a continuación, Iniciar instancias para abrir el nuevo asistente de inicialización de instancias.
3. (Opcional) En la sección Nombre y etiquetas, proporciona un nombre para la instancia, como `PCS-LoginNode`. El nombre se asigna a la instancia como etiqueta de recurso (`Name=PCS-LoginNode`).
4. En la sección Imágenes de aplicaciones y sistemas operativos, seleccione una AMI para uno de los sistemas operativos compatibles con AWS PCS. Para obtener más información, consulte [Sistemas operativos compatibles](#).
5. En la sección Tipo de instancia, seleccione un tipo de instancia compatible. Para obtener más información, consulte [Tipos de instancias admitidas](#).
6. En la sección Par de claves, selecciona el par de claves SSH que quieres usar en la instancia.
7. En la sección Configuración de red:
  - Seleccione Editar.

- i. Seleccione la VPC de su clúster de AWS PCS.
- ii. En Firewall (grupos de seguridad), elija Seleccionar un grupo de seguridad existente.
  - A. Seleccione un grupo de seguridad que permita el tráfico entre la instancia y el controlador Slurm del clúster AWS PCS de destino. Para obtener más información, consulte [Requisitos y consideraciones sobre los grupos de seguridad](#).
  - B. (Opcional) Seleccione un grupo de seguridad que permita el acceso SSH entrante a su instancia.
8. En la sección Almacenamiento, configura los volúmenes de almacenamiento según sea necesario. Asegúrese de configurar suficiente espacio para instalar aplicaciones y bibliotecas a fin de habilitar su caso de uso.
9. En Avanzado, elija un rol de IAM que permita acceder al secreto del clúster. Para obtener más información, consulte [Obtén el secreto del cúmulo de Slurm](#).
10. En el panel de resumen, elija Launch instance.

### Paso 3: Instala Slurm en la instancia

Cuando la instancia se haya lanzado y se active, conéctese a ella mediante el mecanismo que prefiera. Use el instalador de Slurm proporcionado por AWS para instalar Slurm en la instancia. Para obtener más información, consulte [Instalador de Slurm](#).

Descarga el instalador de Slurm, descomprímelo y usa el script para instalar Slurm. `installer.sh`  
Para obtener más información, consulte [Paso 3: Instalar Slurm](#).

### Paso 4: Recupere y almacene el secreto del clúster

Estas instrucciones requieren la AWS CLI. Para obtener más información, consulte [Instalar o actualizar a la última versión de AWS CLI en la](#) Guía del AWS Command Line Interface usuario de la versión 2.

Guarde el secreto del clúster con los siguientes comandos.

- Cree el directorio de configuración de Slurm.

```
sudo mkdir -p /etc/slurm
```

- Recupere, decodifique y almacene el secreto del clúster. Antes de ejecutar este comando, *region-code* sustitúyalo por la región en la que se ejecuta el clúster de destino y *secret-arn* sustitúyalo por el valor secretArn obtenido en el [paso 1](#).

```
aws secretsmanager get-secret-value \  
  --region region-code \  
  --secret-id 'secret-arn' \  
  --version-stage AWSCURRENT \  
  --query 'SecretString' \  
  --output text | base64 -d | sudo tee /etc/slurm/slurm.key
```

#### Warning

En un entorno multiusuario, cualquier usuario con acceso a la instancia podría obtener el secreto del clúster si puede acceder al servicio de metadatos de la instancia (IMDS). Esto, a su vez, podría permitirles hacerse pasar por otros usuarios. Considere la posibilidad de restringir el acceso al IMDS únicamente a los usuarios root o administrativos. Como alternativa, puedes utilizar un mecanismo diferente que no dependa del perfil de la instancia para obtener y configurar el secreto.

- Configura la propiedad y los permisos en el archivo de claves de Slurm.

```
sudo chmod 0600 /etc/slurm/slurm.key  
sudo chown slurm:slurm /etc/slurm/slurm.key
```

#### Note

La clave Slurm debe ser propiedad del usuario y del grupo en los que se ejecuta el sackd servicio.

## Paso 5: Configurar la conexión al clúster de PCS AWS

Para establecer una conexión con el clúster de AWS PCS, ejecútelo sackd como un servicio del sistema siguiendo estos pasos.

1. Configure el archivo de entorno del sackd servicio con el siguiente comando. Antes de ejecutar el comando, sustituya *ip-address* y por *port* los valores recuperados de los puntos finales en el [paso 1](#).

```
sudo echo "SACKD_OPTIONS='--conf-server=ip-address:port'" > /etc/sysconfig/sackd
```

2. Cree un archivo systemd de servicio para gestionar el sackd proceso.

```
sudo cat << EOF > /etc/systemd/system/sackd.service
[Unit]
Description=Slurm auth and cred kiosk daemon
After=network-online.target remote-fs.target
Wants=network-online.target
ConditionPathExists=/etc/sysconfig/sackd

[Service]
Type=notify
EnvironmentFile=/etc/sysconfig/sackd
User=slurm
Group=slurm
RuntimeDirectory=slurm
RuntimeDirectoryMode=0755
ExecStart=/opt/aws/pcs/scheduler/slurm-24.05/sbin/sackd --systemd \${SACKD_OPTIONS}
ExecReload=/bin/kill -HUP \${MAINPID}
KillMode=process
LimitNOFILE=131072
LimitMEMLOCK=infinity
LimitSTACK=infinity

[Install]
WantedBy=multi-user.target
EOF
```

3. Establezca la propiedad del archivo sackd de servicio.

```
sudo chown root:root /etc/systemd/system/sackd.service && \
sudo chmod 0644 /etc/systemd/system/sackd.service
```

4. Habilite el sackd servicio.

```
sudo systemctl daemon-reload && sudo systemctl enable sackd
```

## 5. Inicie el servicio sackd.

```
sudo systemctl start sackd
```

## Paso 6: (opcional) Pruebe la conexión

Confirme que el sackd servicio se esté ejecutando. A continuación, se muestra un resultado de ejemplo. Si hay errores, suelen aparecer aquí.

```
[root@ip-10-3-27-112 ~]# systemctl status sackd
[x] sackd.service - Slurm auth and cred kiosk daemon
   Loaded: loaded (/etc/systemd/system/sackd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2024-12-17 16:34:55 UTC; 8s ago
 Main PID: 9985 (sackd)
   CGroup: /system.slice/sackd.service
           ##9985 /opt/aws/pcs/scheduler/slurm-24.05/sbin/sackd --systemd --conf-
server=10.3.149.220:6817

Dec 17 16:34:55 ip-10-3-27-112.ec2.internal systemd[1]: Starting Slurm auth and cred
kiosk daemon...
Dec 17 16:34:55 ip-10-3-27-112.ec2.internal systemd[1]: Started Slurm auth and cred
kiosk daemon.
Dec 17 16:34:55 ip-10-3-27-112.ec2.internal sackd[9985]: sackd: running
```

Confirme que las conexiones al clúster funcionan mediante comandos del cliente de Slurm como `sinfo` y `squeue`. A continuación se muestra un ejemplo de la salida de `sinfo`.

```
[root@ip-10-3-27-112 ~]# /opt/aws/pcs/scheduler/slurm-24.11/bin/sinfo
PARTITION AVAIL TIMELIMIT NODES STATE NODELIST
all up infinite 4 idle~ compute-[1-4]
```

También deberías poder enviar trabajos. Por ejemplo, un comando similar a este ejemplo lanzaría un trabajo interactivo en un nodo del clúster.

```
/opt/aws/pcs/scheduler/slurm-24.11/bin/srun --nodes=1 -p all --pty bash -i
```

# AWS Redes PCS

El clúster de AWS PCS se crea en una Amazon VPC. En este capítulo se incluyen los siguientes temas sobre las redes para el programador y los nodos del clúster.

A excepción de elegir una subred para lanzar instancias, debe usar plantillas de EC2 lanzamiento para configurar las redes de los grupos de nodos de cómputo de AWS PCS. Para obtener más información acerca de las plantillas de inicialización, consulte [Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS](#).

## Temas

- [AWS Requisitos y consideraciones de PCS, VPC y subred](#)
- [Creación de una VPC para su AWS clúster de PCS](#)
- [Grupos de seguridad en AWS PCS](#)
- [Múltiples interfaces de red en AWS PCS](#)
- [Grupos de ubicación para EC2 instancias en AWS PCS](#)
- [Uso del Elastic Fabric Adapter \(EFA\) con PCS AWS](#)

## AWS Requisitos y consideraciones de PCS, VPC y subred

Al crear un clúster de AWS PCS, se especifica una VPC, una subred en esa VPC. En este tema se proporciona una descripción general de los requisitos y consideraciones específicos del AWS PCS para la VPC y las subredes que se utilizan con el clúster. Si no tiene una VPC para usarla con AWS PCS, puede crear una mediante una plantilla proporcionada AWS. AWS CloudFormation Para obtener más información VPCs, consulte [Nubes privadas virtuales \(VPC\)](#) en la Guía del usuario de Amazon VPC.

## Requisitos y consideraciones de la VPC

Al crear un clúster, la VPC que especifique debe cumplir los siguientes requisitos y consideraciones:

- La VPC debe tener un número suficiente de direcciones IP disponibles para el clúster, los nodos y otros recursos del clúster que desee crear. Para obtener más información, consulte el [direccionamiento IP de su red VPCs y de sus subredes](#) en la Guía del usuario de Amazon VPC.

- La VPC debe tener un nombre de host DNS y ser compatible con la resolución de DNS. De lo contrario, los nodos no podrán registrar el clúster de clientes. Para obtener más información, consulte [Atributos de DNS para su VPC](#) en la Guía del usuario de Amazon VPC.
- Es posible que la VPC requiera el uso de puntos finales de la VPC AWS PrivateLink para poder contactar con la API de PCS. AWS Para obtener más información, consulte [Conectar la VPC a los servicios mediante](#) la Guía del AWS PrivateLink usuario de Amazon VPC.

#### Important

AWS PCS no admite una VPC con arrendamiento de instancias dedicado. La VPC que utilice para AWS PCS debe utilizar la tenencia de default instancias. Puede cambiar la tenencia de la instancia de una VPC existente. Para obtener más información, consulte [Cambiar la tenencia de una instancia de una VPC](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

## Requisitos y consideraciones de la subred

Al crear un clúster de Slurm, AWS PCS crea una [interfaz de red elástica \(ENI\)](#) en la subred que especificó. Esta interfaz de red permite la comunicación entre el controlador del planificador y la VPC del cliente. La interfaz de red también permite a Slurm comunicarse con los componentes implementados en la cuenta del cliente. Solo puede especificar la subred de un clúster en el momento de la creación.

## Requisitos de la subred para los clústeres

La [subred](#) que especifique al crear un clúster debe cumplir los siguientes requisitos:

- La subred debe tener al menos una dirección IP para que la utilice PCS. AWS
- La subred no puede residir en AWS Outposts AWS Wavelength, o en una AWS zona local.
- La subred puede ser pública o privada. Le recomendamos que especifique una subred privada, si es posible. Una subred pública es una subred con una tabla de enrutamiento que incluye una ruta a una [puerta de enlace a Internet](#); una subred privada es una subred con una tabla de enrutamiento que no incluye una ruta a una puerta de enlace a Internet.

## Requisitos de la subred para los nodos

Puede implementar nodos y otros recursos de clúster en la subred que especifique al crear el clúster de AWS PCS y en otras subredes de la misma VPC.

Cualquier subred en la que implementes nodos y recursos de clúster debe cumplir los siguientes requisitos:

- Debe asegurarse de que la subred tenga suficientes direcciones IP disponibles para implementar todos los nodos y los recursos del clúster.
- Si planea implementar nodos en una subred pública, esa subred debe asignar direcciones públicas automáticamente IPv4 .
- Si la subred en la que despliega los nodos es una subred privada y su tabla de enrutamiento no incluye una ruta a un [dispositivo de traducción de direcciones de red \(NAT\) \(IPv4\)](#), añada puntos de enlace de VPC a AWS PrivateLink la VPC del cliente. Los puntos finales de VPC son necesarios para todos los AWS servicios con los que contactan los nodos. El único punto final necesario es que el AWS PCS permita que el nodo inicie la acción de la `RegisterComputeNodeGroupInstance` API. Para obtener más información, consulte la referencia [RegisterComputeNodeGroupInstance](#) de la API de AWS PCS.
- El estado de la subred pública o privada no afecta al AWS PCS; los puntos finales necesarios deben estar accesibles.

## Creación de una VPC para su AWS clúster de PCS

Puede crear una Amazon Virtual Private Cloud (Amazon VPC) para sus clústeres dentro de AWS Parallel Computing Service (AWS PCS).

Utilice Amazon VPC para lanzar recursos de VPC en una red virtual que haya definido. Esta red virtual es prácticamente idéntica a una red tradicional que podría operar en su propio centro de datos. Sin embargo, incluye los beneficios que supone utilizar la infraestructura escalable de Amazon Web Services. Le recomendamos que conozca a fondo el servicio Amazon VPC antes de implementar clústeres de VPC de producción. Para obtener más información, consulte [¿Qué es Amazon VPC?](#) en el modo visual de autor. Guía del usuario de Amazon VPC.

En su Amazon VPC se implementan un clúster de PCS, nodos y recursos de soporte (como sistemas de archivos y servicios de directorio). Si desea utilizar una Amazon VPC existente con PCS, debe cumplir los requisitos descritos en [AWS Requisitos y consideraciones de PCS, VPC y subred](#) En

este tema se describe cómo crear una VPC que cumpla con los requisitos de PCS mediante una plantilla proporcionada AWS. AWS CloudFormation Una vez que haya implementado una plantilla, podrá ver los recursos creados por la plantilla para saber exactamente qué recursos creó y la configuración de esos recursos.

## Requisitos previos

Para crear una Amazon VPC para PCS, debe tener los permisos de IAM necesarios para crear recursos de Amazon VPC. Estos recursos son subredes VPCs, grupos de seguridad, tablas y rutas de enrutamiento y puertas de enlace de Internet y NAT. Para obtener más información, consulte [Crear una VPC con una subred pública en la Guía del usuario](#) de Amazon VPC. Para consultar la lista completa de Amazon EC2, consulta [Acciones, recursos y claves de condición de Amazon EC2](#) en la Referencia de autorización de servicio.

## Creación de una Amazon VPC

Cree una VPC copiando y pegando la URL adecuada para el lugar en el Región de AWS que utilizará la PCS. [También puede descargar la AWS CloudFormation plantilla y subirla usted mismo a la AWS CloudFormation consola.](#)

- EE.UU. Este (Virginia) (us-east-1)

```
https://console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create/review?stackName=hpc-networking&templateURL=https://aws-hpc-recipes.s3.us-east-1.amazonaws.com/main/recipes/net/hpc_large_scale/assets/main.yaml
```

- EE.UU. Este (Ohio) (us-east-2)

```
https://console.aws.amazon.com/cloudformation/home?region=us-east-2#/stacks/create/review?stackName=hpc-networking&templateURL=https://aws-hpc-recipes.s3.us-east-1.amazonaws.com/main/recipes/net/hpc_large_scale/assets/main.yaml
```

- EE.UU. Oeste (Oregón) (us-west-2)

```
https://console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/create/review?stackName=hpc-networking&templateURL=https://aws-hpc-recipes.s3.us-east-1.amazonaws.com/main/recipes/net/hpc_large_scale/assets/main.yaml
```

- Solo plantilla

```
https://aws-hpc-recipes.s3.us-east-1.amazonaws.com/main/recipes/net/hpc_large_scale/assets/main.yaml
```

Para crear una Amazon VPC para PCS

1. Abra la plantilla en la [AWS CloudFormation consola](#).

 Note

Se rellenan previamente en la plantilla, por lo que puede simplemente dejarlos como valores predeterminados.

2. En Proporcione un nombre de pila y, a continuación, en Nombre de pila, introduzca `hpc-networking`.
3. En Parámetros, introduce los siguientes detalles:
  - a. A continuación, en VPC, introduzca `CidrBlock10.3.0.0/16`
  - b. En las subredes A:
    - i. Luego `CidrPublicSubnetA`, introduzca `10.3.0.0/20`
    - ii. Luego `CidrPrivateSubnetA`, ingresa `10.3.128.0/20`
  - c. En las subredes B:
    - i. A continuación, `CidrPublicSubnetB`, introduzca `10.3.16.0/20`
    - ii. Luego `CidrPrivateSubnetA`, ingresa `10.3.144.0/20`
  - d. En las subredes C:
    - i. Para `ProvisionSubnetsC`, seleccione `True`.

 Note

Si va a crear una VPC en una región que tiene menos de tres zonas de disponibilidad, esta opción se ignorará si se establece en `True`

- ii. A continuación, `CidrPublicSubnetB`, introduzca `10.3.32.0/20`
- iii. Luego `CidrPrivateSubnetA`, ingresa `10.3.160.0/20`

4. En Capacidades, marca la casilla Acepto que AWS CloudFormation podría crear recursos de IAM.

Supervise el estado de la AWS CloudFormation pila. Cuando llegue `CREATE_COMPLETE`, el recurso de VPC estará listo para su uso.

 Note

Para ver todos los recursos que creó la AWS CloudFormation plantilla, abra la [AWS CloudFormation consola](#). Elija la pila `hpc-networking` y, a continuación, elija la pestaña Resources (Recursos).

## Grupos de seguridad en AWS PCS

Los grupos de seguridad de Amazon EC2 actúan como firewalls virtuales para controlar el tráfico entrante y saliente a las instancias. Utilice una plantilla de lanzamiento para un grupo de nodos de cómputo de AWS PCS para añadir o eliminar grupos de seguridad en sus instancias. Si la plantilla de lanzamiento no contiene ninguna interfaz de red, utilícela `SecurityGroupIds` para proporcionar una lista de grupos de seguridad. Si la plantilla de lanzamiento define las interfaces de red, debe usar el `Groups` parámetro para asignar grupos de seguridad a cada interfaz de red. Para obtener más información acerca de las plantillas de inicialización, consulte [Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS](#).

 Note

Los cambios en la configuración del grupo de seguridad en la plantilla de lanzamiento solo afectan a las nuevas instancias lanzadas una vez actualizado el grupo de nodos de procesamiento.

## Requisitos y consideraciones sobre los grupos de seguridad

AWS PCS crea una [interfaz de red elástica \(ENI\)](#) entre cuentas en la subred que especifique al crear un clúster. Esto proporciona al programador de HPC, que se ejecuta en una cuenta administrada por AWS, una ruta para comunicarse con las EC2 instancias lanzadas por PCS. AWS Debe proporcionar

un grupo de seguridad para ese ENI que permita la comunicación bidireccional entre el ENI del programador y las instancias del clúster. EC2

Una forma sencilla de lograrlo consiste en crear un grupo de seguridad autorreferenciado permisivo que permita el tráfico TCP/IP en todos los puertos entre todos los miembros del grupo. Puede adjuntarlo tanto al clúster como a las instancias del grupo de nodos. EC2

### Ejemplo de configuración permisiva de un grupo de seguridad

Tipo de regla	Protocolos	Puertos	Origen	Destino
Entrada	Todos	Todos	Auto	
Salida	Todos	Todos		0.0.0.0/0
Salida	Todos	Todos		Auto

[Estas reglas permiten que todo el tráfico fluya libremente entre el controlador Slurm y los nodos, permiten que todo el tráfico saliente se dirija a cualquier destino y habilitan el tráfico EFA.](#)

### Ejemplo de configuración restrictiva de un grupo de seguridad

También puede limitar los puertos abiertos entre el clúster y sus nodos de procesamiento. En el caso del programador de Slurm, el grupo de seguridad adjunto al clúster debe permitir los siguientes puertos:

- 6817: habilita las conexiones entrantes desde y hacia las instancias `slurmctld` EC2
- 6818: habilita las conexiones salientes desde `slurmctld` y hasta que se ejecuten en las instancias `slurmd` EC2

El grupo de seguridad adjunto a sus nodos de procesamiento debe permitir los siguientes puertos:

- 6817: habilita las conexiones salientes `slurmctld` desde EC2 las instancias.
- 6818: habilita las conexiones entrantes y salientes desde y hacia las instancias `slurmd` del grupo de `slurmctld` nodos `slurmd`
- 60001—63000: conexiones entrantes y salientes entre instancias de grupos de nodos para admitir `srn`

- Tráfico de EFA entre instancias de grupos de nodos. Para obtener más información, consulte [Preparar un grupo de seguridad habilitado para EFA](#) en la Guía del usuario para instancias de Linux
- Cualquier otro tráfico entre nodos que requiera su carga de trabajo

## Múltiples interfaces de red en AWS PCS

Algunas EC2 instancias tienen varias tarjetas de red. Esto les permite ofrecer un mayor rendimiento de la red, incluidas capacidades de ancho de banda superiores a 100 Gbps y una mejor gestión de paquetes. Para obtener más información sobre las instancias con varias tarjetas de red, consulte [Interfaces de red elásticas](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Configure tarjetas de red adicionales para las instancias de un grupo de nodos de cómputo de AWS PCS añadiendo interfaces de red a su plantilla de EC2 lanzamiento. A continuación, se muestra un ejemplo de plantilla de lanzamiento que habilita dos tarjetas de red, como las que se encuentran en una `hpc7a.96xlarge` instancia. Tenga en cuenta la siguiente información:

- La subred de cada interfaz de red debe ser la misma que la elegida al configurar el grupo de nodos de cómputo del AWS PCS que utilizará la plantilla de lanzamiento.
- El dispositivo de red principal, donde se producirá la comunicación de red rutinaria, como el tráfico SSH y HTTPS, se establece configurando una `DeviceIndex` de `0`. Otras interfaces de red tienen un `DeviceIndex` de `1`. Solo puede haber una interfaz de red principal; todas las demás interfaces son secundarias.
- Todas las interfaces de red deben tener una única `NetworkCardIndex`. Una práctica recomendada es numerarlas secuencialmente tal como se definen en la plantilla de lanzamiento.
- Los grupos de seguridad para cada interfaz de red se configuran mediante `Groups`. En este ejemplo, se agrega un grupo de seguridad SSH entrante (`sg-SshSecurityGroupId`) a la interfaz de red principal, así como un grupo de seguridad que permite las comunicaciones dentro del clúster (`sg-ClusterSecurityGroupId`). Por último, se agrega un grupo de seguridad que permite las conexiones salientes a Internet (`sg-InternetOutboundSecurityGroupId`) a las interfaces principal y secundaria.

```
{
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
```

```

    "NetworkCardIndex": 0,
    "SubnetId": "subnet-SubnetId",
    "Groups": [
      "sg-SshSecurityGroupId",
      "sg-ClusterSecurityGroupId",
      "sg-InternetOutboundSecurityGroupId"
    ]
  },
  {
    "DeviceIndex": 1,
    "NetworkCardIndex": 1,
    "SubnetId": "subnet-SubnetId",
    "Groups": ["sg-InternetOutboundSecurityGroupId"]
  }
]
}

```

## Grupos de ubicación para EC2 instancias en AWS PCS

Puede utilizar un grupo de ubicación para influir en la ubicación de las EC2 instancias y adaptarlas a las necesidades de la carga de trabajo que se ejecuta en ellas.

### Tipos de grupos de colocación

- **Clúster:** agrupa las instancias juntas en una zona de disponibilidad para optimizar la comunicación de baja latencia.
- **Partición:** distribuye las instancias entre las particiones lógicas para ayudar a maximizar la resiliencia.
- **Distribución:** exige estrictamente que un número reducido de instancias se lance en un hardware distinto, lo que también contribuye a aumentar la resiliencia.

Para obtener más información, consulta [los grupos de ubicación para tus EC2 instancias de Amazon](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Se recomienda incluir un grupo de ubicación de clústeres al configurar un grupo de nodos de cómputo de AWS PCS para usar Elastic Fabric Adapter (EFA).

Para crear un grupo de ubicación en clústeres que funcione con EFA

1. Cree un grupo de ubicación con el tipo cluster para el grupo de nodos de procesamiento.

- Utilice el siguiente AWS CLI comando:

```
aws ec2 create-placement-group --strategy cluster --group-name PLACEMENT-GROUP-NAME
```

- También puede utilizar una CloudFormation plantilla para crear un grupo de ubicación. Para obtener más información, consulte [Trabajar con CloudFormation plantillas](#) en la Guía del AWS CloudFormation usuario. Descargue la plantilla desde la siguiente URL y cárguela en la [CloudFormation consola](#).

```
https://aws-hpc-recipes.s3.amazonaws.com/main/recipes/pcs/enable_efa/assets/efa-placement-group.yaml
```

2. Incluya el grupo de ubicación en la plantilla de EC2 lanzamiento del grupo de nodos de cómputo de AWS PCS.

## Uso del Elastic Fabric Adapter (EFA) con PCS AWS

El Elastic Fabric Adapter (EFA) es una interconexión de red avanzada de alto rendimiento AWS que se puede conectar a la EC2 instancia para acelerar las aplicaciones de computación de alto rendimiento (HPC) y aprendizaje automático. Para permitir que sus aplicaciones se ejecuten en un clúster de AWS PCS con EFA, es necesario configurar las instancias del grupo de nodos de cómputo del AWS PCS para que utilicen EFA de la siguiente manera.

### Note

Instalación de EFA en una AMI AWS compatible con PCS: la AMI utilizada en AWS el grupo de nodos de cómputo de PCS debe tener el controlador EFA instalado y cargado. Para obtener información sobre cómo crear una AMI personalizada con el software EFA instalado, consulte [Imágenes personalizadas de Amazon Machine \(AMIs\) para AWS PCS](#).

### Contenido

- [Identifique las instancias habilitadas para EFA EC2](#)
- [Cree un grupo de seguridad para respaldar las comunicaciones de la EFA](#)
- [\(Opcional\) Cree un grupo de ubicación](#)
- [Cree o actualice una plantilla de EC2 lanzamiento](#)

- [Cree o actualice grupos de nodos de cómputo para EFA](#)
- [\(Opcional\) Pruebe la EFA](#)
- [\(Opcional\) Usa una CloudFormation plantilla para crear una plantilla de lanzamiento compatible con la EFA](#)

## Identifique las instancias habilitadas para EFA EC2

Para usar EFA, todos los tipos de instancias permitidos para un grupo de cómputo de AWS PCS deben admitir la EFA y deben tener el mismo número de v CPUs (y GPUs si corresponde). Para obtener una lista de instancias habilitadas para EFA, consulte [Elastic Fabric Adapter para cargas de trabajo de HPC y ML en Amazon EC2 en](#) la Guía del usuario de Amazon Elastic Compute Cloud. También puedes usarlo AWS CLI para ver una lista de tipos de instancias que admiten la EFA. `region-code` Sustitúyala por la Región de AWS que utilices AWS PCS, por ejemplo `us-east-1`.

```
aws ec2 describe-instance-types \
  --region region-code \
  --filters Name=network-info.efa-supported,Values=true \
  --query "InstanceTypes[*].[InstanceType]" \
  --output text | sort
```

### Note

Determine cuántas interfaces de red están disponibles: algunas EC2 instancias tienen varias tarjetas de red. Esto les permite tener varias EFAs. Para obtener más información, consulte [Múltiples interfaces de red en AWS PCS](#).

## Cree un grupo de seguridad para respaldar las comunicaciones de la EFA

### AWS CLI

Puede usar el siguiente AWS CLI comando para crear un grupo de seguridad que admita la EFA. El comando genera un ID de grupo de seguridad. Realice las siguientes sustituciones:

- `region-code`— Especifique Región de AWS dónde va a utilizar el AWS PCS, por ejemplo. `us-east-1`
- `vpc-id`— Especifique el ID de la VPC que utiliza para AWS PCS.

- *efa-group-name*— Proporcione el nombre que haya elegido para el grupo de seguridad.

```
aws ec2 create-security-group \  
  --group-name efa-group-name \  
  --description "Security group to enable EFA traffic" \  
  --vpc-id vpc-id \  
  --region region-code
```

Utilice los siguientes comandos para adjuntar las reglas de los grupos de seguridad entrantes y salientes. Realice la siguiente sustitución:

- *efa-secgroup-id*— Proporcione el ID del grupo de seguridad de EFA que acaba de crear.

```
aws ec2 authorize-security-group-ingress \  
  --group-id efa-secgroup-id \  
  --protocol -1 \  
  --source-group efa-secgroup-id  
  
aws ec2 authorize-security-group-egress \  
  --group-id efa-secgroup-id \  
  --protocol -1 \  
  --source-group efa-secgroup-id
```

## CloudFormation template

Puede usar una CloudFormation plantilla para crear un grupo de seguridad que admita la EFA. Descargue la plantilla desde la siguiente URL y, a continuación, cárguela en la [AWS CloudFormation consola](#).

```
https://aws-hpc-recipes.s3.amazonaws.com/main/recipes/pcs/enable_efa/assets/efa-  
sg.yaml
```

Con la plantilla abierta en la AWS CloudFormation consola, introduce las siguientes opciones.

- En Proporcione un nombre de pila
  - En Nombre de pila, introduce un nombre como *efa-sg-stack*.
- En Parámetros
  - En SecurityGroupName, introduzca un nombre como *efa-sg*.

- En VPC, seleccione la VPC en la que utilizará PCS. AWS

Termine de crear la CloudFormation pila y supervise su estado. Cuando llegue al EFA, CREATE\_COMPLETE el grupo de seguridad estará listo para su uso.

## (Opcional) Cree un grupo de ubicación

Se recomienda lanzar todas las instancias que utilizan la EFA en un grupo de ubicación en clústeres para minimizar la distancia física entre ellas. Cree un grupo de ubicación para cada grupo de nodos de cómputo en el que vaya a usar EFA. Consulte esta [Grupos de ubicación para EC2 instancias en AWS PCS](#) sección para crear un grupo de ubicación para su grupo de nodos de cómputo.

## Cree o actualice una plantilla de EC2 lanzamiento

Las interfaces de red EFA se configuran en la plantilla de EC2 lanzamiento de un grupo de nodos de cómputo del AWS PCS. Si hay varias tarjetas de red, se EFAs pueden configurar varias. El grupo de seguridad EFA y el grupo de ubicación opcional también se incluyen en la plantilla de lanzamiento.

A continuación, se muestra un ejemplo de plantilla de lanzamiento para instancias con dos tarjetas de red, como hpc7a.96xlarge. Las instancias se lanzarán en un grupo de ubicación en clústeres.

```
subnet-SubnetID1 pg-PlacementGroupId1
```

Los grupos de seguridad se deben agregar específicamente a cada interfaz EFA. Cada EFA necesita el grupo de seguridad que habilita el tráfico EFA (). sg-*EfaSecGroupId* Otros grupos de seguridad, especialmente los que gestionan tráfico normal, como SSH o HTTPS, solo necesitan estar conectados a la interfaz de red principal (designada con un DeviceIndex de). 0 Las plantillas de lanzamiento en las que se definen las interfaces de red no admiten la configuración de grupos de seguridad mediante el SecurityGroupIds parámetro; debe establecer un valor para Groups cada interfaz de red que configure.

```
{
  "Placement": {
    "GroupId": "pg-PlacementGroupId1"
  },
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "InterfaceType": "efa",
      "NetworkCardIndex": 0,
```

```

        "SubnetId": "subnet-SubnetId1",
        "Groups": [
            "sg-SecurityGroupId1",
            "sg-EfaSecGroupId"
        ]
    },
    {
        "DeviceIndex": 1,
        "InterfaceType": "efa",
        "NetworkCardIndex": 1,
        "SubnetId": "subnet-SubnetId1"
        "Groups": ["sg-EfaSecGroupId"]
    }
]
}

```

## Cree o actualice grupos de nodos de cómputo para EFA

Los grupos de nodos de cómputo de AWS PCS deben contener instancias que tengan el mismo número de vCPUs, arquitectura de procesador y compatibilidad con EFA. Configure el grupo de nodos de procesamiento para usar la AMI con el software EFA instalado y para usar la plantilla de lanzamiento que configura las interfaces de red habilitadas para EFA.

### (Opcional) Pruebe la EFA

Para demostrar la comunicación habilitada por EFA entre dos nodos de un grupo de nodos de cómputo, ejecute el `fi_pingpong` programa, que se incluye en la instalación del software EFA. Si esta prueba se realiza correctamente, es probable que el EFA esté configurado correctamente.

Para empezar, necesita dos instancias en ejecución en el grupo de nodos de cómputo. Si tu grupo de nodos de cómputo usa capacidad estática, ya debería haber instancias disponibles. En el caso de un grupo de nodos de cómputo que utilice capacidad dinámica, puede lanzar dos nodos mediante el `salloc` comando. A continuación, se muestra un ejemplo de un clúster con un nombre de grupo de nodos dinámico `hpc7g` asociado a una cola denominada `a11`.

```

% salloc --nodes 2 -p all
salloc: Granted job allocation 6
salloc: Waiting for resource configuration
... a few minutes pass ...
salloc: Nodes hpc7g-[1-2] are ready for job

```

Averigüe la dirección IP de los dos nodos asignados mediante `scontrol`. En el siguiente ejemplo, las direcciones son `10.3.140.69` para `hpc7g-1` y `10.3.132.211` para `hpc7g-2`.

```
% scontrol show nodes hpc7g-[1-2]
NodeName=hpc7g-1 Arch=aarch64 CoresPerSocket=1
  CPUAlloc=0 CPUEfctv=64 CPUTot=64 CPULoad=0.00
  AvailableFeatures=hpc7g
  ActiveFeatures=hpc7g
  Gres=(null)
  NodeAddr=10.3.140.69 NodeHostName=ip-10-3-140-69 Version=23.11.8
  OS=Linux 5.10.218-208.862.amzn2.aarch64 #1 SMP Tue Jun 4 16:52:10 UTC 2024
  RealMemory=124518 AllocMem=0 FreeMem=110763 Sockets=64 Boards=1
  State=IDLE+CLOUD ThreadsPerCore=1 TmpDisk=0 Weight=1 Owner=N/A MCS_label=N/A
  Partitions=efa
  BootTime=2024-07-02T19:00:09 SlurmdStartTime=2024-07-08T19:33:25
  LastBusyTime=2024-07-08T19:33:25 ResumeAfterTime=None
  CfgTRES=cpu=64,mem=124518M,billing=64
  AllocTRES=
  CapWatts=n/a
  CurrentWatts=0 AveWatts=0
  ExtSensorsJoules=n/a ExtSensorsWatts=0 ExtSensorsTemp=n/a
  Reason=Maintain Minimum Number Of Instances [root@2024-07-02T18:59:00]
  InstanceId=i-04927897a9ce3c143 InstanceType=hpc7g.16xlarge

NodeName=hpc7g-2 Arch=aarch64 CoresPerSocket=1
  CPUAlloc=0 CPUEfctv=64 CPUTot=64 CPULoad=0.00
  AvailableFeatures=hpc7g
  ActiveFeatures=hpc7g
  Gres=(null)
  NodeAddr=10.3.132.211 NodeHostName=ip-10-3-132-211 Version=23.11.8
  OS=Linux 5.10.218-208.862.amzn2.aarch64 #1 SMP Tue Jun 4 16:52:10 UTC 2024
  RealMemory=124518 AllocMem=0 FreeMem=110759 Sockets=64 Boards=1
  State=IDLE+CLOUD ThreadsPerCore=1 TmpDisk=0 Weight=1 Owner=N/A MCS_label=N/A
  Partitions=efa
  BootTime=2024-07-02T19:00:09 SlurmdStartTime=2024-07-08T19:33:25
  LastBusyTime=2024-07-08T19:33:25 ResumeAfterTime=None
  CfgTRES=cpu=64,mem=124518M,billing=64
  AllocTRES=
  CapWatts=n/a
  CurrentWatts=0 AveWatts=0
  ExtSensorsJoules=n/a ExtSensorsWatts=0 ExtSensorsTemp=n/a
  Reason=Maintain Minimum Number Of Instances [root@2024-07-02T18:59:00]
  InstanceId=i-0a2c82623cb1393a7 InstanceType=hpc7g.16xlarge
```

Conéctese a uno de los nodos (en este caso de ejemplo hpc7g-1) mediante SSH (o SSM). Tenga en cuenta que se trata de una dirección IP interna, por lo que puede que necesite conectarse desde uno de sus nodos de inicio de sesión si utiliza SSH. Ten en cuenta también que la instancia debe configurarse con una clave SSH mediante la plantilla de lanzamiento del grupo de nodos de cómputo.

```
% ssh ec2-user@10.3.140.69
```

Ahora, `fi_pingpong` ejecútala en modo servidor.

```
/opt/amazon/efa/bin/fi_pingpong -p efa
```

Conéctese a la segunda instancia (hpc7g-2).

```
% ssh ec2-user@10.3.132.211
```

Se ejecuta `fi_pingpong` en modo cliente, conectándose al servidor activado hpc7g-1. Debería ver un resultado parecido al del ejemplo siguiente.

```
% /opt/amazon/efa/bin/fi_pingpong -p efa 10.3.140.69
```

bytes	#sent	#ack	total	time	MB/sec	usec/xfer	Mxfers/sec
64	10	=10	1.2k	0.00s	3.08	20.75	0.05
256	10	=10	5k	0.00s	21.24	12.05	0.08
1k	10	=10	20k	0.00s	82.91	12.35	0.08
4k	10	=10	80k	0.00s	311.48	13.15	0.08

```
[error] util/pingpong.c:1876: fi_close (-22) fid 0
```

## (Opcional) Usa una CloudFormation plantilla para crear una plantilla de lanzamiento compatible con la EFA

Como hay varias dependencias para configurar la EFA, se ha proporcionado una CloudFormation plantilla que puede utilizar para configurar un grupo de nodos de cálculo. Admite instancias con hasta cuatro tarjetas de red. Para obtener más información sobre las instancias con varias tarjetas de red, consulte las [interfaces de red elásticas](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Descargue la CloudFormation plantilla desde la siguiente URL y, a continuación, cárguela en la CloudFormation consola en la Región de AWS que utilice el AWS PCS.

```
https://aws-hpc-recipes.s3.amazonaws.com/main/recipes/pcs/enable_efa/assets/pcs-lt-efa.yaml
```

Con la plantilla abierta en la AWS CloudFormation consola, introduzca los siguientes valores. Tenga en cuenta que la plantilla proporcionará algunos valores de parámetros predeterminados; puede dejarlos como valores predeterminados.

- En Indique un nombre de pila
  - En Nombre de pila, introduce un nombre descriptivo. Le recomendamos que incorpore el nombre que elija para su grupo de nodos de cómputo de AWS PCS, por ejemplo `NODEGROUPNAME-efa-lt`.
- En Parámetros
  - En NumberOfNetworkCards, selecciona el número de tarjetas de red en las instancias que estarán en tu grupo de nodos.
  - En VpcId, elija la VPC en la que se implementa el clúster de AWS PCS.
  - En NodeGroupSubnetId, elija la subred de la VPC de su clúster donde se lanzarán las instancias habilitadas para EFA.
  - En PlacementGroupName, deje el campo en blanco para crear un nuevo grupo de ubicación de clústeres para el grupo de nodos. Si ya tiene un grupo de ubicación que quiere usar, introduzca su nombre aquí.
  - En ClusterSecurityGroupId, elija el grupo de seguridad que va a utilizar para permitir el acceso a otras instancias del clúster y a la API de AWS PCS. Muchos clientes eligen el grupo de seguridad predeterminado de su VPC de clúster.
  - En la sección SshSecurityGroupId, indique el ID del grupo de seguridad que esté utilizando para permitir el acceso SSH entrante a los nodos del clúster.
  - Para SshKeyName, seleccione el par de claves SSH para acceder a los nodos de su clúster.
  - Para LaunchTemplateName, introduzca un nombre descriptivo para la plantilla de lanzamiento, por ejemplo. `NODEGROUPNAME-efa-lt` El nombre debe ser exclusivo del usuario Cuenta de AWS en el Región de AWS lugar en el que vaya a utilizar AWS PCS.
- En Capacidades
  - Marque la casilla Reconozco que AWS CloudFormation podría crear recursos de IAM.

Supervisa el estado de la CloudFormation pila. Cuando llegue a CREATE\_COMPLETE la plantilla de lanzamiento estará lista para ser utilizada. Úselo con un grupo de nodos de cómputo del AWS PCS, tal y como se describe anteriormente en [Cree o actualice grupos de nodos de cómputo para EFA](#).

# Uso de sistemas de archivos de red con AWS PCS

Puede conectar los sistemas de archivos de red a los nodos lanzados en un grupo de nodos de cómputo del Servicio de Computación AWS Paralela (AWS PCS) para proporcionar una ubicación persistente en la que se puedan escribir los datos y los archivos y acceder a ellos. [Puede utilizar los sistemas de archivos proporcionados por AWS los servicios, como Amazon Elastic File System \(Amazon EFS\), Amazon FSx for Lustre, Amazon FSx for NetApp ONTAP, Amazon FSx for OpenZFS y Amazon File Cache.](#) También puede utilizar sistemas de archivos autogestionados, como servidores NFS.

En este tema se describen algunas consideraciones y ejemplos del uso de sistemas de archivos de red con AWS PCS.

## Consideraciones sobre el uso de sistemas de archivos de red

Los detalles de implementación de los distintos sistemas de archivos son diferentes, pero hay algunas consideraciones comunes.

- El software del sistema de archivos correspondiente debe estar instalado en la instancia. Por ejemplo, para usar Amazon FSx for Lustre, el apropiado Lustre el paquete debe estar presente. Esto se puede lograr incluyéndolo en la AMI del grupo de nodos de cómputo o utilizando un script que se ejecute al arrancar la instancia.
- Debe haber una ruta de red entre el sistema de archivos de red compartido y las instancias del grupo de nodos de procesamiento.
- Las reglas del grupo de seguridad tanto para el sistema de archivos de red compartido como para las instancias del grupo de nodos de procesamiento deben permitir las conexiones a los puertos correspondientes.
- Debe mantener una coherencia POSIX espacio de nombres de usuarios y grupos en todos los recursos que acceden a los sistemas de archivos. De lo contrario, los trabajos y los procesos interactivos que se ejecutan en el clúster de PCS podrían producir errores de permisos.
- Los montajes del sistema de archivos se realizan mediante EC2 plantillas de lanzamiento. Los errores o los tiempos de espera al montar un sistema de archivos de red pueden impedir que las instancias estén disponibles para ejecutar trabajos. Esto, a su vez, puede generar costes inesperados. Para obtener más información sobre la depuración de plantillas de lanzamiento, consulte [Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS.](#)

## Ejemplos de montajes de red

Puede crear sistemas de archivos con Amazon EFS, Amazon FSx for Lustre, Amazon FSx for NetApp ONTAP, Amazon FSx for OpenZFS y Amazon File Cache. Amplíe la sección correspondiente a continuación para ver un ejemplo de cada montaje de red.

### Amazon EFS

#### Configuración del sistema de archivos

Crear un sistema de archivos de Amazon EFS. Asegúrese de que tenga un objetivo de montaje en cada zona de disponibilidad en la que vaya a lanzar las instancias del grupo de nodos de cómputo de PCS. Asegúrese también de que cada destino de montaje esté asociado a un grupo de seguridad que permita el acceso entrante y saliente desde las instancias del grupo de nodos de cómputo del PCS. Para obtener más información, consulte [Montar objetivos y grupos de seguridad](#) en la Guía del usuario de Amazon Elastic File System.

#### Plantilla de lanzamiento

Añada los grupos de seguridad de la configuración del sistema de archivos a la plantilla de lanzamiento que utilizará para el grupo de nodos de cómputo.

Incluya datos de usuario que utilicen `cloud-config` un mecanismo para montar el sistema de archivos Amazon EFS. Sustituya los siguientes valores de este script por sus propios detalles:

- *mount-point-directory*— La ruta en cada instancia en la que montará Amazon EFS
- *filesystem-id*— El ID del sistema de archivos del sistema de archivos EFS

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="==MYBOUNDARY=="

--==MYBOUNDARY==
Content-Type: text/cloud-config; charset="us-ascii"

packages:
  - amazon-efs-utils

runcmd:
  - mkdir -p /mount-point-directory
  - echo "filesystem-id:/ mount-point-directory efs tls,_netdev" >> /etc/fstab
```

```
- mount -a -t efs defaults

---MYBOUNDARY---
```

## Amazon FSx para Lustre

### Configuración del sistema de archivos

Cree un sistema de archivos FSx para Lustre en la VPC donde utilizará AWS PCS. Para minimizar las transferencias entre zonas, despléguelo en una subred de la misma zona de disponibilidad donde lanzará la mayoría de las instancias del grupo de nodos de cómputo de PCS. Asegúrese de que el sistema de archivos esté asociado a un grupo de seguridad que permita el acceso entrante y saliente desde las instancias del grupo de nodos de cómputo del PCS. Para obtener más información sobre los grupos de seguridad, consulte [Control de acceso al sistema de archivos con Amazon VPC](#) en la Guía del usuario de Amazon FSx for Lustre.

### Plantilla de lanzamiento

Incluya los datos de usuario que se utilizan `cloud-config` para montar el sistema de FSx archivos de Lustre. Sustituya los siguientes valores de este script por sus propios detalles:

- *mount-point-directory*— La ruta de la instancia en la que quieres montarla FSx para Lustre
- *filesystem-id*— El ID del sistema de archivos del sistema de archivos FSx de Lustre
- *mount-name*— El nombre de montaje del sistema de FSx archivos para Lustre
- *region-code*— El Región de AWS lugar donde se implementa el sistema de archivos FSx for Lustre (debe ser el mismo que su sistema AWS PCS)
- (Opcional) *latest*: cualquier versión de Lustre compatible con FSx for Lustre

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary==="MYBOUNDARY==="

---MYBOUNDARY==
Content-Type: text/cloud-config; charset="us-ascii"

runcmd:
- amazon-linux-extras install -y lustre=latest
- mkdir -p /mount-point-directory
- mount -t lustre filesystem-id.fsx.region-code.amazonaws.com@tcp:/mount-name /mount-point-directory
```

```
--==MYBOUNDARY==
```

## Amazon FSx para NetApp ONTAP

### Configuración del sistema de archivos

Cree un sistema de archivos Amazon FSx for NetApp ONTAP en la VPC en la que utilizará AWS PCS. Para minimizar las transferencias entre zonas, despléguelo en una subred de la misma zona de disponibilidad donde lanzará la mayoría de las instancias del grupo de nodos de cómputo de AWS PCS. Asegúrese de que el sistema de archivos esté asociado a un grupo de seguridad que permita el acceso entrante y saliente desde las instancias del grupo de nodos de cómputo de AWS PCS. Para obtener más información sobre los grupos de seguridad, consulte [Control de acceso al sistema de archivos con Amazon VPC](#) en la Guía del usuario FSx de ONTAP.

### Plantilla de lanzamiento

Incluya los datos de usuario que se utilizan `cloud-config` para montar el volumen raíz de un sistema de archivos FSx de ONTAP. Sustituya los siguientes valores de este script por sus propios detalles:

- *mount-point-directory*— La ruta de la instancia en la que desea montar su volumen FSx para ONTAP
- *svm-id*— El ID de SVM del sistema de archivos FSx ONTAP
- *filesystem-id*— El ID del sistema de archivos del sistema de archivos FSx de ONTAP
- *region-code*— El Región de AWS lugar donde se implementa el FSx sistema de archivos de ONTAP (debe ser el mismo que el de su sistema AWS PCS)
- *volume-name*— El nombre del FSx volumen de ONTAP

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=="MYBOUNDARY=="

--==MYBOUNDARY==
Content-Type: text/cloud-config; charset="us-ascii"

runcmd:
- mkdir -p /mount-point-directory
```

```
- mount -t nfs svm-id.filesystem-id.fsx.region-code.amazonaws.com:/volume-name /mount-point-directory

--==MYBOUNDARY==
```

## Amazon FSx para OpenZFS

### Configuración del sistema de archivos

Cree un sistema de archivos FSx para OpenZFS en la VPC en el que utilizará PCS. AWS Para minimizar las transferencias entre zonas, impleméntelo en una subred de la misma zona de disponibilidad donde lanzará la mayoría de las instancias del grupo de nodos de cómputo de AWS PCS. Asegúrese de que el sistema de archivos esté asociado a un grupo de seguridad que permita el acceso entrante y saliente desde las instancias del grupo de nodos de cómputo de AWS PCS. Para obtener más información sobre los grupos de seguridad, consulte [Administrar el acceso al sistema de archivos con Amazon VPC](#) en la Guía del usuario FSx de OpenZFS.

### Plantilla de lanzamiento

Incluya los datos de usuario que se utilizan c`loud-config` para montar el volumen raíz de un sistema de archivos FSx para OpenZFS. Sustituya los siguientes valores de este script por sus propios detalles:

- *mount-point-directory*— La ruta de una instancia en la que quieres montar tu recurso compartido FSx para OpenZFS
- *filesystem-id*— El ID del sistema de archivos del sistema de archivos FSx OpenZFS
- *region-code*— El Región de AWS lugar donde se implementa el sistema de archivos FSx para OpenZFS (debe ser el mismo que el de su sistema PCS) AWS

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="==MYBOUNDARY=="

--==MYBOUNDARY==
Content-Type: text/cloud-config; charset="us-ascii"

runcmd:
- mkdir -p /mount-point-directory
- mount -t nfs -o noatime,nfsvers=4.2,sync,rsync,rsync,rsync,rsync,rsync filesystem-id.fsx.region-code.amazonaws.com:/fsx/ /mount-point-directory
```

```
--==MYBOUNDARY==
```

## Amazon File Cache

### Configuración del sistema de archivos

Cree una [caché de archivos de Amazon](#) en la VPC en la que utilizará AWS PCS. Para minimizar las transferencias entre zonas, elija una subred en la misma zona de disponibilidad en la que lanzará la mayoría de las instancias del grupo de nodos de cómputo de PCS. Asegúrese de que la caché de archivos esté asociada a un grupo de seguridad que permita el tráfico entrante y saliente en el puerto 988 entre las instancias de PCS y la caché de archivos. Para obtener más información sobre los grupos de seguridad, consulte [Control de acceso a caché con Amazon VPC](#) en la Guía del usuario de Amazon File Cache.

### Plantilla de lanzamiento

Añada los grupos de seguridad de la configuración de su sistema de archivos a la plantilla de lanzamiento que utilizará para el grupo de nodos de cómputo.

Incluye los datos de usuario que se utilizan `cloud-config` para montar la caché de archivos de Amazon. Sustituya los siguientes valores de este script por sus propios detalles:

- *mount-point-directory*— La ruta de la instancia en la que quieres montarla FSx para Lustre
- *cache-dns-name*— El nombre del sistema de nombres de dominio (DNS) de la caché de archivos
- *mount-name*— El nombre de montaje de la caché de archivos

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="==MYBOUNDARY=="

--==MYBOUNDARY==
Content-Type: text/cloud-config; charset="us-ascii"

runcmd:
- amazon-linux-extras install -y lustre=2.12
- mkdir -p /mount-point-directory
- mount -t lustre -o relatime,flock cache-dns-name@tcp:/mount-name /mount-point-
directory
```

```
--==MYBOUNDARY==
```

# Amazon Machine Images (AMIs) para AWS PCS

AWS PCS trabaja con los AMIs que usted proporciona, lo que ofrece una gran flexibilidad en el software y la configuración que se encuentran en los nodos de su clúster. Si está probando AWS PCS, puede utilizar un ejemplo de AMI proporcionado y mantenido por AWS. Si utiliza AWS PCS en producción, le recomendamos que construya el suyo propio AMIs. En este tema se explica cómo descubrir y utilizar el ejemplo AMIs, así como cómo crear y utilizar el suyo propio personalizado AMIs.

## Temas

- [Uso de Amazon Machine Images \(AMIs\) de muestra con AWS PCS](#)
- [Imágenes personalizadas de Amazon Machine \(AMIs\) para AWS PCS](#)
- [Instaladores de software para crear PCS personalizados AMIs AWS](#)
- [Notas de publicación para un ejemplo de AWS PCS AMIs](#)

## Uso de Amazon Machine Images (AMIs) de muestra con AWS PCS

AWS proporciona un [ejemplo AMIs](#) que puede utilizar como punto de partida para trabajar con AWS PCS.

### Important

AMIs Los ejemplos son para fines de demostración y no se recomiendan para cargas de trabajo de producción.

## Encuentre un ejemplo de AWS PCS actual AMIs

### AWS Management Console

AMIs Los ejemplos de PCS de AWS tienen la siguiente convención de nomenclatura:

```
aws-pcs-sample_ami-OS-architecture-scheduler-scheduler-major-version
```

### Valores aceptados

- *OS* – amzn2

- *architecture* – x86\_64 o arm64
- *scheduler* – slurm
- *scheduler-major-version* – 24.11

Para encontrar un ejemplo de AWS PCS AMIs

1. Abra la [EC2 consola de Amazon](#).
2. Vaya a AMIs.
3. Seleccione Imágenes públicas.
4. En Buscar AMI por atributo o etiqueta, busque una AMI con el nombre de la plantilla.

### Ejemplos

- Ejemplo de AMI para Slurm 24.11 en instancias Arm64

```
aws-pcs-sample_ami-amzn2-arm64-slurm-24.11
```

- Ejemplo de AMI para Slurm 24.11 en instancias x86

```
aws-pcs-sample_ami-amzn2-x86_64-slurm-24.11
```

#### Note

Si hay varios AMIs, utilice la AMI con la marca de tiempo más reciente.

5. Use el ID de AMI cuando cree o actualice un grupo de nodos de cómputo.

## AWS CLI

Puede encontrar el ejemplo más reciente de AMI de AWS PCS con los siguientes comandos. *region-code* Sustitúyala por la Región de AWS que utilices AWS PCS, por ejemplo `us-east-1`.

- x86\_64

```
aws ec2 describe-images --region region-code --owners amazon \  
--filters 'Name=name,Values=aws-pcs-sample_ami-amzn2-x86_64-slurm-24.11*' \  
          'Name=state,Values=available' \  
          'Name=architecture,Values=x86_64'
```

```
--query 'sort_by(Images, &CreationDate)[-1].[Name,ImageId]' --output text
```

- Arm64

```
aws ec2 describe-images --region region-code --owners amazon \  
--filters 'Name=name,Values=aws-pcs-sample_ami-amzn2-arm64-slurm-24.11*' \  
          'Name=state,Values=available' \  
--query 'sort_by(Images, &CreationDate)[-1].[Name,ImageId]' --output text
```

Use el ID de AMI cuando cree o actualice un grupo de nodos de cómputo.

## Obtenga más información sobre el ejemplo de AWS PCS AMIs

Para ver el contenido y los detalles de configuración de las versiones actuales y anteriores del ejemplo de AWS PCS AMIs, consulte [Notas de publicación para un ejemplo de AWS PCS AMIs](#).

## Cree la suya propia AMIs compatible con AWS PCS

Para obtener información sobre cómo crear uno propio AMIs que funcione con AWS PCS, consulte [Imágenes personalizadas de Amazon Machine \(AMIs\) para AWS PCS](#).

## Imágenes personalizadas de Amazon Machine (AMIs) para AWS PCS

AWS El PCS está diseñado para funcionar con Amazon Machine Images (AMI) que usted incorpore al servicio. AMIs Pueden tener instalados software y configuraciones arbitrarios, siempre que tengan el agente AWS PCS y una versión compatible de Slurm instalados y configurados correctamente. Debe utilizar los AWS instaladores proporcionados para instalar el software AWS PCS en su AMI personalizada. Le recomendamos que utilice los AWS instaladores proporcionados para instalar Slurm en su AMI personalizada, pero puede instalar Slurm por su cuenta si lo prefiere (no se recomienda).

### Note

Si quiere probar AWS PCS sin crear una AMI personalizada, puede utilizar un ejemplo de AMI proporcionado por AWS. Para obtener más información, consulte [Uso de Amazon Machine Images \(AMIs\) de muestra con AWS PCS](#).

Este tutorial le ayuda a crear una AMI que se pueda usar con grupos de nodos de cómputo de PCS para impulsar sus cargas de trabajo de HPC e AI/ML.

## Temas

- [Paso 1: Lanzar una instancia temporal](#)
- [Paso 2: Instalar el agente AWS PCS](#)
- [Paso 3: Instalar Slurm](#)
- [Paso 4: \(opcional\) Instalar controladores, bibliotecas y software de aplicación adicionales](#)
- [Paso 5: Crear una AMI compatible con AWS PCS](#)
- [Paso 6: Utilice la AMI personalizada con un grupo de nodos de cómputo de AWS PCS](#)
- [Paso 7: Finalizar la instancia temporal](#)

## Paso 1: Lanzar una instancia temporal

Lance una instancia temporal que pueda usar para instalar y configurar el software AWS PCS y el programador Slurm. Esta instancia se utiliza para crear una AMI compatible con AWS PCS.

Para iniciar una instancia temporal

1. Abra la [EC2 consola de Amazon](#).
2. En el panel de navegación, selecciona Instances y, a continuación, selecciona Launch instances para abrir el asistente de nuevas instancias de lanzamiento.
3. (Opcional) En la sección Nombre y etiquetas, proporciona un nombre para la instancia, por ejemplo PCS-AMI-instance. El nombre se asigna a la instancia como etiqueta de recurso (Name=PCS-AMI-instance).
4. En la sección Application and OS Images (Imágenes de aplicaciones y sistema operativo), seleccione una AMI para uno de los [sistemas operativos compatibles](#).
5. En la sección Tipo de instancia, seleccione el [tipo de instancia admitida](#).
6. En la sección Par de claves, seleccione el par de claves que desea utilizar en la instancia.
7. En la sección Configuración de red:
  - En Firewall (grupos de seguridad), selecciona Seleccionar un grupo de seguridad existente y, a continuación, selecciona un grupo de seguridad que permita el acceso SSH entrante a la instancia.

8. En la sección Almacenamiento, configure los volúmenes según sea necesario. Asegúrese de configurar suficiente espacio para instalar sus propias aplicaciones y bibliotecas.
9. En el panel Resumen, elija Iniciar instancia.

## Paso 2: Instalar el agente AWS PCS

Instale el agente que configura las instancias lanzadas por AWS PCS para su uso con Slurm. Para obtener más información sobre el agente AWS PCS, consulte [AWS Versiones del agente PCS](#)

### Para instalar el agente AWS PCS

1. Conéctese a la instancia que lanzó. Para obtener más información, consulte [Conexión con la instancia de Linux](#).
2. (Opcional) Para asegurarse de que todos los paquetes de software estén actualizados, realice una actualización rápida del software de la instancia. Este proceso puede demorar unos minutos.
  - Amazon Linux 2, RHEL 9, Rocky Linux 9

```
sudo yum update -y
```

- Ubuntu 22.04

```
sudo apt-get update && sudo apt-get upgrade -y
```

3. Reinicie la instancia y vuelva a conectarse a ella.
4. Descargue los archivos de instalación del agente AWS PCS. Los archivos de instalación se empaquetan en un archivo tarball (`.tar.gz`) comprimido. Para descargar la última versión estable, utilice el comando siguiente. *region* Sustitúyala por la ubicación Región de AWS en la que lanzaste la instancia temporal, por ejemplo. `us-east-1`

```
curl https://aws-pcs-repo-region.s3.amazonaws.com/aws-pcs-agent/aws-pcs-agent-v1.2.0-1.tar.gz -o aws-pcs-agent-v1.2.0-1.tar.gz
```

También puede obtener la última versión sustituyendo el número de versión por `latest` el del comando anterior (por ejemplo: `aws-pcs-agent-v1-latest.tar.gz`).

 Note

Esto podría cambiar en futuras versiones del software del agente AWS PCS.

5. (Opcional) Compruebe la autenticidad e integridad del archivo tar del software del AWS PCS. Le recomendamos que lo haga para verificar la identidad del editor de software y para verificar que el archivo no se haya modificado ni dañado desde que se publicó.

- a. Descarga la clave GPG pública para AWS PCS e impórtala a tu conjunto de claves. *region* Sustitúyala por la Región de AWS ubicación en la que lanzaste la instancia temporal. El comando debe devolver un valor de clave. Registre el valor clave y utilícelo en el siguiente paso.

```
wget https://aws-pcs-repo-public-keys-region.s3.amazonaws.com/aws-pcs-public-key.pub && \  
  gpg --import aws-pcs-public-key.pub
```

- b. Ejecuta el siguiente comando para verificar la huella digital de la clave GPG.

```
gpg --fingerprint 7EEF030EDDF5C21C
```

El comando debería devolver una huella digital idéntica a la siguiente:

```
1C24 32C1 862F 64D1 F90A 239A 7EEF 030E DDF5 C21C
```

 Important

No ejecute el script de instalación del agente AWS PCS si la huella digital no coincide. Contacte con [AWS Support](#).

- c. Descargue el archivo de firma y verifique la firma del archivo tar del software AWS PCS. *region* Sustitúyalo por el Región de AWS lugar donde lanzaste la instancia temporal, por ejemplo. us-east-1

```
wget https://aws-pcs-repo-region.s3.amazonaws.com/aws-pcs-agent/aws-pcs-agent-v1.2.0-1.tar.gz.sig && \  
  gpg --verify ./aws-pcs-agent-v1.2.0-1.tar.gz.sig
```

El resultado debería ser similar al siguiente:

```
gpg: assuming signed data in './aws-pcs-agent-v1.2.0-1.tar.gz'  
gpg: Signature made Fri Dec 13 18:50:19 2024 CEST  
gpg:                using RSA key 4BAA531875430EB0739E6D961BA7F0AF6E34C496  
gpg: Good signature from "AWS PCS Packages (AWS PCS Packages)" [unknown]  
gpg: WARNING: This key is not certified with a trusted signature!  
gpg:                There is no indication that the signature belongs to the owner.  
Primary key fingerprint: 1C24 32C1 862F 64D1 F90A 239A 7EEF 030E DDF5 C21C  
Subkey fingerprint: 4BAA 5318 7543 0EB0 739E 6D96 1BA7 F0AF 6E34 C496
```

Si el resultado incluye Good signature y la huella digital coincide con la huella digital devuelta en el paso anterior, continúe con el paso siguiente.

 Important

No ejecute el script de instalación del software AWS PCS si la huella digital no coincide. Contacte con [AWS Support](#).

6. Extraiga los archivos del .tar.gz archivo comprimido y navegue hasta el directorio extraído.

```
tar -xf aws-pcs-agent-v1.2.0-1.tar.gz && \  
cd aws-pcs-agent
```

7. Instale el software AWS PCS.

```
sudo ./installer.sh
```

8. Compruebe el archivo de versión del software AWS PCS para confirmar que la instalación se ha realizado correctamente.

```
cat /opt/aws/pcs/version
```

El resultado debería ser similar al siguiente:

```
AGENT_INSTALL_DATE='Fri Dec 13 12:28:43 UTC 2024'  
AGENT_VERSION='1.2.0'  
AGENT_RELEASE='1'
```

## Paso 3: Instalar Slurm

Instale una versión de Slurm que sea compatible con el PCS. AWS Para obtener más información, consulte [Versiones Slurm en PCS AWS](#).

### Note

Si tiene una AMI con una versión anterior del software Slurm instalada, debe realizar los siguientes pasos para instalar la nueva versión de Slurm. El agente AWS PCS habilita la versión correcta de los binarios de Slurm en tiempo de ejecución, de acuerdo con la versión de Slurm configurada en el momento de la creación del clúster.

Para instalar Slurm

1. Conéctese a la misma instancia temporal en la que instaló el software AWS PCS.
2. Descargue el software de instalación de Slurm. El instalador de Slurm está empaquetado en un archivo tarball () comprimido. `.tar.gz` Para descargar la última versión estable, utilice el comando siguiente. *region*Sustitúyalo por el Región de AWS de su instancia temporal, por ejemplo. `us-east-1`

```
curl https://aws-pcs-repo-region.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz \
-o aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz
```

También puede obtener la última versión sustituyendo el número de versión por `latest` el del comando anterior (por ejemplo: `aws-pcs-slurm-24.11-installer-latest.tar.gz`).

### Note

Esto podría cambiar en futuras versiones del software de instalación de Slurm.

3. (Opcional) Compruebe la autenticidad e integridad del archivo tar del instalador de Slurm. Le recomendamos que lo haga para verificar la identidad del editor de software y para verificar que el archivo no se haya modificado ni dañado desde que se publicó.
  - a. Descarga la clave GPG pública para AWS PCS e impórtala a tu conjunto de claves. *region*Sustitúyala por la Región de AWS ubicación en la que lanzaste la instancia

temporal. El comando debe devolver un valor de clave. Registre el valor clave y utilícelo en el siguiente paso.

```
wget https://aws-pcs-repo-public-keys-region.s3.amazonaws.com/aws-pcs-public-key.pub && \
  gpg --import aws-pcs-public-key.pub
```

- b. Ejecuta el siguiente comando para verificar la huella digital de la clave GPG.

```
gpg --fingerprint 7EEF030EDDF5C21C
```

El comando debería devolver una huella digital idéntica a la siguiente:

```
1C24 32C1 862F 64D1 F90A 239A 7EEF 030E DDF5 C21C
```

**⚠ Important**

No ejecute el script de instalación de Slurm si la huella digital no coincide. Contacte con [AWS Support](#).

- c. Descargue el archivo de firma y verifique la firma del archivo tarball del instalador de Slurm. *region* Sustitúyalo por el Región de AWS lugar en el que lanzaste la instancia temporal, por ejemplo. us-east-1

```
wget https://aws-pcs-repo-region.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz.sig && \
  gpg --verify ./aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz.sig
```

El resultado debería ser similar al siguiente:

```
gpg: assuming signed data in './aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz'
gpg: Signature made Wed May 14 14:23:38 2025 UTC
gpg:                using RSA key 4BAA531875430EB0739E6D961BA7F0AF6E34C496
gpg: Good signature from "AWS PCS Packages (AWS PCS Packages)" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:                There is no indication that the signature belongs to the owner.
Primary key fingerprint: 1C24 32C1 862F 64D1 F90A 239A 7EEF 030E DDF5 C21C
Subkey fingerprint: 4BAA 5318 7543 0EB0 739E 6D96 1BA7 F0AF 6E34 C496
```

Si el resultado incluye `Good signature` y la huella digital coincide con la huella digital devuelta en el paso anterior, continúe con el paso siguiente.

**⚠ Important**

No ejecute el script de instalación de Slurm si la huella digital no coincide. Contacte con [AWS Support](#).

4. Extraiga los archivos desde el archivo `.tar.gz` comprimido y acceda al directorio extraído.

```
tar -xf aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz && \  
cd aws-pcs-slurm-24.11-installer
```

5. Instala Slurm. El instalador descarga, compila e instala Slurm y sus dependencias. Tarda varios minutos, según las especificaciones de la instancia temporal que haya seleccionado.

```
sudo ./installer.sh -y
```

6. Compruebe el archivo de versión del programador para confirmar la instalación.

```
cat /opt/aws/pcs/scheduler/slurm-24.11/version
```

El resultado debería ser similar al siguiente:

```
SLURM_INSTALL_DATE='Wed May 14 14:23:38 UTC 2025'  
SLURM_VERSION='24.11.5'  
PCS_SLURM_RELEASE='1'
```

## Paso 4: (opcional) Instalar controladores, bibliotecas y software de aplicación adicionales

Instale controladores, bibliotecas y software de aplicación adicionales en la instancia temporal. Los procedimientos de instalación variarán en función de las aplicaciones y bibliotecas específicas. Si no ha creado una AMI personalizada para AWS PCS anteriormente, le recomendamos que primero cree y pruebe una AMI solo con el software de AWS PCS y Slurm instalados y, a continuación, añada gradualmente su propio software y configuraciones una vez que haya confirmado el éxito inicial.

## Ejemplos

- Software Elastic Fabric Adapter (EFA). Para [obtener más información, consulte Introducción a EFA y MPI para cargas de trabajo de HPC en Amazon EC2 en](#) la Guía del usuario de Amazon Elastic Compute Cloud.
- Cliente Amazon Elastic File System (Amazon EFS). Para obtener más información, consulte [Instalación manual del cliente Amazon EFS](#) en la Guía del usuario de Amazon Elastic File System.
- Cliente Lustre, para usar Amazon FSx for Lustre y Amazon File Cache. Para obtener más información, consulte [Instalación del cliente de Lustre](#) en la Guía del usuario FSx de Lustre.
- CloudWatch Agente de Amazon, para usar CloudWatch Logs and Metrics. Para obtener más información, consulte [Instalar el CloudWatch agente](#) en la Guía del CloudWatch usuario de Amazon.
- AWS Neuron, para usar los tipos de instancia trn\* e inf\*. [Para obtener más información, consulte la documentación de Neuron.AWS](#)
- Controlador NVIDIA, CUDA y DCGM para usar los tipos de instancia p\* o g\*.

## Paso 5: Crear una AMI compatible con AWS PCS

Una vez instalados los componentes de software necesarios, crea una AMI que puede reutilizar para lanzar instancias en grupos de nodos de cómputo de AWS PCS.

Para crear una AMI desde la instancia temporal

1. Abre la [EC2 consola de Amazon](#).
2. En el panel de navegación, seleccione Instances (Instancias).
3. Selecciona la instancia temporal que has creado. Selecciona Acciones, Imagen y Crear imagen.
4. En Crear imagen, realice lo siguiente:
  - a. En Nombre de imagen, ingrese un nombre descriptivo para la AMI.
  - b. (Opcional) En Descripción de imagen, ingrese una breve descripción del propósito la AMI.
  - c. Elija Crear imagen.
5. En el panel de navegación, elija AMIs.
6. Busque la AMI que creó en la lista. Espere a que su estado cambie de Pendiente a Disponible y, a continuación, utilícela con un grupo de nodos de cómputo de AWS PCS.

## Paso 6: Utilice la AMI personalizada con un grupo de nodos de cómputo de AWS PCS

Puede usar su AMI personalizada con un grupo de nodos de cómputo de AWS PCS nuevo o existente.

### New compute node group

Para usar la AMI personalizada

1. Abra la [consola AWS PCS](#).
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. Elija el clúster en el que utilizará la AMI personalizada y, a continuación, seleccione Compute node groups.
4. Cree un nuevo grupo de nodos de procesamiento. Para obtener más información, consulte [Creación de un grupo de nodos de cómputo en AWS PCS](#). En ID de AMI, busque el nombre o la ID de la AMI personalizada que desee usar. Termine de configurar el grupo de nodos de cómputo y, a continuación, seleccione Crear grupo de nodos de cómputo.
5. (Opcional) Confirme que la AMI admite el lanzamiento de instancias. Lanza una instancia en el grupo de nodos de cómputo. Para ello, configura el grupo de nodos de cómputo para que tenga una única instancia estática, o puedes enviar un trabajo a una cola que utilice el grupo de nodos de cómputo.
  - a. Comprueba la EC2 consola de Amazon hasta que aparezca una instancia etiquetada con el nuevo ID de grupo de nodos de cómputo. Para obtener más información al respecto, consulta [Búsqueda de instancias de grupos de nodos de cómputo en AWS PCS](#).
  - b. Cuando veas que una instancia se lanza y completa su proceso de arranque, confirma que usa la AMI esperada. Para ello, selecciona la instancia y, a continuación, inspecciona el ID de AMI en Detalles. Debe coincidir con la AMI que configuró en la configuración del grupo de nodos de cómputo.
  - c. (Opcional) Actualice la configuración de escalado del grupo de nodos de cómputo a sus valores preferidos.

## Existing compute node group

Para usar la AMI personalizada

1. Abra la [consola AWS PCS](#).
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. Elija el clúster en el que utilizará la AMI personalizada y, a continuación, seleccione Compute node groups.
4. Seleccione el grupo de nodos que desee configurar y elija Editar. En ID de AMI, busque el nombre o la ID de la AMI personalizada que desee usar. Termine de configurar el grupo de nodos de procesamiento y, a continuación, seleccione Actualizar. Las nuevas instancias lanzadas en el grupo de nodos de procesamiento utilizarán el ID de AMI actualizado. Las instancias existentes seguirán utilizando la AMI anterior hasta que AWS PCS las sustituya. Para obtener más información, consulte [Actualización de un grupo de nodos de cómputo AWS PCS](#).
5. (Opcional) Confirme que la AMI admite el lanzamiento de instancias. Lanza una instancia en el grupo de nodos de cómputo. Para ello, configura el grupo de nodos de cómputo para que tenga una única instancia estática, o puedes enviar un trabajo a una cola que utilice el grupo de nodos de cómputo.
  - a. Comprueba la EC2 consola de Amazon hasta que aparezca una instancia etiquetada con el nuevo ID de grupo de nodos de cómputo. Para obtener más información al respecto, consulta [Búsqueda de instancias de grupos de nodos de cómputo en AWS PCS](#).
  - b. Cuando veas que una instancia se lanza y completa su proceso de arranque, confirma que usa la AMI esperada. Para ello, selecciona la instancia y, a continuación, inspecciona el ID de AMI en Detalles. Debe coincidir con la AMI que configuró en la configuración del grupo de nodos de cómputo.
  - c. (Opcional) Actualice la configuración de escalado del grupo de nodos de cómputo a sus valores preferidos.

## Paso 7: Finalizar la instancia temporal

Una vez que haya confirmado que su AMI funciona según lo previsto con AWS PCS, puede cancelar la instancia temporal para dejar de incurrir en cargos por ella.

Para finalizar la instancia temporal

1. Abra la [EC2 consola de Amazon](#).
2. En el panel de navegación, seleccione Instancias (Instancia[s]).
3. Seleccione la instancia temporal que ha creado y seleccione Acciones, Estado de la instancia y Finalizar instancia.
4. Cuando se le pida que confirme, elija Finalizar.

## Instaladores de software para crear PCS personalizados AMIs AWS

AWS proporciona un archivo descargable que puede instalar el software AWS PCS en una instancia. AWS también proporciona software que puede descargar, compilar e instalar las versiones pertinentes de Slurm y sus dependencias. Puede usar estas instrucciones para crear una versión personalizada AMIs para su uso con AWS PCS o puede usar sus propios métodos.

Contenido

- [AWS Instalador del software PCS Agent](#)
- [Instalador de Slurm](#)
- [Sistemas operativos compatibles](#)
- [Tipos de instancias admitidas](#)
- [Versiones de Slurm compatibles](#)
- [Verifique los instaladores mediante una suma de verificación](#)

### AWS Instalador del software PCS Agent

El instalador del software del agente AWS PCS configura una instancia para que funcione con el AWS PCS durante el proceso de arranque de la instancia. Debe utilizar los AWS instaladores proporcionados para instalar el agente AWS PCS en la AMI personalizada.

Para obtener más información sobre el software del agente AWS PCS, consulte [AWS Versiones del agente PCS](#)

## Instalador de Slurm

El instalador de Slurm descarga, compila e instala las versiones relevantes de Slurm y sus dependencias. Puede usar el instalador de Slurm para crear versiones personalizadas para PCS. AMIs AWS También puede utilizar sus propios mecanismos si son coherentes con la configuración de software que proporciona el instalador de Slurm. Para obtener más información sobre la compatibilidad de AWS PCS con Slurm, consulte. [Versiones Slurm en PCS AWS](#)

El software AWS suministrado instala lo siguiente:

- [Utilice la versión principal y de mantenimiento solicitada \(actualmente la versión 24.11.x\): licencia GPL 2](#)
  - Slurm está construido con un conjunto de `--sysconfdir /etc/slurm`
  - Slurm está diseñado con la opción y `--enable-pam --without-munge`
  - Slurm se construye con la opción `--sharedstatedir=/run/slurm/`
  - Slurm está construido con soporte para PMIX y JWT
  - Slurm está instalado en `/opt/aws/pcs/schedulers/slurm-24.11`
- [OpenPMix \(versión 4.2.6\) — Licencia](#)
  - OpenPMIX se instala como un subdirectorío de `/opt/aws/pcs/scheduler/`
- [libjwt \(versión 1.17.0\) — Licencia MPL-2.0](#)
  - libjwt se instala como un subdirectorío de `/opt/aws/pcs/scheduler/`

El software AWS suministrado cambia la configuración del sistema de la siguiente manera:

- El `systemd` archivo Slurm creado por la compilación se copia `/etc/systemd/system/` con el nombre del archivo. `slurmd-24.11.service`
- Si no existen, se crean un usuario y un grupo de Slurm (`slurm:slurm`) con un UID/GID de. 401
- En Amazon Linux 2 y Rocky Linux 9, la instalación añade el repositorio EPEL para instalar el software necesario para compilar Slurm o sus dependencias.
- Durante RHEL9 la instalación, se habilitará `codeready-builder-for-rhel-9-rhui-rpms` y `epel-release-latest-9` se instalará el software necesario `fedoraproject` para compilar Slurm o sus dependencias.

## Sistemas operativos compatibles

El software AWS PCS y los instaladores de Slurm son compatibles con los siguientes sistemas operativos:

- Amazon Linux 2
- RedHat Linux empresarial 9
- Rocky Linux 9
- Ubuntu 22.04

Para obtener más información, consulte [Sistemas operativos compatibles en AWS PCS](#).

### Note

AWS Deep Learning AMIs Las versiones (DLAMI) basadas en Amazon Linux 2 y Ubuntu 22.04 deben ser compatibles con el software PCS y los instaladores de AWS Slurm. Para obtener más información, consulte [Cómo elegir su DLAMI](#) en AWS Deep Learning AMIs la Guía para desarrolladores.

## Tipos de instancias admitidas

AWS El software PCS y los instaladores de Slurm admiten cualquier tipo de instancia x86\_64 o arm64 que pueda ejecutar uno de los sistemas operativos compatibles.

## Versiones de Slurm compatibles

Se admiten las siguientes versiones principales de Slurm:

- Slurm 24.11
- Slurm 24.05
- Slurm 23.11

Para obtener más información, consulte [Versiones Slurm en PCS AWS](#).

## Verifique los instaladores mediante una suma de verificación

Puede utilizar SHA256 sumas de comprobación para comprobar los archivos tar (.tar.gz) del instalador. Le recomendamos que lo haga para verificar la identidad del editor de software y para comprobar que la aplicación no se ha modificado ni dañado desde que se publicó.

Para verificar un tarball

Utilice la utilidad sha256sum para la suma de SHA256 comprobación y especifique el nombre del archivo tarball. Debe ejecutar el comando desde el directorio en el que guardó el archivo tarball.

- SHA256

```
$ sha256sum tarball_filename.tar.gz
```

El comando debe devolver un valor de suma de comprobación con el siguiente formato.

```
checksum_value tarball_filename.tar.gz
```

Compare el valor de la suma de verificación devuelto por el comando con el valor de la suma de verificación que se proporciona en la siguiente tabla. Si las sumas de comprobación coinciden, es seguro ejecutar el script de instalación.

### Important

Si las sumas de comprobación no coinciden, no ejecute el script de instalación. Ponte en contacto con [Soporte](#).

Por ejemplo, el siguiente comando genera la SHA256 suma de comprobación del tarball Slurm 24.11.5-1.

```
$ sha256sum aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz
```

Ejemplo de salida:

```
593efe4d66bef2f3e46d5a382fb5a32f7a3ca2510bcf1b3c85739f4f951810d5 aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz
```

En las tablas siguientes se muestran las sumas de comprobación de las versiones recientes de los instaladores. *us-east-1* Sustitúyalo por el Región de AWS lugar en el que utilice PCS AWS .

### AWS Agente de PCS

Installer (Instalador)	Descargar URL	SHA256 suma de control
AWS Agente PCS 1.2.0-1	<code>https://aws-pcs-repo-<i>us-east-1</i>.s3.amazonaws.com/aws-pcs-agent/aws-pcs-agent-v1.2.0-1.tar.gz</code>	470db8c4fc9e50277b6317f98584b6b547e73523043e34f018eeca e767846805
AWS Agente PCS 1.1.1-1	<code>https://aws-pcs-repo-<i>us-east-1</i>.s3.amazonaws.com/aws-pcs-agent/aws-pcs-agent-v1.1.1-1.tar.gz</code>	bef078bf60a6d8ecde2e6c49cd34d088703f02550279e3bf483d57a235334dc6
AWS Agente PCS 1.1.0-1	<code>https://aws-pcs-repo-<i>us-east-1</i>.s3.amazonaws.com/aws-pcs-agent/aws-pcs-agent-v1.1.0-1.tar.gz</code>	594c32194c71bccc5d66e5213213ae38dd2c6d2f9a950bb01accea0bbab0873a
AWS Agente PCS 1.0.1-1	<code>https://aws-pcs-repo-<i>us-east-1</i>.s3.amazonaws.com/aws-pcs-agent/aws-pcs-agent-v1.0.1-1.tar.gz</code>	04e22264019837e3f42d8346daf5886eaaced21571742eb505ea8911786bcb2
AWS Agente PCS 1.0.0-1	<code>https://aws-pcs-repo-<i>us-east-1</i>.s3.amazonaws.com/aws-pcs-agent/aws-pcs-agent-v1.0.0-1.tar.gz</code>	d2d3d68d00c685435c38af471d7e2492dde5ce9eb222d7b6ef0042144b134ce0

## Instalador Slurm

Installer (Instalador)	Descargar URL	SHA256 suma de verificación
Slurm 24.11.5-1	<a href="https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz">https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-24.11-installer-24.11.5-1.tar.gz</a>	593efe4d66bef2f3e46d5a382fb5a32f7a3ca2510bcf1b3c85739f4f951810d5
Slurm 24.05.7-1	<a href="https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-24.05-installer-24.05.7-1.tar.gz">https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-24.05-installer-24.05.7-1.tar.gz</a>	0b5ed7c81195de2628c78f37c79e63fc4ae99132ca6b019b53a0d68792ee82c5
Slurm 24.05.5-2	<a href="https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-24.05-installer-24.05.5-2.tar.gz">https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-24.05-installer-24.05.5-2.tar.gz</a>	7cc8d8294f2fbff95fe0602cf9e21e02003b5d96c0730e0a18c6aa04c7a4967b
Slurm 23.11.10-3	<a href="https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-23.11-installer-23.11.10-3.tar.gz">https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-23.11-installer-23.11.10-3.tar.gz</a>	488a10ee0fbd57ec0e0ff7ea708a9e3038fafdc025c6bb391c75c2e2a7852a00
Slurm 23.11.10-2	<a href="https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-23.11-installer-23.11.10-2.tar.gz">https://aws-pcs-repo-us-east-1.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-23.11-installer-23.11.10-2.tar.gz</a>	0bbe85423305c05987931168caf98da08a34c25f9eec0690e8e74de0b7bc8752

Installer (Instalador)	Descargar URL	SHA256 suma de verificación
Slurm 23.11.10-1	<pre>https://aws-pcs-repo-<i>us-east-1</i>.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-23.11-installer-23.11.10-1.tar.gz</pre>	<pre>27e8faa9980e92cdfd8cfdc71f937777f0934552ce61e33dac4ecf5a20321e44</pre>
Slurm 23.11.9-1	<pre>https://aws-pcs-repo-<i>us-east-1</i>.s3.amazonaws.com/aws-pcs-slurm/aws-pcs-slurm-23.11-installer-23.11.9-1.tar.gz</pre>	<pre>1de7d919c8632fe8e2806611bed4fde1005a4fadc795412456e935c7bba2a9b8</pre>

## Notas de publicación para un ejemplo de AWS PCS AMIs

AMIs para las últimas versiones principales compatibles del programador, reciba actualizaciones de seguridad y correcciones de errores críticos. Estos parches de seguridad incrementales no se incluyen en las notas oficiales de la versión.

### Important

Los ejemplos AMIs relacionados con las versiones antiguas del programador no son compatibles y no reciben actualizaciones.

### Important

AMIs Los ejemplos son para fines de demostración y no se recomiendan para cargas de trabajo de producción.

## Contenido

- [AWS Ejemplo de PCS AMIs para x86\\_64 \(Amazon Linux 2\)](#)
- [AWS Ejemplo de PCS AMIs para Arm64 \(Amazon Linux 2\)](#)

## AWS Ejemplo de PCS AMIs para x86\_64 (Amazon Linux 2)

### Slurm 24.11

#### Note

AWS PCS admite la contabilidad de Slurm 24.11 y versiones posteriores. Para obtener más información, consulte [Contabilidad de barrios bajos en PCS AWS](#).

#### Nombre de la AMI

- `aws-pcs-sample_ami-amzn2-x86_64-slurm-24.11`

#### EC2 Instancias compatibles

- Todas las instancias con un procesador x86 de 64 bits. Para encontrar instancias compatibles, navega a la [EC2 consola de Amazon](#). Selecciona Tipos de instancia y, a continuación, busca `Architectures=x86_64`.

#### Contenido de AMI

- AWS Servicio compatible: AWS PCS
- Sistema operativo: Amazon Linux 2
- Arquitectura de cómputo: x86\_64
- Tipo de volumen de EBS: gp2
- Instalador de EFA: 1.33.0
- GDRCopy: 2.4
- Controlador NVIDIA: 550.127.08
- NVIDIA CUDA: 12.4.1\_550.54.15

### Slurm 24.05

#### Nombre de la AMI

- `aws-pcs-sample_ami-amzn2-x86_64-slurm-24.05`

## EC2 Instancias compatibles

- Todas las instancias con un procesador x86 de 64 bits. Para encontrar instancias compatibles, navega a la [EC2 consola de Amazon](#). Selecciona Tipos de instancia y, a continuación, buscaArchitectures=x86\_64.

### Contenido de AMI

- AWS Servicio compatible: AWS PCS
- Sistema operativo: Amazon Linux 2
- Arquitectura de cómputo: x86\_64
- Tipo de volumen de EBS: gp2
- Instalador de EFA: 1.33.0
- GDRCopy: 2.4
- Controlador NVIDIA: 550.127.08
- NVIDIA CUDA: 12.4.1\_550.54.15

### Slurm 23.11

#### Nombre de la AMI

- aws-pcs-sample\_ami-amzn2-x86\_64-slurm-23.11

## EC2 Instancias compatibles

- Todas las instancias con un procesador x86 de 64 bits. Para encontrar instancias compatibles, navega a la [EC2 consola de Amazon](#). Selecciona Tipos de instancia y, a continuación, buscaArchitectures=x86\_64.

### Contenido de AMI

- AWS Servicio compatible: AWS PCS
- Sistema operativo: Amazon Linux 2
- Arquitectura de cómputo: x86\_64
- Tipo de volumen de EBS: gp2

- Instalador de EFA: 1.33.0
- GDRCopy: 2.4
- Controlador NVIDIA: 550.127.08
- NVIDIA CUDA: 12.4.1\_550.54.15

## AWS Ejemplo de PCS AMIs para Arm64 (Amazon Linux 2)

Slurm 24.11

### Note

AWS PCS admite la contabilidad de Slurm 24.11 y versiones posteriores. Para obtener más información, consulte [Contabilidad de barrios bajos en PCS AWS](#).

Nombre de la AMI

- `aws-pcs-sample_ami-amzn2-arm64-slurm-24.11`

EC2 Instancias compatibles

- Todas las instancias con un procesador Arm de 64 bits. Para encontrar instancias compatibles, navega a la [EC2 consola de Amazon](#). Selecciona Tipos de instancia y, a continuación, busca `Architectures=arm64`.

Contenido de AMI

- AWS Servicio compatible: AWS PCS
- Sistema operativo: Amazon Linux 2
- Arquitectura de cómputo: arm64
- Tipo de volumen de EBS: gp2
- Instalador de EFA: 1.33.0
- GDRCopy: 2.4
- Controlador NVIDIA: 550.127.08

- NVIDIA CUDA: 12.4.1\_550.54.15

## Slurm 24.05

### Nombre de la AMI

- `aws-pcs-sample_ami-amzn2-arm64-slurm-24.05`

### EC2 Instancias compatibles

- Todas las instancias con un procesador Arm de 64 bits. Para encontrar instancias compatibles, navega a la [EC2 consola de Amazon](#). Selecciona Tipos de instancia y, a continuación, busca `Architectures=arm64`.

### Contenido de AMI

- AWS Servicio compatible: AWS PCS
- Sistema operativo: Amazon Linux 2
- Arquitectura de cómputo: arm64
- Tipo de volumen de EBS: gp2
- Instalador de EFA: 1.33.0
- GDRCopy: 2.4
- Controlador NVIDIA: 550.127.08
- NVIDIA CUDA: 12.4.1\_550.54.15

## Slurm 23.11

### Nombre de la AMI

- `aws-pcs-sample_ami-amzn2-arm64-slurm-23.11`

### EC2 Instancias compatibles

- Todas las instancias con un procesador Arm de 64 bits. Para encontrar instancias compatibles, navega a la [EC2 consola de Amazon](#). Selecciona Tipos de instancia y, a continuación, busca `Architectures=arm64`.

## Contenido de AMI

- AWS Servicio compatible: AWS PCS
- Sistema operativo: Amazon Linux 2
- Arquitectura de cómputo: arm64
- Tipo de volumen de EBS: gp2
- Instalador de EFA: 1.33.0
- GDRCopy: 2.4
- Controlador NVIDIA: 550.127.08
- NVIDIA CUDA: 12.4.1\_550.54.15

# Sistemas operativos compatibles en AWS PCS

AWS PCS usa la Amazon Machine Image (AMI) configurada para un grupo de nodos de cómputo para lanzar EC2 instancias en ese grupo de nodos de cómputo. La AMI determina el sistema operativo que utilizan las EC2 instancias. No se puede cambiar el sistema operativo en el ejemplo de AWS PCS AMIs. Debe crear una AMI personalizada si desea utilizar un sistema operativo diferente. Para obtener más información, consulte [Amazon Machine Images \(AMIs\) para AWS PCS](#).

## Sistemas operativos compatibles

- Amazon Linux 2

Este es el sistema operativo del ejemplo de AWS PCS AMIs.

### Important

AMIs Los ejemplos son para fines de demostración y no se recomiendan para cargas de trabajo de producción. Debe crear y usar una AMI personalizada para las cargas de trabajo de producción, incluso si piensa usar Amazon Linux 2.

- RedHat Linux empresarial 9 (RHEL 9)

El coste bajo demanda de cualquier tipo de instancia de RHEL es superior al de otros sistemas operativos compatibles. Para obtener más información sobre los precios, consulte [Precios bajo demanda](#) y [¿Cómo se ofrece y se cotiza Red Hat Enterprise Linux en Amazon Elastic Compute Cloud?](#).

- Rocky Linux 9

Puedes usar el [Rocky Linux 9 oficial AMIs](#) como base para una AMI personalizada. La compilación de la AMI personalizada podría fallar si la AMI base no tiene el núcleo más reciente.

Para actualizar el núcleo

1. Lance una instancia con un ID de AMI de rocky9 desde aquí: <https://rockylinux.org/cloud-images/>
2. Inicie sesión en la instancia y ejecute el comando siguiente:

```
sudo yum -y update
```

3. Cree una imagen a partir de la instancia. Especifique esta imagen como imagen ParentImage para su AMI personalizada.
- Ubuntu 22.04

Ubuntu 22.04 requiere claves más seguras para SSH y no admite claves RSA de forma predeterminada. Te recomendamos que generes y utilices una ED25519 clave en su lugar.

 Note

No puedes actualizar Ubuntu 22.04 a la última versión del núcleo porque no hay un FSx cliente para ese núcleo.

## AWS Versiones del agente PCS

El software del agente AWS PCS configura las EC2 instancias que AWS PCS lanza para usarlas con Slurm. El agente se incluye en una Amazon Machine Images (AMI) que se especifica al crear grupos de nodos de procesamiento para el clúster. Las EC2 instancias lanzadas en esos grupos de nodos de cómputo utilizan la AMI especificada y el software de agente AWS PCS incluido. El agente AWS PCS permite que una EC2 instancia se registre como parte del clúster. Para utilizar el software de agente de AWS PCS más reciente, debe actualizar su versión personalizada AMIs. Para obtener más información, consulta [Paso 2: Instalar el agente AWS PCS](#) en [Imágenes personalizadas de Amazon Machine \(AMIs\) para AWS PCS](#).

AWS Versión del agente de PCS	Fecha de publicación	Notas de la versión
v1.2.0-1	7 de marzo de 2025	<ul style="list-style-type: none"> <li>• Soporte habilitado para IPv6 <code>in slurmd.conf</code> .</li> </ul>
v1.1.1-1	13 de diciembre de 2024	<ul style="list-style-type: none"> <li>• Se ha corregido un error que provocaba que en la llamada a <code>se informara de una versión incorrecta de Slurm. RegisterC omputeNodeGroupInstance</code></li> <li>• Se ha corregido un problema por el que los metadatos de la instancia no se recuperaban correctamente si se ejecutaba un script personalizado. <code>/opt/aws/pcs/etc/bootstrap_hooks/</code></li> </ul>
v1.1.0-1	6 de diciembre de 2024	<ul style="list-style-type: none"> <li>• Se habilitó la ejecución de scripts personalizados antes <code>/opt/aws/pcs/etc/b</code></li> </ul>

AWS Versión del agente de PCS	Fecha de publicación	Notas de la versión
		ootstrap_hooks/ de los pasos de arranque.
v1.0.1-1	22 de octubre de 2024	<ul style="list-style-type: none"><li>Se ha corregido un problema que provocaba que los dispositivos NVIDIA no funcionaran cuando se <code>slurmd</code> iniciaban en instancias con GPU habilitada.</li></ul>
v1.0.0-1	28 de agosto de 2024	<ul style="list-style-type: none"><li>Versión inicial.</li></ul>

## Versiones Slurm en PCS AWS

SchedMD mejora continuamente Slurm con nuevas capacidades, optimizaciones y parches de seguridad. SchedMD lanza una nueva versión principal a [intervalos regulares](#) y planea admitir hasta 3 versiones en un momento dado. AWS El PCS está diseñado para actualizar automáticamente el controlador Slurm con versiones de parches.

Cuando SchedMD deja de dar [soporte a](#) una versión principal en particular, AWS PCS también deja de dar soporte a esa versión principal. AWS PCS envía un aviso anticipado si una versión principal de Slurm está cerca del final de su vida útil, para que los clientes sepan cuándo actualizar sus clústeres a una versión compatible más reciente.

Le recomendamos que utilice la última versión compatible de Slurm para implementar su clúster y acceder a los avances y mejoras más recientes.

## Versiones de Slurm compatibles en PCS AWS

La siguiente tabla muestra las versiones de Slurm compatibles y las fechas e información importantes de cada versión.

Versión Slurm	Fecha de lanzamiento de SchedMD	AWS Fecha de lanzamiento de PCS	Fecha de finalización del soporte de AWS PCS	Versión mínima compatible del agente de AWS PCS	Ejemplo de AWS PCS compatible AMIs
24.11	29/11/2024	14/05/2025	31/05/2026	1.0.0-1	<ul style="list-style-type: none"> <li>aws- pcs-s ample_ami -amzn2- x86_64- slur m-24.11</li> <li>aws- pcs-s ample_ami</li> </ul>

Versión Slurm	Fecha de lanzamiento de SchedMD	AWS Fecha de lanzamiento de PCS	Fecha de finalización del soporte de AWS PCS	Versión mínima compatible del agente de AWS PCS	Ejemplo de AWS PCS compatible AMIs
					-amzn2-arm64-slurm-24.11
24,05	30/05/2024	18/12/2024	30/11/2025	1,00-1	<ul style="list-style-type: none"> <li>• aws-pcs-s ample_ami -amzn2-x86_64-slurm-24.05</li> <li>• aws-pcs-s ample_ami -amzn2-arm64-slurm-24.05</li> </ul>

Versión Slurm	Fecha de lanzamiento de SchedMD	AWS Fecha de lanzamiento de PCS	Fecha de finalización del soporte de AWS PCS	Versión mínima compatible del agente de AWS PCS	Ejemplo de AWS PCS compatible AMIs
23,11	21/11/2023	28/8/2024	31/05/2025	1.0,0-1	<ul style="list-style-type: none"> <li>aws-pcs-s ample_ami-amzn2-x86_64-slurm-23.11</li> <li>aws-pcs-s ample_ami-amzn2-arm64-slurm-23.11</li> </ul>

## Notas de publicación de las versiones de Slurm en PCS AWS

En este tema se describen los cambios importantes de cada versión de Slurm actualmente compatible con el PCS. AWS Le recomendamos que revise los cambios entre la versión antigua y la nueva cuando actualice el clúster.

### Slurm 24.11

#### Cambios implementados en el PCS AWS

- AWS PCS admite la contabilidad de Slurm. Para obtener más información, consulte [Contabilidad de barrios bajos en PCS AWS](#).

Para obtener más información sobre Slurm 24.11, consulte las siguientes publicaciones:

- [Anuncio de lanzamiento de SchedMD](#)
- [Notas de lanzamiento de SchedMD](#)

## Slurm 24.05

### Cambios implementados en el PCS AWS

- El nuevo módulo Slurm Step Manager ahora está activado por defecto en AWS el PCS. Este módulo ofrece importantes ventajas al transferir la gestión por pasos del controlador central a los nodos de cómputo, lo que mejora sustancialmente la simultaneidad del sistema en entornos con un uso intensivo de pasos. Para admitir esta configuración y aislar Prolog y Epilog procesar mejor los procesos, están habilitados los nuevos indicadores de prólogo (Contain,Alloc).
- La comunicación jerárquica entre el controlador y los nodos de cómputo permite optimizar la comunicación entre los nodos de Slurm, lo que mejora la escalabilidad y el rendimiento. Además, la configuración de enrutamiento ahora usa listas de nodos de partición para las comunicaciones desde el controlador, en lugar del algoritmo de enrutamiento predeterminado del complemento, lo que mejora la resiliencia del sistema.
- Un nuevo complemento de hash HashPlugin=hash/sha3 reemplaza al anteriorhash/k12 plugin. Ahora está activado de forma predeterminada en los clústeres de AWS PCS.
- Los registros del controlador Slurm ahora incluyen capacidades de auditoría mejoradas para todas las llamadas entrantes a procedimientos remotos (RPC). slurmctld Los registros incluyen la dirección de origen, el usuario autenticado y el tipo de RPC antes del procesamiento de la conexión.

Para obtener más información sobre Slurm 24.05, consulte las siguientes publicaciones:

- [Anuncio de lanzamiento de SchedMD](#)
- [Notas de lanzamiento de SchedMD](#)

## Slurm 23.11

### La configuración de Slurm se puede cambiar en PCS AWS

- El SuspendTime valor predeterminado es. 60 Utilice el parámetro de scaleDownIdleTimeInSeconds configuración AWS PCS para configurarlo. Para obtener

más información, consulte el [scaleDownIdleTimeInSeconds](#) parámetro del tipo de `ClusterSlurmConfiguration` datos en la referencia de la API de AWS PCS.

- El `MaxJobCount` y `MaxArraySize` se basa en el tamaño que elija para el clúster. Para obtener más información, consulte el [size](#) parámetro de la acción de la `CreateCluster` API en la referencia de la API de AWS PCS.
- La configuración predeterminada de `SelectTypeParameters` Slurm es. `CR_CPU` Puede proporcionarlo como un valor para configurarlo `slurmCustomSettings` al crear un clúster. Para obtener más información, consulte el [slurmCustomSettings](#) parámetro de la acción de la `CreateCluster` API y [SlurmCustomSetting](#) en la Referencia de la API de AWS PCS.
- Puede configurar `Prolog` y `Epilog` a nivel de clúster. Puede proporcionarlo como un valor `slurmCustomSettings` para configurarlo al crear un clúster. Para obtener más información, consulte [CreateCluster](#) y [SlurmCustomSetting](#) en la referencia de la API de AWS PCS.
- Puede configurar `Weight` y `RealMemory` a nivel de grupo de nodos de cómputo. Puede proporcionarlo como un valor para configurarlo `slurmCustomSettings` al crear un grupo de nodos de procesamiento. Para obtener más información, consulta [CreateComputeNodeGroup](#) consulta [SlurmCustomSetting](#) la referencia de la API de AWS PCS.

## Preguntas frecuentes sobre las versiones de Slurm en PCS AWS

AWS El PCS mantiene el soporte para varias versiones de Slurm. Cuando se presenta una nueva versión de Slurm, AWS PCS proporciona soporte técnico y parches de seguridad hasta que SchedMD llegue a su fin de soporte (EOS). AWS Para mantener la coherencia con la terminología utilizada en PCS, una versión de Slurm indica el final de su vida útil (EOL) para mantener la coherencia con la terminología. AWS

¿Durante cuánto tiempo es compatible AWS PCS con una versión Slurm?

AWS El soporte de PCS para las versiones de Slurm se alinea con los ciclos de soporte de SchedMD para las versiones principales. AWS PCS admite la versión actual y las 2 versiones principales anteriores más recientes. Cuando SchedMD lanza una nueva versión principal, AWS PCS deja de dar soporte a la versión compatible más antigua. AWS PCS lanza las nuevas versiones principales de Slurm lo antes posible, pero es posible que haya un retraso entre el lanzamiento de SchedMD y su disponibilidad en PCS. AWS

¿Cómo obtienen mis clústeres las nuevas versiones de parches de Slurm?

Para corregir errores y corregir problemas de seguridad, el AWS PCS está diseñado para aplicar automáticamente los parches a los controladores de clúster que se ejecutan en las cuentas internas propiedad del servicio. Para instalar parches en sus EC2 instancias Cuenta de AWS, actualice la Amazon Machine Image (AMI) de sus grupos de nodos de cómputo y actualice los grupos de nodos de cómputo para usar la AMI actualizada. Para obtener más información, consulte [Imágenes personalizadas de Amazon Machine \(AMIs\) para AWS PCS](#).

 Note

Los controladores Slurm no estarán disponibles mientras los actualizamos. Los trabajos en ejecución no se ven afectados. Los trabajos enviados antes de que el controlador del clúster dejara de estar disponible se retienen hasta que el controlador esté disponible.

¿Cómo me informan sobre un próximo evento de EOL de la versión de Slurm?

Te enviamos un mensaje de correo electrónico 6 meses antes de la fecha de fin de vida. Le enviamos un mensaje de correo electrónico cada mes antes de la EOL, y un último mensaje de correo electrónico una semana antes de la fecha de EOL. Después de la fecha de fin de vida, enviamos mensajes de correo electrónico mensuales durante 12 meses a los clientes que utilizan clústeres de AWS PCS con versiones de EOL Slurm. Podríamos suspender un clúster con una versión de EOL Slurm si se identifican vulnerabilidades de seguridad en esa versión.

¿Cómo puedo determinar si la versión de Slurm que utiliza mi clúster ejecuta una versión de Slurm de EOL?

Le enviamos un mensaje de correo electrónico para notificarle que tiene un clúster en ejecución con una versión de EOL Slurm. Publicamos una alerta en las AWS Health Dashboard alertas que contiene los detalles de sus clústeres con versiones de EOL Slurm. También puede utilizar la consola AWS PCS para identificar los clústeres con las versiones de EOL Slurm.

¿Qué debo hacer si mi versión de Slurm se acerca o supera el EOL?

Cree un clúster nuevo con una versión compatible más reciente de Slurm y actualice la versión de Slurm en su grupo de nodos de cómputo. AMIs La versión de Slurm en tus EC2 instancias AMIs y en ejecución no puede estar más de 2 versiones por detrás de la versión de Slurm del clúster. Para obtener más información, consulte [Imágenes personalizadas de Amazon Machine \(AMIs\) para AWS PCS](#).

¿Qué pasará si no cambio a una versión más reciente de Slurm antes de la fecha de fin de vida?

No puedes crear nuevos clústeres con una versión de EOL Slurm. Los clústeres existentes pueden funcionar hasta 12 meses sin AWS soporte y no se requiere ninguna acción inmediata para mantener su funcionamiento. Después de la fecha de fin de vida, no se garantizan el soporte, las actualizaciones de seguridad ni la disponibilidad. Es posible que suspendamos un clúster por motivos de seguridad. Le recomendamos encarecidamente que utilice una versión de Slurm compatible para mantener la seguridad y el soporte de sus clústeres de AWS PCS.

¿Cuáles son los riesgos de operar un clúster con las versiones de EOL Slurm?

Los clústeres con versiones de EOL Slurm presentan importantes riesgos operativos y de seguridad. Sin la supervisión activa de SchedMD, es posible que las vulnerabilidades de seguridad pasen desapercibidas o no se aborden. Si se descubren vulnerabilidades críticas, podríamos suspender sus clústeres de inmediato.

¿Qué ocurre con mis trabajos, la computación del clúster, el almacenamiento y los recursos de red cuando mi clúster está suspendido?

Se cancelan todos los recursos gestionados por AWS PCS. Esto incluye el controlador Slurm, los grupos de nodos de cómputo y EC2 las instancias. Todos los trabajos que se ejecuten en las instancias de procesamiento finalizan inmediatamente y el clúster pasa a un estado suspendido. Los recursos administrados por el cliente, como los sistemas de archivos externos, permanecen intactos. Puede utilizar la consola AWS PCS y las acciones de la API para acceder a la configuración del clúster.

¿Puedo reiniciar un clúster suspendido para reanudar sus tareas restantes?

No, no puedes reiniciar un clúster suspendido. Puedes usar la configuración del clúster suspendido para crear un clúster nuevo con una versión de Slurm compatible. Puede ejecutar los trabajos restantes si los ha guardado en un sistema de archivos externo.

¿Puedo solicitar una prórroga más allá del período de gracia de 12 meses?

No, no puedes solicitar una extensión para ejecutar tu clúster más allá del período de gracia de 12 meses. Proporcionamos la prórroga para ayudarte a cambiar a una versión de Slurm compatible. Para evitar que se interrumpan las operaciones del clúster, le recomendamos que cambie antes de que la versión de Slurm llegue a su fin de vida.

# Contabilidad de barrios bajos en PCS AWS

Puede habilitar la contabilidad en sus nuevos clústeres de AWS PCS para supervisar el uso de los clústeres, hacer cumplir los límites de recursos y gestionar un control de acceso detallado a colas o grupos de nodos de cómputo específicos. AWS PCS crea y administra la base de datos de contabilidad para su clúster, lo que elimina la necesidad de crear y administrar su propia base de datos de contabilidad independiente. AWS PCS utiliza la función de contabilidad de Slurm. [Para obtener más información sobre la función de contabilidad de Slurm, consulte la documentación de Slurm en SchedMD.](#)

Para usar la contabilidad, habilítela al crear un nuevo clúster y, si lo desea, configure los parámetros contables. Cuando el estado del clúster sea `Active` y tenga grupos de nodos de cálculo, puede conectarse al shell de Linux de un nodo de inicio de sesión para realizar funciones de contabilidad, como ver los datos del trabajo con el comando `Slurmsacct`.

## Note

La contabilidad es compatible con Slurm 24.11 o versiones posteriores.

## AWS PCS console

En la página Crear clúster, debe seleccionar una versión válida de Slurm (versión 24.11 o posterior). En la configuración del programador, habilite la contabilidad.

## AWS PCS API

Proporciona la `accounting` configuración en tu llamada a la acción de la `CreateCluster` API. En el `accounting` objeto, `mode` defina `STANDARD`. Para obtener más información, consulte [CreateCluster](#) la referencia sobre la [contabilidad](#) en la API de AWS PCS.

En el siguiente ejemplo, se utiliza AWS CLI para llamar a la acción `CreateCluster` de la API. La subcadena de valores del parámetro `accounting={mode=STANDARD}` permite la contabilidad.

```
aws pcs create-cluster --cluster-name cluster-name \  
                      --scheduler type=SLURM,version=24.11 \  
                      --size SMALL \  
                      --networking subnetIds=cluster-subnet-  
id,securityGroupIds=cluster-security-group-id \  
                      --accounting {mode=STANDARD}
```

```
--slurm-configuration  
scaleDownIdleTimeInSeconds=180,accounting='{mode=STANDARD}',slurmCustomSettings='[{parameter
```

### Important

Obtendrá cargos de facturación adicionales si habilita la contabilidad. Para obtener más información, consulte la [página de precios de AWS PCS](#).

### Important

No puede deshabilitar la contabilidad en un clúster que la tenga habilitada. Debe eliminar el clúster.

## Conceptos clave para la contabilidad de Slurm en PCS AWS

Los siguientes conceptos son específicos de AWS PCS y controlan la forma AWS en que PCS implementa la contabilidad de Slurm.

### Base de datos de contabilidad

AWS PCS almacena sus datos contables en una base de datos creada en una Cuenta de AWS entidad AWS propietaria. No tiene acceso a la `slurmdbd.conf`.

### Tiempo de purga predeterminado

Esta configuración de AWS PCS especifica el período de retención (en días) para todos los tipos de registros contables (trabajos, eventos, reservas, pasos, suspensiones, transacciones y datos de uso). Por ejemplo, si el valor es 30, AWS PCS conserva los registros contables durante 30 días. Este valor se proporciona al crear el clúster. Si no proporciona un valor, AWS PCS conserva los registros contables en la base de datos de forma indefinida.

### AWS PCS console

El tiempo de purga predeterminado se especifica como parte de los pasos para crear un clúster. En la página Crear clúster, debe seleccionar una versión válida de Slurm (versión 24.11 o

posterior) y activar la contabilidad. En la configuración del programador, proporcione un valor entero para el tiempo de purga predeterminado (días).

## AWS PCS API

Especifica esto `defaultPurgeTimeInDays` como parte de la `accounting` información que proporciona en la llamada a la acción de la `CreateCluster` API. Para obtener más información, consulta [CreateCluster](#) la referencia sobre la [contabilidad](#) en la API de AWS PCS.

### Note

Cuando utiliza la API de AWS PCS para crear un clúster, el valor predeterminado `defaultPurgeTimeInDays` es `-1` y `0` no es un valor válido.

## Aplicación de la política contable

Esta configuración determina el rigor con el que Slurm aplica las reglas de envío de trabajos, los límites de recursos y las políticas contables para su clúster. Esta configuración corresponde al `AccountingStorageEnforce` parámetro del archivo del clúster. `slurm.conf` Puede seleccionar cualquier combinación de opciones de aplicación. Si no selecciona ninguna opción, no se aplicarán restricciones contables a los trabajos del clúster. AWS PCS admite las siguientes opciones:

- asociaciones: job-to-account mapeo
- límites: restricciones de recursos
- QoS: requisitos de calidad de servicio
- modo seguro: finalización garantizada dentro de los límites
- nosteps: desactiva la contabilidad de pasos
- nojobs: desactiva la contabilidad de trabajos

Para obtener más información sobre estas opciones, consulte la [documentación de Slurm](#) en SchedMD.

## AWS PCS console

Las opciones se configuran como parte de los pasos para crear un clúster. En la página Crear clúster, debe seleccionar una versión válida de Slurm (versión 24.11 o posterior) y activar la

contabilidad. Seleccione las opciones que desee de la lista desplegable de aplicación de las políticas contables en la configuración del programador.

### AWS PCS API

En Slurm, estas opciones se configuran en un archivo de clúster. `slurm.conf` No tiene acceso directo al clúster de `slurm.conf` su AWS PCS. En su lugar, usted proporciona `SlurmCustomSettings` a la `CreateCluster` API una acción al crear un clúster. Para obtener más información, consulta la referencia [CreateCluster](#) de la API de AWS PCS.

## Obtenga la configuración de contabilidad de un clúster de AWS PCS existente

La configuración de contabilidad de Slurm se incluye en la configuración de Slurm de su clúster.

### AWS PCS console

1. Seleccione Clústeres en el panel de navegación.
2. Elija el nombre del clúster de la lista.
3. En la pestaña Configuración, busque la configuración de cuentas en Configuración de Slurm

### AWS PCS API

Utilice la acción de la `GetCluster` API para obtener la configuración del clúster. Puede encontrar la configuración de contabilidad en `slurmConfiguration`. La configuración `mode` y el valor de `defaultPurgeTimeInDays` son inferiores a `accounting`. Las opciones de aplicación de la política contable seleccionadas se muestran a continuación `slurmCustomSettings`. Para obtener más información, consulte la referencia [GetCluster](#) de la API de AWS PCS.

# Servicio de seguridad en computación AWS paralela

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [AWS programas](#) de de . Para obtener más información sobre los programas de conformidad que se aplican al servicio de computación AWS paralela, consulte [AWS Servicios incluidos en el ámbito de aplicación del programa de conformidad AWS](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar AWS PCS. Los siguientes temas muestran cómo configurar el AWS PCS para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos de su AWS PCS.

## Temas

- [Protección de datos en AWS Parallel Computing Service](#)
- [Acceda AWS Parallel Computing Service mediante un punto final de interfaz \(\)AWS PrivateLink](#)
- [Servicio de Gestión de Identidad y Acceso para Computación AWS Paralela](#)
- [Validación de la conformidad del servicio de computación AWS paralela](#)
- [Servicio de resiliencia en la computación AWS paralela](#)
- [Servicio de seguridad de infraestructura en computación AWS paralela](#)
- [Análisis y gestión de vulnerabilidades en Parallel Computing Service AWS](#)
- [Prevención de la sustitución confusa entre servicios](#)
- [Prácticas recomendadas de seguridad para AWS Parallel Computing Service](#)

# Protección de datos en AWS Parallel Computing Service

El [modelo de](#) se aplica a protección de datos en AWS Parallel Computing Service. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y GDPR](#) en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta [Estándar de procesamiento de la información federal \(FIPS\) 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS PCS u otros dispositivos Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese

en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

## Cifrado en reposo

El cifrado está habilitado de forma predeterminada para los datos en reposo cuando se crea un clúster de AWS Parallel Computing Service (AWS PCS) con la AWS Management Console API de AWS PCS o AWS SDKs. AWS CLI AWS El PCS utiliza AWS una clave KMS propia para cifrar los datos en reposo. Para obtener más información, consulte [las claves y AWS claves del cliente](#) en la Guía para AWS KMS desarrolladores. También puede utilizar una clave gestionada por el cliente. Para obtener más información, consulte [Política de claves de KMS obligatoria para su uso con volúmenes de EBS cifrados en PCS AWS](#).

El secreto del clúster se almacena AWS Secrets Manager y cifra con la clave KMS gestionada por Secrets Manager. Para obtener más información, consulte [Trabajar con secretos de clústeres en AWS PCS](#).

En un clúster de AWS PCS, los siguientes datos están en reposo:

- Estado del planificador: incluye datos sobre las tareas en ejecución y los nodos aprovisionados en el clúster. Estos son los datos en los que Slurm persiste según lo definido en su `StateSaveLocation` `slurm.conf`. Para obtener más información, consulte la descripción de la documentación [StateSaveLocation](#) de Slurm. AWS El PCS elimina los datos del trabajo una vez finalizado un trabajo.
- Secreto de autenticación del programador: AWS PCS lo usa para autenticar todas las comunicaciones del programador en el clúster.

Para obtener información sobre el estado del programador, el AWS PCS cifra automáticamente los datos y los metadatos antes de escribirlos en el sistema de archivos. El sistema de archivos cifrados utiliza el algoritmo de cifrado AES-256 estándar del sector para los datos en reposo.

## Cifrado en tránsito

Sus conexiones a la API de AWS PCS utilizan el cifrado TLS con el proceso de firma Signature versión 4, independientemente de si utiliza AWS Command Line Interface (AWS CLI) o AWS SDKs. Para obtener más información, consulte [Firmar las solicitudes de la AWS API](#) en la Guía del AWS

Identity and Access Management usuario. AWS gestiona el control de acceso a través de la API con las políticas de IAM para las credenciales de seguridad que se utilizan para conectarse.

AWS PCS usa TLS para conectarse a otros AWS servicios.

Dentro de un clúster de Slurm, el programador se configura con el complemento de autenticación que proporciona la `auth/slurm` autenticación para todas las comunicaciones del programador. Slurm no proporciona cifrado a nivel de aplicación para sus comunicaciones, ya que todos los datos que fluyen entre las instancias del clúster permanecen locales en la EC2 VPC y, por lo tanto, están sujetos al cifrado de la VPC si esas instancias admiten el cifrado en tránsito. Para obtener más información, consulte [Cifrado en tránsito](#) en la Guía del usuario de Amazon Elastic Compute Cloud. La comunicación se cifra entre el controlador (aprovisionado en una cuenta de servicio) y los nodos del clúster de su cuenta.

## Administración de claves

AWS PCS utiliza una clave AWS KMS propia para cifrar los datos. Para obtener más información, consulte [Claves y AWS claves del cliente](#) en la Guía para AWS KMS desarrolladores. También puede utilizar una clave gestionada por el cliente. Para obtener más información, consulte [Política de claves de KMS obligatoria para su uso con volúmenes de EBS cifrados en PCS AWS](#).

El secreto del clúster se almacena AWS Secrets Manager y cifra con la clave KMS gestionada por Secrets Manager. Para obtener más información, consulte [Trabajar con secretos de clústeres en AWS PCS](#).

## Privacidad del tráfico entre redes

AWS Los recursos informáticos de PCS de un clúster residen en 1 VPC de la cuenta del cliente. Por lo tanto, todo el tráfico del servicio de AWS PCS interno dentro de un clúster permanece dentro de la AWS red y no viaja a través de Internet. La comunicación entre el usuario y los nodos AWS PCS puede viajar a través de Internet y recomendamos usar SSH o Systems Manager para conectarse a los nodos. Para obtener más información, consulte [¿Qué es? AWS Systems Manager](#) en la Guía AWS Systems Manager del usuario.

También puede utilizar las siguientes ofertas para conectar su red local a AWS:

- AWS Site-to-Site VPN. Para obtener más información, consulte [¿Qué es AWS Site-to-Site VPN?](#) en la Guía AWS Site-to-Site VPN del usuario.
- Un AWS Direct Connect. Para obtener más información, consulte [¿Qué es AWS Direct Connect?](#) en la Guía AWS Direct Connect del usuario.

Se accede a la API de AWS PCS para realizar tareas administrativas para el servicio. Usted y sus usuarios acceden a los puertos de punto final de Slurm para interactuar directamente con el programador.

## Cifrar el tráfico de la API

Para acceder a la API de AWS PCS, los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o una versión posterior. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3. Los clientes también deben admitir conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos. Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede usar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar las solicitudes.

## Cifrado del tráfico de datos

El cifrado de los datos en tránsito está habilitado desde EC2 las instancias compatibles que acceden al punto final del programador y entre ComputeNodeGroup instancias desde dentro del Nube de AWS. Para obtener más información, consulte [Cifrado en tránsito](#).

## Política de claves de KMS obligatoria para su uso con volúmenes de EBS cifrados en PCS AWS

AWS PCS utiliza [funciones vinculadas a servicios](#) para delegar permisos a otras personas. Servicios de AWS La función vinculada al servicio de AWS PCS está predefinida e incluye los permisos que AWS PCS necesita para llamar a otras Servicios de AWS personas en su nombre. Los permisos predefinidos también incluyen el acceso a sus claves gestionadas por el cliente Claves administradas por AWS , pero no a las que administra el cliente.

En este tema se describe cómo configurar la política de claves necesaria para lanzar instancias cuando se especifica una clave gestionada por el cliente para el cifrado de Amazon EBS.

### Note

AWS El PCS no requiere una autorización adicional para usar la predeterminada Clave administrada de AWS a fin de proteger los volúmenes cifrados de su cuenta.

## Contenido

- [Descripción general](#)
- [Configuración de las políticas de claves](#)
- [Ejemplo 1: secciones de la política de claves que permiten el acceso a la clave administrada por el cliente](#)
- [Ejemplo 2: secciones de la política de claves que permiten el acceso entre cuentas a la clave administrada por el cliente](#)
- [Edición de las políticas de claves en la consola de AWS KMS](#)

## Descripción general

Puede usar lo siguiente AWS KMS keys para el cifrado de Amazon EBS cuando AWS PCS lance instancias:

- [Clave administrada de AWS](#): una clave de cifrado de su cuenta que Amazon EBS crea, posee y administra. Esta es la clave de cifrado predeterminada en las cuentas nuevas. Amazon EBS la utiliza Clave administrada de AWS para el cifrado, a menos que especifique una clave gestionada por el cliente.
- [Clave administrada por el cliente](#): una clave de cifrado personalizada que usted crea, posee y administra. Para obtener más información, consulte [Crear una clave KMS](#) en la Guía para AWS Key Management Service desarrolladores.

### Note

La clave debe ser simétrica. Amazon EBS no admite claves asimétricas administradas por el cliente.

Las claves administradas por el cliente se configuran cuando se crean instantáneas cifradas o una plantilla de lanzamiento que especifica los volúmenes cifrados, o cuando se decide habilitar el cifrado de forma predeterminada.

## Configuración de las políticas de claves

Sus claves de KMS deben tener una política de claves que permita a AWS PCS lanzar instancias con volúmenes de Amazon EBS cifrados con una clave administrada por el cliente.

Utilice los ejemplos de esta página para configurar una política de claves que permita a AWS PCS acceder a su clave gestionada por el cliente. Puede modificar la política de claves de la clave gestionada por el cliente al crear la clave o más adelante.

La política clave debe incluir las siguientes declaraciones:

- Una declaración que permite que la identidad de IAM especificada en el `Principal` elemento utilice directamente la clave gestionada por el cliente. Incluye permisos para realizar las `DescribeKey` operaciones `AWS KMS EncryptDecrypt, ReEncrypt*, GenerateDataKey*`, y en la clave.
- Una declaración que permite a la identidad de IAM especificada en el `Principal` elemento utilizar la `CreateGrant` operación para generar concesiones que deleguen un subconjunto de sus propios permisos en uno de los Servicios de AWS que estén integrados con AWS KMS o con otro principal. Esto les permite utilizar la clave para crear recursos cifrados en su nombre.

No modifique ninguna declaración existente en la política cuando añada las nuevas declaraciones de política a su política clave.

Para obtener más información, consulte:

- [create-key en la Referencia de comandos AWS CLI](#)
- [put-key-policy](#) en la Referencia de comandos de la AWS CLI
- [Busque el ID de clave y el ARN clave](#) en la AWS Key Management Service Guía para desarrolladores
- [Funciones vinculadas al servicio para PCS AWS](#)
- [Cifrado de Amazon EBS](#) en la Guía del usuario de Amazon EBS
- [AWS Key Management Service](#) en la Guía para desarrolladores AWS Key Management Service

**Ejemplo 1: secciones de la política de claves que permiten el acceso a la clave administrada por el cliente**

Añada las siguientes declaraciones de política a la política clave de la clave gestionada por el cliente. Sustituya el ARN de ejemplo por el ARN de su función vinculada al servicio. `AWSServiceRoleForPCS` Esta política de ejemplo otorga a la función vinculada al servicio de AWS PCS permisos para usar la clave `AWSServiceRoleForPCS` administrada por el cliente.

```
{
```

```

    "Sid": "Allow service-linked role use of the customer managed key",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::account-id:role/aws-service-role/pcs.amazonaws.com/
AWSServiceRoleForPCS"
      ]
    },
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  }
}

```

```

{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::account-id:role/aws-service-role/pcs.amazonaws.com/
AWSServiceRoleForPCS"
    ]
  },
  "Action": [
    "kms:CreateGrant"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:GrantIsForAWSResource": true
    }
  }
}
}

```

## Ejemplo 2: secciones de la política de claves que permiten el acceso entre cuentas a la clave administrada por el cliente

Si crea una clave gestionada por el cliente en una cuenta diferente a la de su clúster de AWS PCS, debe utilizar una concesión en combinación con la política de claves para permitir el acceso a la clave entre cuentas.

Para conceder el acceso a la clave

1. Añada las siguientes declaraciones de política a la política clave de la clave gestionada por el cliente. Sustituya el ARN de ejemplo por el ARN de la otra cuenta. **111122223333** Sustitúyalo por el ID de cuenta real en el Cuenta de AWS que desea crear el clúster de AWS PCS. Esto le permite otorgar a un usuario o rol de IAM en la cuenta especificada permiso para crear una concesión para la clave mediante el siguiente comando CLI. De forma predeterminada, los usuarios no tienen acceso a la clave.

```
{
  "Sid": "Allow external account 111122223333 use of the customer managed key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

```
{
  "Sid": "Allow attachment of persistent resources in external
account 111122223333",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root"
    ]
  }
}
```

```

    ]
  },
  "Action": [
    "kms:CreateGrant"
  ],
  "Resource": "*"
}

```

- Desde la cuenta en la que desee crear el clúster de AWS PCS, cree una concesión que delegue los permisos pertinentes a la función vinculada al servicio de AWS PCS. El valor de `grantee-principal` es el ARN del rol vinculado al servicio. El valor de `key-id` es el ARN de la clave.

El siguiente ejemplo de comando [CLI create-grant](#) otorga **111122223333** permisos al rol vinculado al servicio mencionado `AWSServiceRoleForPCS` en la cuenta para usar la clave administrada por el cliente en la cuenta. **444455556666**

```

aws kms create-grant \
  --region us-west-2 \
  --key-id arn:aws:kms:us-west-2:444455556666:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d \
  --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/pcs.amazonaws.com/AWSServiceRoleForPCS \
  --operations "Encrypt" "Decrypt" "ReEncryptFrom" "ReEncryptTo" "GenerateDataKey" "GenerateDataKeyWithoutPlaintext" "DescribeKey" "CreateGrant"

```

### Note

El usuario que realiza la solicitud debe tener permisos para usar la acción. `kms:CreateGrant`

El siguiente ejemplo de política de IAM permite que una identidad de IAM (usuario o rol) en la cuenta **111122223333** cree una concesión para la cuenta clave gestionada por el cliente. **444455556666**

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCreationOfGrantForTheKMSKeyinExternalAccount444455556666",

```

```
"Effect": "Allow",
  "Action": "kms:CreateGrant",
  "Resource": "arn:aws:kms:us-
west-2:444455556666:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
}
]
}
```

Para obtener más información acerca de cómo crear una concesión para una clave KMS en una Cuenta de AWS diferente, consulte [Concesiones en AWS KMS](#) en la AWS Key Management Service Guía para desarrolladores.

#### Important

El nombre del rol vinculado al servicio especificado como principal del beneficiario debe ser el nombre de un rol existente. Tras crear la concesión, para asegurarse de que permite a AWS PCS utilizar la clave de KMS especificada, no elimine ni vuelva a crear la función vinculada al servicio.

## Edición de las políticas de claves en la consola de AWS KMS

En los ejemplos que aparecen en las secciones anteriores, solo se explica cómo agregar instrucciones a una política de claves, que es una de las múltiples formas de cambiar una de dichas políticas. La forma más sencilla de cambiar una política clave es utilizar la vista predeterminada de la AWS KMS consola para las políticas clave y convertir una identidad de IAM (usuario o rol) en uno de los usuarios clave de la política clave correspondiente. Para obtener más información, consulte [Uso de la vista AWS Management Console predeterminada](#) en la Guía para AWS Key Management Service desarrolladores.

#### Warning

Las declaraciones de política de visualización predeterminadas de la consola incluyen permisos para realizar AWS KMS Revoke operaciones en la clave gestionada por el cliente. Si revocas una concesión que daba Cuenta de AWS acceso a una clave gestionada por el cliente en tu cuenta, los usuarios de esa cuenta Cuenta de AWS pierden el acceso a los datos cifrados y a la clave.

## Acceda AWS Parallel Computing Service mediante un punto final de interfaz ()AWS PrivateLink

Puede usarlo AWS PrivateLink para crear una conexión privada entre su VPC y AWS Parallel Computing Service ()AWS PCS. Puede acceder AWS PCS como si estuviera en su VPC, sin el uso de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect una conexión. Las instancias de la VPC no necesitan direcciones IP públicas para acceder a AWS PCS.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a AWS PCS.

Para obtener más información, consulte [Acceso Servicios de AWS directo AWS PrivateLink](#) en la AWS PrivateLink Guía.

## Consideraciones sobre AWS PCS

Antes de configurar un punto de enlace de interfaz para AWS PCS, consulte [Acceder a un servicio de AWS mediante un punto de enlace de VPC de interfaz](#) en la AWS PrivateLink Guía.

AWS PCS admite realizar llamadas a todas sus acciones de API a través del punto final de la interfaz.

Si tu VPC no tiene acceso directo a Internet, debes configurar un punto de conexión de VPC para permitir que las instancias del grupo de nodos de cómputo invoquen la acción de la API. AWS PCS [RegisterComputeNodeGroupInstance](#)

## Crea un punto final de interfaz para AWS PCS

Puede crear un punto final de interfaz para AWS PCS usar la consola de Amazon VPC o AWS Command Line Interface ()AWS CLI. Para obtener más información, consulte [Creación de un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink .

Cree un punto final de interfaz para AWS PCS usar el siguiente nombre de servicio:

```
com.amazonaws.region.pcs
```

*region* Sustitúyalo por el ID del punto final en el que se va Región de AWS a crear el punto final, por ejemplo `us-east-1`.

Si habilita DNS privado para el punto de conexión de interfaz, puede realizar solicitudes a la API para AWS PCS usando su nombre de DNS predeterminado para la región. Por ejemplo, `pcs.us-east-1.amazonaws.com`.

## Creación de una política de puntos de conexión para el punto de conexión de interfaz

Una política de punto de conexión es un recurso de IAM que puede adjuntar al punto de conexión de su interfaz. La política de puntos finales predeterminada permite el acceso total a AWS PCS través del punto final de la interfaz. Para controlar el acceso permitido AWS PCS desde su VPC, adjunte una política de punto final personalizada al punto final de la interfaz.

Una política de punto de conexión especifica la siguiente información:

- Las entidades principales que pueden llevar a cabo acciones (Cuentas de AWS, usuarios de IAM y roles de IAM).
- Las acciones que se pueden realizar.
- El recurso en el que se pueden realizar las acciones.

Para obtener más información, consulte [Control del acceso a los servicios con políticas de punto de conexión](#) en la Guía del usuario de AWS PrivateLink .

Ejemplo: política de puntos finales de VPC para acciones AWS PCS

El siguiente es un ejemplo de una política de un punto de conexión personalizado. Al adjuntar esta política al punto final de la interfaz, se concede acceso a las AWS PCS acciones enumeradas a todos los principales del clúster con las especificadas. *cluster-id* *region* Sustitúyalo por el ID Región de AWS del clúster, por ejemplo `us-east-1`. *account-id* Sustitúyalo por el Cuenta de AWS número del clúster.

```
{
  "Statement": [
    {
      "Action": [
        "pcs:CreateCluster",
```

```
        "pcs:ListClusters",
        "pcs>DeleteCluster",
        "pcs:GetCluster",
    ],
    "Effect": "Allow",
    "Principal": "*",
    "Resource": [
        "arn:aws:pcs:region:account-id:cluster/cluster-id*"
    ]
    }
]
```

## Servicio de Gestión de Identidad y Acceso para Computación AWS Paralela

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar AWS los recursos del PCS. El IAM es un Servicio de AWS servicio que puede utilizar sin coste adicional.

### Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona AWS Parallel Computing Service con IAM](#)
- [Ejemplos de políticas basadas en la identidad para Parallel Computing Service AWS](#)
- [AWS políticas administradas para AWS Parallel Computing Service](#)
- [Funciones vinculadas al servicio para PCS AWS](#)
- [Función de Amazon EC2 Spot para AWS PCS](#)
- [Permisos mínimos para PCS AWS](#)
- [Perfiles de instancia de IAM para AWS Parallel Computing Service](#)
- [Solución de problemas de identidad y acceso al Servicio de Computación AWS Paralela](#)

## Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en AWS PCS.

Usuario del servicio: si utiliza el servicio AWS PCS para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de AWS PCS para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una función de AWS PCS, consulte [Solución de problemas de identidad y acceso al Servicio de Computación AWS Paralela](#).

Administrador de servicios: si está a cargo de los recursos de AWS PCS en su empresa, probablemente tenga acceso total a AWS PCS. Su trabajo consiste en determinar a qué funciones y recursos del AWS PCS deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestor de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con AWS PCS, consulte [Cómo funciona AWS Parallel Computing Service con IAM](#).

Administrador de IAM: si es administrador de IAM, puede que desee obtener más información sobre cómo redactar políticas para administrar el acceso a PCS. Para ver ejemplos de políticas de AWS PCS basadas en la identidad que puede utilizar en IAM, consulte [Ejemplos de políticas basadas en la identidad para Parallel Computing Service AWS](#)

## Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestor habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte [Cómo iniciar sesión Cuenta de AWS en su](#) Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte [AWS Signature Versión 4 para solicitudes API](#) en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactor](#) en la Guía del usuario de AWS IAM Identity Center y [Autenticación multifactor AWS en IAM](#) en la Guía del usuario de IAM.

## Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

## Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta [¿Qué es el Centro de identidades de IAM?](#) en la Guía del usuario de AWS IAM Identity Center .

## Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte [Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

## Roles de IAM

Un [rol de IAM](#) es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede [cambiar de un rol de usuario a uno de IAM](#) (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte [Crear un rol para un proveedor de identidad de terceros \(federación\)](#) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
- **Sesiones de acceso directo (FAS):** cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).
- **Rol de servicio:** un rol de servicio es un [rol de IAM](#) que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para obtener más información, consulte [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

- **Función vinculada al servicio:** una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- **Aplicaciones que se ejecutan en Amazon EC2:** puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte [Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del usuario de IAM.

## Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte [Información general de políticas JSON](#) en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción

`iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

## Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte [Elegir entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

## Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

## Listas de control de acceso ( ) ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la [descripción general de la lista de control de acceso \(ACL\)](#) en la Guía para desarrolladores de Amazon Simple Storage Service.

## Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- **Límites de permisos:** un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- **Políticas de control de servicios (SCPs):** SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las [políticas de control de servicios](#) en la Guía del AWS Organizations usuario.
- **Políticas de control de recursos (RCPs):** RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte [Políticas de control de recursos \(RCPs\)](#) en la Guía del AWS Organizations usuario.
- **Políticas de sesión:** las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades

del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

## Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

## Cómo funciona AWS Parallel Computing Service con IAM

Antes de utilizar IAM para gestionar el acceso al AWS PCS, conozca las funciones de IAM disponibles para su uso con el PCS. AWS

### Funciones de IAM que puede utilizar con AWS Parallel Computing Service

Característica de IAM	AWS Soporte para PCS
<a href="#">Políticas basadas en identidades</a>	Sí
<a href="#">Políticas basadas en recursos</a>	No
<a href="#">Acciones de políticas</a>	Sí
<a href="#">Recursos de políticas</a>	Sí
<a href="#">Claves de condición de política (específicas del servicio)</a>	Sí
<a href="#">ACLs</a>	No
<a href="#">ABAC (etiquetas en políticas)</a>	Sí
<a href="#">Credenciales temporales</a>	Sí
<a href="#">Permisos de entidades principales</a>	Sí
<a href="#">Roles de servicio</a>	No

Característica de IAM	AWS Soporte para PCS
<a href="#">Roles vinculados al servicio</a>	Sí

Para obtener una visión general de cómo funcionan los AWS PCS y otros AWS servicios con la mayoría de las funciones de IAM, consulte [AWS los servicios que funcionan con IAM](#) en la Guía del usuario de IAM.

## Políticas de PCS basadas en la identidad AWS

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte [Referencia de los elementos de las políticas de JSON de IAM](#) en la Guía del usuario de IAM.

### Ejemplos de políticas basadas en la identidad para PCS AWS

Para ver ejemplos de políticas de AWS PCS basadas en la identidad, consulte. [Ejemplos de políticas basadas en la identidad para Parallel Computing Service AWS](#)

## Políticas basadas en recursos dentro de PCS AWS

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte [Cross account resource access in IAM](#) en la Guía del usuario de IAM.

## Acciones políticas para AWS el PCS

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones del AWS PCS, consulte [las acciones definidas por AWS Parallel Computing Service](#) en la referencia de autorización del servicio.

Las acciones políticas del AWS PCS utilizan el siguiente prefijo antes de la acción:

```
pcs
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [  
  "pcs:action1",  
  "pcs:action2"  
]
```

## Recursos de políticas para PCS AWS

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (\*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de AWS PCS y sus tipos ARNs, consulte [los recursos definidos por AWS Parallel Computing Service](#) en la referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte [Acciones definidas por AWS Parallel Computing Service](#).

Para ver ejemplos de políticas de AWS PCS basadas en la identidad, consulte [Ejemplos de políticas basadas en la identidad para Parallel Computing Service AWS](#)

## Claves de condición de la política para PCS AWS

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación AND lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta [Elementos de la política de IAM: variables y etiquetas](#) en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales en la Guía](#) del usuario de IAM.

Para ver una lista de las claves de condición del AWS PCS, consulte [las claves de condición del servicio de computación AWS paralela](#) en la Referencia de autorización del servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte [Acciones definidas por AWS Parallel Computing Service](#).

Para ver ejemplos de políticas de AWS PCS basadas en la identidad, consulte [Ejemplos de políticas basadas en la identidad para Parallel Computing Service AWS](#)

## ACLs en PCS AWS

Soportes ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

## ABAC con PCS AWS

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte [Definición de permisos con la autorización de ABAC](#) en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte [Uso del control de acceso basado en atributos \(ABAC\)](#) en la Guía del usuario de IAM.

## Uso de credenciales temporales con PCS AWS

Compatibilidad con credenciales temporales: sí

Algunos Servicios de AWS no funcionan cuando se inicia sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta [Cómo Servicios de AWS funcionan con IAM](#) en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte [Cambio de un usuario a un rol de IAM \(consola\)](#) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda

generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte [Credenciales de seguridad temporales en IAM](#).

## Permisos principales entre servicios para PCS AWS

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en él AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).

## Funciones de servicio para AWS PCS

Compatible con roles de servicio: No

Un rol de servicio es un [rol de IAM](#) que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

### Warning

Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad del AWS PCS. Edite las funciones de servicio solo cuando el AWS PCS le dé instrucciones para hacerlo.

## Funciones vinculadas al servicio para PCS AWS

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o administración de funciones vinculadas al servicio de AWS PCS, consulte [Funciones vinculadas al servicio para PCS AWS](#)

## Ejemplos de políticas basadas en la identidad para Parallel Computing Service AWS

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AWS PCS. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios puede asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM \(consola\)](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por el AWS PCS, incluido el ARNs formato de cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición del servicio de computación AWS paralela](#) en la Referencia de autorización de servicios.

### Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la consola PCS AWS](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)

## Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de AWS PCS de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están

disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de tarea](#) en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte [Validación de políticas con el Analizador de acceso de IAM](#) en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte [Acceso seguro a la API con MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

## Uso de la consola PCS AWS

Para acceder a la consola del Servicio de Computación AWS Paralela, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de AWS PCS de su propiedad Cuenta de AWS. Si crea una política basada en identidades que sea más

restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para obtener más información sobre los permisos mínimos necesarios para usar la consola AWS PCS, consulte [Permisos mínimos para PCS AWS](#).

## Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",

```

```
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

## AWS políticas administradas para AWS Parallel Computing Service

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir [políticas administradas por el cliente](#) específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte [Políticas administradas de AWS](#) en la Guía del usuario de IAM.

### AWS política gestionada: AWSPCSService RolePolicy

No puede adjuntarse AWSPCSService RolePolicy a sus entidades de IAM. Esta política está asociada a una función vinculada al servicio que permite a AWS PCS realizar acciones en su nombre. Para obtener más información, consulte [Funciones vinculadas al servicio para PCS AWS](#).

#### Detalles de los permisos

Esta política incluye los siguientes permisos.

- `ec2`— Permite a AWS PCS crear y gestionar EC2 los recursos de Amazon.
- `iam`— Permite a AWS PCS crear un rol vinculado al servicio para la EC2 flota de Amazon y pasarlo a Amazon. EC2
- `cloudwatch`— Permite a AWS PCS publicar métricas de servicio en Amazon CloudWatch.
- `secretsmanager`— Permite a AWS PCS gestionar los secretos de los recursos del clúster de AWS PCS.

```
{  
  "Version" : "2012-10-17",
```

```

"Statement" : [
  {
    "Sid" : "PermissionsToCreatePCSNetworkInterfaces",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSPCSManaged" : "false"
      }
    }
  },
  {
    "Sid" : "PermissionsToCreatePCSNetworkInterfacesInSubnet",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  },
  {
    "Sid" : "PermissionsToManagePCSNetworkInterfaces",
    "Effect" : "Allow",
    "Action" : [
      "ec2>DeleteNetworkInterface",
      "ec2:CreateNetworkInterfacePermission"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSPCSManaged" : "false"
      }
    }
  },
  {
    "Sid" : "PermissionsToDescribePCSResources",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSubnets",

```

```

    "ec2:DescribeVpcs",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeImages",
    "ec2:DescribeImageAttribute"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PermissionsToCreatePCSLaunchTemplates",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSPCSManaged" : "false"
    }
  }
},
{
  "Sid" : "PermissionsToManagePCSLaunchTemplates",
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions",
    "ec2>CreateLaunchTemplateVersion"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSPCSManaged" : "false"
    }
  }
},
{

```

```

    "Sid" : "PermissionsToTerminatePCSMangedInstances",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSPCSManaged" : "false"
      }
    }
  },
  {
    "Sid" : "PermissionsToPassRoleToEC2",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/*/AWSPCS*",
      "arn:aws:iam:*:*:role/AWSPCS*",
      "arn:aws:iam:*:*:role/aws-pcs/*",
      "arn:aws:iam:*:*:role/*/aws-pcs/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "PermissionsToControlClusterInstanceAttributes",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2:CreateFleet"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume*"
    ]
  }
}

```

```

    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:capacity-reservation/*",
    "arn:aws:resource-groups:*:*:group/*",
    "arn:aws:ec2:*:*:fleet/*",
    "arn:aws:ec2:*:*:spot-instances-request/*"
  ]
},
{
  "Sid" : "PermissionsToProvisionClusterInstances",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances",
    "ec2:CreateFleet"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSPCSManaged" : "false"
    }
  }
},
{
  "Sid" : "PermissionsToTagPCSResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances",
        "CreateLaunchTemplate",
        "CreateFleet",
        "CreateNetworkInterface"
      ]
    }
  }
}
}

```

```

    },
    {
      "Sid" : "PermissionsToPublishMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/PCS"
        }
      }
    },
    {
      "Sid" : "PermissionsToManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager>DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:pcs!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "pcs",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}

```

## AWS PCS actualiza las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas para AWS PCS desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial de documentos de AWS PCS.

Cambio	Descripción	Fecha
Se actualizó el JSON de este documento	Se corrigió el JSON de este documento para incluirlo <code>"arn:aws:ec2:*:*:spot-instances-request/*"</code> .	5 de septiembre de 2024
AWS PCS comenzó a rastrear los cambios	AWS PCS comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	28 de agosto de 2024

## Funciones vinculadas al servicio para PCS AWS

AWS [Parallel Computing Service](#) utiliza [funciones vinculadas a servicios AWS Identity and Access Management \(IAM\)](#). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a PCS. AWS Los roles vinculados al servicio están predefinidos por AWS PCS e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración del AWS PCS, ya que no es necesario añadir manualmente los permisos necesarios. AWS PCS define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS PCS puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. Esto protege sus recursos de AWS PCS porque no puede eliminar accidentalmente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte [AWS los servicios que funcionan con IAM](#) y busque los servicios con la palabra Sí en la columna Funciones vinculadas a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

## Permisos de roles vinculados al servicio para PCS AWS

AWS PCS utiliza el rol vinculado al servicio denominado `AWSServiceRoleForPCS`: permite que AWS PCS gestione los recursos de Amazon EC2 .

El rol vinculado al servicio de `AWSService RoleFor PCS` confía en los siguientes servicios para asumir el rol:

- `pcs . amazonaws . com`

La política de permisos de roles denominada [AWSPCSServiceRolePolicy](#) permite a AWS PCS completar acciones en recursos específicos.

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

## Crear un rol vinculado a un servicio para PCS AWS

No es necesario crear manualmente un rol vinculado a un servicio. AWS PCS le crea un rol vinculado a un servicio cuando crea un clúster.

## Edición de un rol vinculado a un servicio para PCS AWS

AWS PCS no permite editar el rol vinculado al servicio de `AWSService RoleFor PCS`. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

## Eliminar un rol vinculado a un servicio para PCS AWS

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

**Note**

Si el servicio AWS PCS utiliza la función al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos del AWS PCS utilizados por el AWSService RoleFor PCS

Debe eliminar todos los clústeres para eliminar la función vinculada al servicio de AWSService RoleFor PCS. Para obtener más información, consulte [Eliminar un clúster](#).

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al servicio de AWSService RoleFor PCS. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones compatibles para AWS las funciones vinculadas al servicio de PCS

AWS PCS admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte [Puntos de conexión y Regiones de AWS](#).

## Función de Amazon EC2 Spot para AWS PCS

Si desea crear un grupo de nodos de cómputo de AWS PCS que utilice Spot como opción de compra, también debe tener en su seno la función vinculada al servicio de AWSServiceRoleForEC2Spot. Cuenta de AWS Puede usar el siguiente AWS CLI comando para crear el rol. Para obtener más información, consulte [Crear un rol vinculado a un servicio](#) y [Crear un rol para delegar permisos a un AWS servicio](#) en la Guía del AWS Identity and Access Management usuario.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

**Note**

Aparece el siguiente error si Cuenta de AWS ya tiene un rol de AWSServiceRoleForEC2Spot IAM.

An error occurred (InvalidInput) when calling the CreateServiceLinkedRole operation: Service role name AWSServiceRoleForEC2Spot has been taken in this account, please try a different suffix.

## Permisos mínimos para PCS AWS

En esta sección se describen los permisos de IAM mínimos necesarios para que una identidad de IAM (usuario, grupo o rol) utilice el servicio.

### Contenido

- [Permisos mínimos para usar las acciones de la API](#)
- [Permisos mínimos para usar etiquetas](#)
- [Permisos mínimos para admitir registros](#)
- [Permisos mínimos para un administrador de servicios](#)

### Permisos mínimos para usar las acciones de la API

Acción de la API	Permisos mínimos	Permisos adicionales para la consola
CreateCluster	<pre>ec2:CreateNetworkInterface, ec2:DescribeVpcs, ec2:DescribeSubnets, ec2:DescribeSecurityGroups, ec2:GetSecurityGroupsForVpc, iam:CreateServiceLinkedRole, secretsmanager:CreateSecret, secretsmanager:TagResource,</pre>	

Acción de la API	Permisos mínimos	Permisos adicionales para la consola
	<code>pcs:CreateCluster</code>	
ListClusters	<code>pcs:ListClusters</code>	
GetCluster	<code>pcs:GetCluster</code>	<code>ec2:DescribeSubnets</code>
DeleteCluster	<code>pcs&gt;DeleteCluster</code>	
CreateComputeNodeGroup	<code>ec2:DescribeVpcs,</code> <code>ec2:DescribeSubnets,</code> <code>ec2:DescribeSecurityGroups,</code> <code>ec2:DescribeLaunchTemplates,</code> <code>ec2:DescribeLaunchTemplateVersions,</code> <code>ec2:DescribeInstanceTypes,</code> <code>ec2:DescribeInstanceTypeOfferings,</code> <code>ec2:RunInstances,</code> <code>ec2:CreateFleet,</code> <code>ec2:CreateTags,</code> <code>iam:PassRole,</code> <code>iam:GetInstanceProfile,</code> <code>pcs:CreateComputeNodeGroup</code>	<code>iam:ListInstanceProfiles,</code> <code>ec2:DescribeImages,</code> <code>pcs:GetCluster</code>
ListComputerNodeGroups	<code>pcs:ListComputeNodeGroups</code>	<code>pcs:GetCluster</code>
GetComputeNodeGroup	<code>pcs:GetComputeNodeGroup</code>	<code>ec2:DescribeSubnets</code>

Acción de la API	Permisos mínimos	Permisos adicionales para la consola
UpdateComputeNodeGroup	<pre>ec2:DescribeVpcs, ec2:DescribeSubnets, ec2:DescribeSecurityGroups, ec2:DescribeLaunchTemplates, ec2:DescribeLaunchTemplateVersions, ec2:DescribeInstanceTypes, ec2:DescribeInstanceTypeOfferings, ec2:RunInstances, ec2:CreateFleet, ec2:CreateTags, iam:PassRole, iam:GetInstanceProfile, pcs:UpdateComputeNodeGroup</pre>	<pre>pcs:GetComputeNodeGroup, iam:ListInstanceProfiles, ec2:DescribeImages, pcs:GetCluster</pre>
DeleteComputeNodeGroup	<pre>pcs&gt;DeleteComputeNodeGroup</pre>	
CreateQueue	<pre>pcs&gt;CreateQueue</pre>	<pre>pcs:ListComputeNodeGroups, pcs:GetCluster</pre>
ListQueues	<pre>pcs:ListQueues</pre>	<pre>pcs:GetCluster</pre>
GetQueue	<pre>pcs:GetQueue</pre>	

Acción de la API	Permisos mínimos	Permisos adicionales para la consola
UpdateQueue	<code>pcs:UpdateQueue</code>	<code>pcs:ListComputeNodeGroups,</code> <code>pcs:GetQueue</code>
DeleteQueue	<code>pcs&gt;DeleteQueue</code>	

## Permisos mínimos para usar etiquetas

Se requieren los siguientes permisos para usar etiquetas con sus recursos en AWS PCS.

```
pcs:ListTagsForResource,
pcs:TagResource,
pcs:UntagResource
```

## Permisos mínimos para admitir registros

AWS PCS envía los datos de registro a Amazon CloudWatch Logs (CloudWatch Logs). Debe asegurarse de que su identidad tiene los permisos mínimos para usar CloudWatch Logs. Para obtener más información, consulte [Descripción general de la gestión de los permisos de acceso a sus recursos de CloudWatch Logs](#) en la Guía del usuario de Amazon CloudWatch Logs.

Para obtener información sobre los permisos necesarios para que un servicio envíe CloudWatch registros a Logs, consulte [Habilitar el registro desde AWS los servicios](#) en la Guía del usuario de Amazon CloudWatch Logs.

## Permisos mínimos para un administrador de servicios

La siguiente política de IAM especifica los permisos mínimos necesarios para que una identidad de IAM (usuario, grupo o rol) configure y administre el servicio AWS PCS.

### Note

Los usuarios que no configuran ni administran el servicio no necesitan estos permisos. Los usuarios que solo ejecutan trabajos utilizan un shell seguro (SSH) para conectarse al clúster.

AWS Identity and Access Management (IAM) no gestiona la autenticación ni la autorización de SSH.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PCSAccess",
      "Effect": "Allow",
      "Action": [
        "pcs:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EC2Access",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeImages",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IamInstanceProfile",
      "Effect": "Allow",
      "Action": [
        "iam:GetInstanceProfile"
      ],
      "Resource": "*"
    }
  ],
}
```

```

{
  "Sid": "IamPassRole",
  "Effect": "Allow",
  "Action": [
    "iam:PassRole"
  ],
  "Resource": [
    "arn:aws:iam::*:role/*/AWSPCS*",
    "arn:aws:iam::*:role/AWSPCS*",
    "arn:aws:iam::*:role/aws-pcs/*",
    "arn:aws:iam::*:role/*/aws-pcs/*"
  ],
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": [
        "ec2.amazonaws.com"
      ]
    }
  }
},
{
  "Sid": "SLRAccess",
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": [
    "arn:aws:iam::*:role/aws-service-role/pcs.amazonaws.com/AWSServiceRoleFor*",
    "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/AWSServiceRoleFor*"
  ],
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": [
        "pcs.amazonaws.com",
        "spot.amazonaws.com"
      ]
    }
  }
},
{
  "Sid": "AccessKMSKey",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",

```

```

    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "SecretManagementAccess",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:CreateSecret",
    "secretsmanager:TagResource",
    "secretsmanager:UpdateSecret"
  ],
  "Resource": "*"
},
{
  "Sid": "ServiceLogsDelivery",
  "Effect": "Allow",
  "Action": [
    "pcs:AllowVendedLogDeliveryForResource",
    "logs:PutDeliverySource",
    "logs:PutDeliveryDestination",
    "logs:CreateDelivery"
  ],
  "Resource": "*"
}
]
}

```

## Perfiles de instancia de IAM para AWS Parallel Computing Service

Las aplicaciones que se ejecutan en una EC2 instancia deben incluir AWS credenciales en todas las solicitudes de AWS API que realicen. Te recomendamos que utilices una función de IAM para gestionar las credenciales temporales de la EC2 instancia. Para ello, puede definir un perfil de instancia y adjuntarlo a sus instancias. Para obtener más información, consulta las [funciones de IAM para Amazon EC2](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

**Note**

Cuando utilizas el AWS Management Console para crear un rol de IAM para Amazon EC2, la consola crea un perfil de instancia automáticamente y le da el mismo nombre que el rol de IAM. Si utilizas las acciones de la AWS CLI AWS API o un AWS SDK para crear el rol de IAM, creas el perfil de instancia como una acción independiente. Para obtener más información, consulte [Perfiles de instancia](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Debe especificar el nombre de recurso de Amazon (ARN) de un perfil de instancia al crear un grupo de nodos de cómputo. Puede elegir diferentes perfiles de instancia para algunos o todos los grupos de nodos de cómputo.

## Requisitos del perfil de instancia

### ARN del perfil de instancia

El nombre de la función de IAM que forma parte del ARN debe AWSPCS empezar por o /aws-pcs/ contener en su ruta:

- `arn:aws:iam::*:instance-profile/AWSPCS-example-role-1` y
- `arn:aws:iam::*:instance-profile/aws-pcs/example-role-2`.

**Note**

Si usa el AWS CLI, proporcione un `--path` valor para `iam create-instance-profile` incluirlo /aws-pcs/ en la ruta del ARN. Por ejemplo:

```
aws iam create-instance-profile --path /aws-pcs/ --instance-profile-name
example-role-2
```

## Permisos

Como mínimo, el perfil de instancia de AWS PCS debe incluir la siguiente política. Permite que los nodos de cómputo notifiquen al servicio AWS PCS cuando estén operativos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "pcs:RegisterComputeNodeGroupInstance"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

## Políticas adicionales

Puede considerar la posibilidad de añadir políticas administradas al perfil de la instancia. Por ejemplo:

- [AmazonS3 ReadOnlyAccess](#) proporciona acceso de solo lectura a todos los buckets de S3.
- [Amazon SSMManaged InstanceCore](#) habilita las funciones principales del servicio AWS Systems Manager, como el acceso remoto directamente desde la consola de administración de Amazon.
- [CloudWatchAgentServerPolicy](#) contiene los permisos necesarios para su uso AmazonCloudWatchAgent en los servidores.

También puede incluir sus propias políticas de IAM que respalden su caso de uso específico.

## Creación de un perfil de instancia

Puedes crear un perfil de instancia directamente desde la EC2 consola de Amazon. Para obtener más información, consulta Cómo [usar perfiles de instancia](#) en la Guía del AWS Identity and Access Management usuario.

## Enumere los perfiles de instancia para AWS PCS

Puede usar el siguiente AWS CLI comando para enumerar los perfiles de instancia de una forma Región de AWS que cumpla con los requisitos de nombre del AWS PCS. *us-east-1* Sustitúyalos por los adecuados Región de AWS.

```
aws iam list-instance-profiles --region us-east-1 --query "InstanceProfiles[?starts_with(InstanceProfileName, 'AWSPCS') || contains(Path, '/aws-pcs/')].[InstanceProfileName]" --output text
```

## Solución de problemas de identidad y acceso al Servicio de Computación AWS Paralela

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con AWS PCS e IAM.

### Temas

- [No estoy autorizado a realizar ninguna acción en PCS AWS](#)
- [No estoy autorizado a realizar tareas como: PassRole](#)
- [Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de AWS PCS](#)

### No estoy autorizado a realizar ninguna acción en PCS AWS

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio `my-example-widget`, pero no tiene los permisos ficticios `pcs:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: pcs:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso `my-example-widget` mediante la acción `pcs:GetWidget`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

### No estoy autorizado a realizar tareas como: PassRole

Si recibe un mensaje de error que indica que no está autorizado a realizar la `iam:PassRole` acción, sus políticas deben actualizarse para que pueda transferir una función a AWS PCS.

Algunos Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en PCS. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

## Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de AWS PCS

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede utilizar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS PCS admite estas funciones, consulte [Cómo funciona AWS Parallel Computing Service con IAM](#)
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte [Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en](#) la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta [Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

## Validación de la conformidad del servicio de computación AWS paralela

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa de cumplimiento](#) [Servicios de AWS](#) de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- [Cumplimiento de seguridad y gobernanza](#): en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- [Referencia de servicios válidos de HIPAA](#): muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- [AWS Recursos de](#) de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- [AWS Guías de cumplimiento para clientes](#): comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- [Evaluación de los recursos con reglas](#) en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.

- [AWS Security Hub](#)— Este Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).
- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- [AWS Audit Manager](#)— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

## Servicio de resiliencia en la computación AWS paralela

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

[Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS](#)

## Servicio de seguridad de infraestructura en computación AWS paralela

Como servicio gestionado, AWS Parallel Computing Service está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder al AWS PCS a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Cuando AWS PCS crea un clúster, el servicio lanza el controlador Slurm en una cuenta propiedad del servicio, independiente de los nodos de procesamiento de su cuenta. Para conectar la comunicación entre el controlador y los nodos de cómputo, AWS PCS crea una interfaz de red elástica (ENI) multicuenta en la VPC. El controlador Slurm utiliza el ENI para gestionar y comunicarse con los distintos nodos de cómputo Cuentas de AWS, manteniendo la seguridad y el aislamiento de los recursos y, al mismo tiempo, facilitando las operaciones eficientes de HPC e IA/ML.

## Análisis y gestión de vulnerabilidades en Parallel Computing Service AWS

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted. Para obtener más información, consulte el [modelo de responsabilidad AWS compartida](#). AWS gestiona las tareas de seguridad básicas de la infraestructura subyacente de la cuenta de servicio, como la aplicación de parches al sistema operativo en las instancias del controlador, la configuración del firewall y la recuperación ante desastres de la AWS infraestructura. Estos procedimientos han sido revisados y certificados por los terceros pertinentes. Para obtener más información, consulte las [Prácticas recomendadas sobre seguridad, identidad y conformidad](#).

### Note

Los controladores Slurm no estarán disponibles mientras los actualizamos. Los trabajos en ejecución no se ven afectados. Los trabajos enviados cuando el controlador del clúster no está disponible se retienen hasta que el controlador esté disponible.

Usted es responsable de la seguridad de la infraestructura subyacente de su Cuenta de AWS:

- Mantenga su código, incluidas las actualizaciones y los parches de seguridad.
- Aplica parches y actualiza el sistema operativo en Amazon Machine Image (AMI) para tus grupos de nodos de cómputo y actualiza tus grupos de nodos de cómputo para usar la AMI actualizada.
- Actualice el programador para mantenerlo dentro de las versiones compatibles. Actualice la AMI de sus grupos de nodos de cómputo y actualice su grupo de nodos de cómputo para usar la AMI actualizada.
- Autentica y cifra la comunicación entre los clientes usuarios y los nodos a los que se conectan.

Para obtener más información sobre la actualización de la AMI para sus grupos de nodos de cómputo, consulte [Amazon Machine Images \(AMIs\) para AWS PCS](#).

## Prevención de la sustitución confusa entre servicios

El problema del suplente confuso es una cuestión de seguridad en la que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios pueden producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se pueden manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición [aws:SourceAccount](#) global [aws:SourceArn](#) las claves de contexto en las políticas de recursos para limitar los permisos que AWS Parallel Computing Service (AWS PCS) concede a otro servicio al recurso. Utiliza `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utiliza `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con caracteres comodines (\*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:service:*:123456789012:*`.

Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos.

El valor de `aws:SourceArn` debe ser un ARN de clúster.

El siguiente ejemplo muestra cómo se pueden utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves de contexto del AWS PCS para evitar el confuso problema de los diputados.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "pcs.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:pcs:us-east-1:123456789012:cluster/*"
        ]
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

## Función de IAM para EC2 instancias de Amazon aprovisionadas como parte de un grupo de nodos de cómputo

AWS PCS organiza automáticamente la EC2 capacidad de Amazon para cada uno de los grupos de nodos de procesamiento configurados de un clúster. Al crear un grupo de nodos de cómputo, los usuarios deben proporcionar un perfil de instancia de IAM a través del `iamInstanceProfileArn` campo. El perfil de instancia especifica los permisos asociados a las instancias aprovisionadas EC2. AWS PCS acepta cualquier rol que tenga `AWSPCS` como prefijo de nombre de rol o `/aws-pcs/` como parte de la ruta del rol. El `iam:PassRole` permiso es obligatorio para la identidad de IAM (usuario o rol) que crea o actualiza un grupo de nodos de procesamiento. Cuando un usuario llama

a las acciones `CreateComputeNodeGroup` o a la `UpdateComputeNodeGroup` API, AWS PCS comprueba si el usuario tiene permiso para realizar la `iam:PassRole` acción.

La siguiente política de ejemplo otorga permisos para transferir únicamente los roles de IAM cuyo nombre comience por `AWSPCS`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/AWSPCS*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": [
            "ec2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

## Prácticas recomendadas de seguridad para AWS Parallel Computing Service

En esta sección se describen las mejores prácticas de seguridad específicas de AWS Parallel Computing Service (AWS PCS). Para obtener más información sobre las prácticas recomendadas de seguridad AWS, consulte [Prácticas recomendadas en materia de seguridad, identidad y conformidad](#).

### Seguridad relacionada con la AMI

- No utilice la muestra de AWS PCS AMIs para las cargas de trabajo de producción. Las muestras no AMIs son compatibles y solo están destinadas a ser probadas.
- Actualice periódicamente el sistema operativo y el software de la AMI para sus grupos de nodos de cómputo a fin de mitigar las vulnerabilidades.
- Utilice únicamente paquetes de AWS PCS oficiales autenticados y descargados de AWS fuentes oficiales.

- Actualice periódicamente los paquetes de AWS PCS en la AMI para los grupos de nodos de cómputo y actualice los nodos de cómputo para usar la AMI actualizada. Considere la posibilidad de automatizar este proceso para minimizar las vulnerabilidades.

Para obtener más información, consulte [Imágenes personalizadas de Amazon Machine \(AMIs\) para AWS PCS](#).

## Seguridad de Slurm Workload Manager

- Implemente controles de acceso y restricciones de red para proteger los nodos de control y cómputo de Slurm. Permita que solo los usuarios y sistemas de confianza envíen trabajos y accedan a los comandos de administración de Slurm.
- Utilice las funciones de seguridad integradas de Slurm, como la autenticación de Slurm, para garantizar que las solicitudes de trabajo y las comunicaciones estén autenticadas.
- Actualice las versiones de Slurm para mantener un funcionamiento fluido y la compatibilidad con clústeres.

### Important

Cualquier clúster que utilice una versión de Slurm que haya llegado al final de su vida útil (EOSL) se detendrá inmediatamente. Utilice el enlace que aparece en la parte superior de las páginas de la guía del usuario para suscribirse a la fuente RSS de documentación del AWS PCS y recibir notificaciones cuando una versión de Slurm se acerque a la EOSL.

Para obtener más información, consulte [Versiones Slurm en PCS AWS](#).

## Supervisión y registro

- Use Amazon CloudWatch Logs AWS CloudTrail para monitorear y registrar las acciones en sus clústeres y Cuenta de AWS. Utilice los datos para la solución de problemas y la auditoría.

## Seguridad de la red

- Implemente sus clústeres de AWS PCS en una VPC independiente para aislar su entorno de HPC del resto del tráfico de red.

- Utilice grupos de seguridad y listas de control de acceso a la red (ACLs) para controlar el tráfico entrante y saliente a las instancias y subredes de AWS PCS.
- Utilice AWS PrivateLink nuestros puntos de enlace de VPC para mantener el tráfico de red entre los clústeres y otros AWS servicios de la red. Para obtener más información, consulte [Acceda AWS Parallel Computing Service mediante un punto final de interfaz \(VPC\) de AWS PrivateLink](#).

# Registro y supervisión para AWS PCS

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS PCS y del resto de los recursos de AWS. AWS proporciona las siguientes herramientas de supervisión para vigilar el AWS PCS, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puedes CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de tus EC2 instancias de Amazon y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde EC2 instancias de Amazon y otras fuentes. CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcanzan ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la [Guía del usuario CloudWatch de Amazon Logs](#).
- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la [Guía del usuario de AWS CloudTrail](#).

## AWS Registros del programador PCS

Puede configurar AWS PCS para que envíe datos de registro detallados desde el programador de clústeres a Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3) y Amazon Data Firehose. Esto puede ayudar con la supervisión y la solución de problemas. Puede configurar los registros del programador de AWS PCS mediante la consola de AWS PCS, así como mediante programación mediante el AWS CLI SDK.

### Contenido

- [Requisitos previos](#)

- [Configuración de los registros del programador mediante la AWS consola PCS](#)
- [Configurar los registros del programador mediante el AWS CLI](#)
  - [Cree un destino de entrega](#)
  - [Habilite el clúster AWS PCS como fuente de entrega](#)
  - [Conecte la fuente de entrega del clúster al destino de entrega](#)
- [Rutas y nombres de los flujos de registro del programador](#)
- [Ejemplo de registro del programador AWS PCS](#)

## Requisitos previos

El principal de IAM utilizado para administrar el clúster PCS de AWS debe `pcs:AllowVendedLogDeliveryForResource` permitirlo. A continuación, se muestra un ejemplo de la política de IAM de AWS que lo habilita.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PcsAllowVendedLogsDelivery",
      "Effect": "Allow",
      "Action": ["pcs:AllowVendedLogDeliveryForResource"],
      "Resource": [
        "arn:aws:pcs:::cluster/*"
      ]
    }
  ]
}
```

## Configuración de los registros del programador mediante la AWS consola PCS

Para configurar los registros del programador de AWS PCS en la consola, siga estos pasos:

1. Abra la [consola AWS PCS](#).
2. Elija Clústeres y vaya a la página de detalles del clúster AWS PCS, donde habilitará el registro.
3. Seleccione Logs (Registros).
4. En Entregas de registros: Scheduler Logs (opcional)

- a. Agregue hasta tres destinos de entrega de registros. Las opciones incluyen CloudWatch Logs, Amazon S3 o Firehose.
- b. Selecciona Actualizar entregas de registros.

Para volver a configurar, añadir o eliminar las entregas de registros, vuelva a visitar esta página.

## Configurar los registros del programador mediante el AWS CLI

Para ello, necesita al menos un destino de entrega, una fuente de entrega (el clúster PCS) y una entrega, que es una relación que conecta una fuente con un destino.

### Cree un destino de entrega

Necesita al menos un destino de entrega para recibir los registros del programador de un clúster de AWS PCS. Puede obtener más información sobre este tema en la PutDeliveryDestination sección de la Guía del usuario de la CloudWatch API.

Para crear un destino de entrega mediante el AWS CLI

- Cree un destino con el siguiente comando. Antes de ejecutar el comando, realice los siguientes reemplazos:
  - *region-code* Sustitúyalo por el Región de AWS lugar donde crearás tu destino. Por lo general, será la misma región en la que se implementó el clúster de AWS PCS.
  - *pcs-logs-destination* Sustitúyalo por el nombre que prefiera. Debe ser único para todos los destinos de entrega de tu cuenta.
  - *resource-arn* Sustitúyalo por el ARN de un grupo de CloudWatch registros existente en Logs, un bucket de S3 o un flujo de entrega en Firehose. Entre los ejemplos se incluyen:
    - CloudWatch Grupo de registros

```
arn:aws:logs:region-code:account-id:log-group:/log-group-name:*
```

- S3 bucket

```
arn:aws:s3:::bucket-name
```

- Flujo de entrega de Firehose

```
arn:aws:firehose:region-code:account-id:deliverystream/stream-name
```

```
aws logs put-delivery-destination --region region-code \  
  --name pcs-logs-destination \  
  --delivery-destination-configuration destinationResourceArn=resource-arn
```

Toma nota del ARN del nuevo destino de entrega, ya que lo necesitarás para configurar las entregas.

## Habilite el clúster AWS PCS como fuente de entrega

Para recopilar los registros del programador de AWS PCS, configure el clúster como fuente de entrega. Para obtener más información, consulta [PutDeliverySource](#) la referencia de la API CloudWatch de Amazon Logs.

Para configurar un clúster como fuente de entrega mediante el AWS CLI

- Habilite la entrega de registros desde su clúster con el siguiente comando. Antes de ejecutar el comando, realice los siguientes reemplazos:
  - *region-code* Sustitúyalo por el Región de AWS lugar en el que está desplegado el clúster.
  - *cluster-logs-source-name* Sustitúyalo por un nombre para esta fuente. Debe ser único para todas las fuentes de entrega de su Cuenta de AWS. Considere la posibilidad de incorporar el nombre o el ID del clúster de AWS PCS.
  - *cluster-arn* Sustitúyalo por el ARN de su clúster PCS AWS

```
aws logs put-delivery-source \  
  --region region-code \  
  --name cluster-logs-source-name \  
  --resource-arn cluster-arn \  
  --log-type PCS_SCHEDULER_LOGS
```

## Conecte la fuente de entrega del clúster al destino de entrega

Para que los datos de registro del programador fluyan del clúster al destino, debe configurar una entrega que los conecte. Para obtener más información, consulta [CreateDelivery](#) la referencia de la API CloudWatch de Amazon Logs.

Para crear una entrega mediante el AWS CLI

- Cree una entrega mediante el siguiente comando. Antes de ejecutar el comando, realice los siguientes reemplazos:

- *region-code* Reemplácelo por el Región de AWS lugar donde se encuentran su origen y su destino.
- *cluster-logs-source-name* Sustitúyalo por el nombre de la fuente de entrega que aparece arriba.
- *destination-arn* Sustitúyalo por el ARN de un destino de entrega al que desee que se entreguen los registros.

```
aws logs create-delivery \
  --region region-code \
  --delivery-source-name cluster-logs-source \
  --delivery-destination-arn destination-arn
```

## Rutas y nombres de los flujos de registro del programador

La ruta y el nombre de los registros del programador de AWS PCS dependen del tipo de destino.

- CloudWatch Registros
  - Una transmisión CloudWatch de Logs sigue esta convención de nomenclatura.

```
AWSLogs/PCS/${cluster_id}/${log_name}_${scheduler_major_version}.log
```

### Example

```
AWSLogs/PCS/abcdef0123/slurmctld_24.05.log
```

- S3 bucket
  - La ruta de salida de un bucket de S3 sigue esta convención de nomenclatura:

```
AWSLogs/${account-id}/PCS/${region}/${cluster_id}/${log_name}/
${scheduler_major_version}/yyyy/MM/dd/HH/
```

### Example

```
AWSLogs/111111111111/PCS/us-east-2/abcdef0123/slurmctld/24.05/2024/09/01/00.
```

- El nombre de un objeto de S3 sigue esta convención:

```
PCS_${log_name}_${scheduler_major_version}_#{expr date 'event_timestamp', format:
"yyyy-MM-dd-HH"}_${cluster_id}_${hash}.log
```

### Example

```
PCS_slurmctld_24.05_2024-09-01-00_abcdef0123_0123abcdef.log
```

## Ejemplo de registro del programador AWS PCS

Los registros del programador de AWS PCS están estructurados. Incluyen campos como el identificador del clúster, el tipo de programador y las versiones principales y del parche, además del mensaje de registro emitido por el proceso del controlador Slurm. A continuación se muestra un ejemplo.

```
{
  "resource_id": "s3431v9rx2",
  "resource_type": "PCS_CLUSTER",
  "event_timestamp": 1721230979,
  "log_level": "info",
  "log_name": "slurmctld",
  "scheduler_type": "slurm",
  "scheduler_major_version": "23.11",
  "scheduler_patch_version": "8",
  "node_type": "controller_primary",
  "message": "[2024-07-17T15:42:58.614+00:00] Running as primary controller\n"
}
```

## Servicio de monitorización de computación AWS paralela con Amazon CloudWatch

Amazon CloudWatch supervisa el estado y el rendimiento del clúster de AWS Parallel Computing Service (AWS PCS) mediante la recopilación de métricas del clúster a intervalos. Estas métricas se conservan, lo que le permite acceder a los datos históricos y obtener información sobre el rendimiento de su clúster a lo largo del tiempo.

CloudWatch también le permite monitorear las EC2 instancias lanzadas por AWS PCS para cumplir con sus requisitos de escalado. Si bien puede inspeccionar los registros de las instancias en

ejecución, CloudWatch las métricas y los datos de registro normalmente se eliminan una vez que las instancias se cierran. Sin embargo, puede configurar el CloudWatch agente en las instancias mediante una plantilla de EC2 lanzamiento para conservar las métricas y los registros incluso después de la finalización de la instancia, lo que permite la supervisión y el análisis a largo plazo.

Explore los temas de esta sección para obtener más información sobre la supervisión del uso de AWS PCS CloudWatch.

#### Temas

- [Monitorear las métricas del AWS PCS mediante CloudWatch](#)
- [Supervisión de instancias de AWS PCS mediante Amazon CloudWatch](#)

## Monitorear las métricas del AWS PCS mediante CloudWatch

Puede supervisar el estado del clúster de AWS PCS con Amazon CloudWatch, que recopila datos de su clúster y los convierte en métricas prácticamente en tiempo real. Estas estadísticas se conservan durante un período de 15 meses, para que pueda acceder a la información histórica y obtener una mejor perspectiva del rendimiento de su clúster. Las métricas del clúster se envían CloudWatch en períodos de 1 minuto. Para obtener más información CloudWatch, consulta [¿Qué es Amazon CloudWatch?](#) en la Guía del CloudWatch usuario de Amazon.

AWS PCS publica las siguientes métricas en el espacio de nombres AWS/PCS en. CloudWatch Tienen una sola dimensión, `ClusterId`

Nombre	Descripción	Unidades
ActualCapacity	IdleCapacity + UtilizedCapacity	Recuento
CapacityUtilization	UtilizedCapacity / ActualCapacity	Recuento
DesiredCapacity	ActualCapacity + PendingCapacity	Recuento
IdleCapacity	Recuento de instancias que se están ejecutando pero que no están asignadas a trabajos	Recuento

Nombre	Descripción	Unidades
UtilizedCapacity	Recuento de instancias que se están ejecutando y asignadas a trabajos	Recuento

## Supervisión de instancias de AWS PCS mediante Amazon CloudWatch

AWS PCS lanza EC2 las instancias de Amazon según sea necesario para cumplir con los requisitos de escalado definidos en sus grupos de nodos de cómputo de PCS. Puedes monitorizar estas instancias mientras están en ejecución con Amazon CloudWatch. Puede inspeccionar los registros de las instancias en ejecución iniciando sesión en ellas y utilizando herramientas de línea de comandos interactivas. Sin embargo, de forma predeterminada, los datos de CloudWatch las métricas solo se conservan durante un período limitado una vez que se cierra una instancia y, por lo general, los registros de la instancia se eliminan junto con los volúmenes de EBS que respaldan la instancia. Para conservar las métricas o los datos de registro de las instancias lanzadas por PCS una vez finalizadas, puede configurar el CloudWatch agente de las instancias con una plantilla de EC2 lanzamiento. En este tema se proporciona información general sobre la supervisión de las instancias en ejecución y se proporcionan ejemplos de cómo configurar las métricas y los registros de las instancias persistentes.

### Supervisión de instancias en ejecución

#### Búsqueda de instancias de AWS PCS

Para monitorear las instancias lanzadas por PCS, busque las instancias en ejecución asociadas a un clúster o grupo de nodos de cómputo. A continuación, en la EC2 consola de una instancia determinada, inspeccione las secciones de estado y alarmas y de supervisión. Si el acceso de inicio de sesión está configurado para esas instancias, puede conectarse a ellas e inspeccionar los distintos archivos de registro de las instancias. Para obtener más información sobre cómo identificar qué instancias administra PCS, consulte [Búsqueda de instancias de grupos de nodos de cómputo en AWS PCS](#).

#### Habilitar métricas detalladas

De forma predeterminada, las métricas de las instancias se recopilan en intervalos de 5 minutos. Para recopilar métricas en intervalos de un minuto, habilita la CloudWatch supervisión detallada en la

plantilla de lanzamiento de tu grupo de nodos de cómputo. Para obtener más información, consulte [Active la CloudWatch supervisión detallada](#).

## Configurar las métricas y los registros de las instancias persistentes

Puedes conservar las métricas y los registros de tus instancias instalando y configurando el CloudWatch agente de Amazon en ellas. Consta de tres pasos principales:

1. Cree una configuración de CloudWatch agente.
2. Guarde la configuración en un lugar donde las instancias de PCS puedan recuperarla.
3. Escriba una plantilla de EC2 lanzamiento que instale el software del CloudWatch agente, busque la configuración e inicie el CloudWatch agente con la configuración.

Para obtener más información, consulte [Recopilar métricas, registros y seguimientos con el CloudWatch agente](#) en la Guía del CloudWatch usuario de Amazon y [Uso de plantillas de EC2 lanzamiento de Amazon con AWS PCS](#).

### Cree una configuración CloudWatch de agente

Antes de implementar el CloudWatch agente en las instancias, debe generar un archivo de configuración JSON que especifique las métricas, los registros y los seguimientos que desea recopilar. Los archivos de configuración se pueden crear mediante un asistente o manualmente, mediante un editor de texto. El archivo de configuración se creará manualmente para esta demostración.

En un equipo en el que tenga instalada la AWS CLI, cree un archivo de CloudWatch configuración denominado config.json con el contenido siguiente. También puede usar la siguiente URL para descargar una copia del archivo.

```
https://aws-hpc-recipes.s3.amazonaws.com/main/recipes/pcs/cloudwatch/assets/config.json
```

### Notas

- Las rutas de registro del archivo de ejemplo son para Amazon Linux 2. Si sus instancias utilizarán un sistema operativo base diferente, cambie las rutas según corresponda.
- Para capturar otros registros, añada entradas adicionales en `collect_list`.

- Los valores incluidos {brackets} son variables modeladas. Para ver la lista completa de variables admitidas, consulte [Crear o editar manualmente el archivo de configuración del CloudWatch agente](#) en la Guía del CloudWatch usuario de Amazon.
- Puede optar por omitir logs metrics o no recopilar estos tipos de información.

```
{
  "agent": {
    "metrics_collection_interval": 60
  },
  "logs": {
    "logs_collected": {
      "files": {
        "collect_list": [
          {
            "file_path": "/var/log/cloud-init.log",
            "log_group_class": "STANDARD",
            "log_group_name": "/PCSLogs/instances",
            "log_stream_name": "{instance_id}.cloud-init.log",
            "retention_in_days": 30
          },
          {
            "file_path": "/var/log/cloud-init-output.log",
            "log_group_class": "STANDARD",
            "log_stream_name": "{instance_id}.cloud-init-output.log",
            "log_group_name": "/PCSLogs/instances",
            "retention_in_days": 30
          },
          {
            "file_path": "/var/log/amazon/pcs/bootstrap.log",
            "log_group_class": "STANDARD",
            "log_stream_name": "{instance_id}.bootstrap.log",
            "log_group_name": "/PCSLogs/instances",
            "retention_in_days": 30
          },
          {
            "file_path": "/var/log/slurmd.log",
            "log_group_class": "STANDARD",
            "log_stream_name": "{instance_id}.slurmd.log",
            "log_group_name": "/PCSLogs/instances",
            "retention_in_days": 30
          }
        ]
      }
    }
  }
}
```

```

        "file_path": "/var/log/messages",
        "log_group_class": "STANDARD",
        "log_stream_name": "{instance_id}.messages",
        "log_group_name": "/PCSLogs/instances",
        "retention_in_days": 30
    },
    {
        "file_path": "/var/log/secure",
        "log_group_class": "STANDARD",
        "log_stream_name": "{instance_id}.secure",
        "log_group_name": "/PCSLogs/instances",
        "retention_in_days": 30
    }
]
}
},
"metrics": {
    "aggregation_dimensions": [
        [
            "InstanceId"
        ]
    ],
    "append_dimensions": {
        "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
        "ImageId": "${aws:ImageId}",
        "InstanceId": "${aws:InstanceId}",
        "InstanceType": "${aws:InstanceType}"
    },
    "metrics_collected": {
        "cpu": {
            "measurement": [
                "cpu_usage_idle",
                "cpu_usage_iowait",
                "cpu_usage_user",
                "cpu_usage_system"
            ],
            "metrics_collection_interval": 60,
            "resources": [
                "*"
            ],
            "totalcpu": false
        },
        "disk": {

```



- `/var/log/amazon/pcs/bootstrap.log`— Resultado de las operaciones específicas de PCS que se ejecutan durante la configuración de la instancia
- `/var/log/slurmd.log`— Resultado del daemon slurmd del administrador de cargas de trabajo de Slurm
- `/var/log/messages`— Mensajes del sistema desde el núcleo, los servicios del sistema y las aplicaciones
- `/var/log/secure`— Registros relacionados con los intentos de autenticación, como SSH, sudo y otros eventos de seguridad

Los archivos de registro se envían a un grupo de CloudWatch registros denominado `/PCSLogs/instances`. Los flujos de registro son una combinación del ID de instancia y el nombre base del archivo de registro. El grupo de registros tiene un tiempo de retención de 30 días.

Además, el archivo indica al CloudWatch agente que recopile varias métricas comunes y las agregue por ID de instancia.

### Guarde la configuración

El archivo de configuración del CloudWatch agente debe almacenarse en un lugar donde las instancias del nodo de cómputo de PCS puedan acceder a él. Existen dos formas comunes de hacerlo. Puede cargarlo en un bucket de Amazon S3 al que las instancias de su grupo de nodos de cómputo tendrán acceso a través de su perfil de instancia. También puede almacenarlo como un parámetro de SSM en el almacén de parámetros de Amazon Systems Manager.

### Cárguelo a un bucket de S3

Para almacenar el archivo en S3, utilice los comandos de la AWS CLI que se indican a continuación. Antes de ejecutar el comando, realice los siguientes reemplazos:

- `amzn-s3-demo-bucket` Sustitúyalo por el nombre de su propio bucket de S3

En primer lugar (esto es opcional si tiene un depósito existente), cree un depósito para almacenar sus archivos de configuración.

```
aws s3 mb s3://amzn-s3-demo-bucket
```

A continuación, sube el archivo al depósito.

```
aws s3 cp ./config.json s3://amzn-s3-demo-bucket/
```

## Almacénelo como un parámetro SSM

Para almacenar el archivo como un parámetro SSM, utilice el siguiente comando. Antes de ejecutar el comando, realice las siguientes sustituciones:

- *region-code* Sustitúyalo por la región de AWS en la que trabaja con AWS PCS.
- (Opcional) *AmazonCloudWatch-PCS* Sustitúyalo por su propio nombre para el parámetro. Ten en cuenta que si cambias el prefijo del nombre de, AmazonCloudWatch- tendrás que añadir específicamente el acceso de lectura al parámetro SSM en el perfil de instancia de tu grupo de nodos.

```
aws ssm put-parameter \
  --region region-code \
  --name "AmazonCloudWatch-PCS" \
  --type String \
  --value file://config.json
```

## Escribe una plantilla de lanzamiento EC2

Los detalles específicos de la plantilla de lanzamiento dependen de si el archivo de configuración está almacenado en S3 o SSM.

### Utilice una configuración almacenada en S3

Este script instala el CloudWatch agente, importa un archivo de configuración de un bucket de S3 e inicia el CloudWatch agente con él. Sustituya los siguientes valores de este script por sus propios detalles:

- *amzn-s3-demo-bucket*— El nombre de un bucket de S3 desde el que puede leer su cuenta
- */config.json*— Ruta relativa a la raíz del bucket de S3 donde se almacena la configuración

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=="MYBOUNDARY=="

--MYBOUNDARY==
Content-Type: text/cloud-config; charset="us-ascii"
```

```

packages:
- amazon-cloudwatch-agent

runcmd:
- aws s3 cp s3://amzn-s3-demo-bucket/config.json /etc/s3-cw-config.json
- /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m
  ec2 -s -c file:///etc/s3-cw-config.json

--==MYBOUNDARY==--

```

El perfil de instancia de IAM del grupo de nodos debe tener acceso al bucket. A continuación, se muestra un ejemplo de política de IAM para el depósito en el script de datos de usuario anterior.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}

```

Tenga en cuenta también que las instancias deben permitir el tráfico saliente al S3 y CloudWatch a los puntos finales. Esto se puede lograr mediante grupos de seguridad o puntos finales de VPC, según la arquitectura del clúster.

Utilice una configuración almacenada en SSM

Este script instala el CloudWatch agente, importa un archivo de configuración desde un parámetro de SSM e inicia el CloudWatch agente con él. Sustituya los siguientes valores de este script por sus propios detalles:

- (Opcional) *AmazonCloudWatch-PCS* Sustitúyalo por su propio nombre para el parámetro.

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary==="MYBOUNDARY==="

--===MYBOUNDARY==
Content-Type: text/cloud-config; charset="us-ascii"

packages:
- amazon-cloudwatch-agent

runcmd:
- /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m
  ec2 -s -c ssm:AmazonCloudWatch-PCS

--===MYBOUNDARY===--
```

La política de instancias de IAM para el grupo de nodos debe tener la `CloudWatchAgentServerPolicy` información adjunta.

Si el nombre de su parámetro no comienza por `AmazonCloudWatch-` tendrá que añadir específicamente el acceso de lectura al parámetro SSM en el perfil de instancia de su grupo de nodos. A continuación, se muestra un ejemplo de política de IAM que ilustra esto para el prefijo.

#### *DOC-EXAMPLE-PREFIX*

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CustomCwSsmMParamReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/DOC-EXAMPLE-PREFIX*"
    }
  ]
}
```

Tenga en cuenta también que las instancias deben permitir el tráfico saliente hacia el SSM y los puntos finales. CloudWatch Esto se puede lograr mediante grupos de seguridad o puntos finales de VPC, según la arquitectura del clúster.

# Registro de llamadas a la API de AWS Parallel Computing Service mediante AWS CloudTrail

AWS PCS está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS PCS. CloudTrail captura todas las llamadas a la API de AWS PCS como eventos. Las llamadas capturadas incluyen las llamadas desde la consola del AWS PCS y las llamadas en código a las operaciones de la API del AWS PCS. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS PCS. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a AWS PCS, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

## AWS Información sobre el PCS en CloudTrail

CloudTrail está habilitada Cuenta de AWS cuando crea la cuenta. Cuando se produce una actividad en AWS PCS, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de AWS PCS, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas las acciones del AWS PCS se registran CloudTrail y se documentan en la [referencia de la API del Servicio de Computación AWS Paralela](#). Por ejemplo, las llamadas a las `CreateComputeNodeGroup` `DeleteCluster` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `UpdateQueue`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el [elemento `userIdentity` de CloudTrail](#).

## Descripción de las entradas de los archivos de CloudTrail registro del AWS PCS

Un registro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro para una `CreateQueue` acción.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:admin",
    "arn": "arn:aws:sts::012345678910:assumed-role/Admin/admin",
    "accountId": "012345678910",
    "accessKeyId": "ASIAY36PTPIEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
```

```
        "type": "Role",
        "principalId": "AROAY36PTPIEEXAMPLE",
        "arn": "arn:aws:iam::012345678910:role/Admin",
        "accountId": "012345678910",
        "userName": "Admin"
    },
    "attributes": {
        "creationDate": "2024-07-16T17:05:51Z",
        "mfaAuthenticated": "false"
    }
}
},
"eventTime": "2024-07-16T17:13:09Z",
"eventSource": "pcs.amazonaws.com",
"eventName": "CreateQueue",
"awsRegion": "us-east-1",
"sourceIPAddress": "127.0.0.1",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36",
"requestParameters": {
    "clientToken": "c13b7baf-2894-42e8-acec-example",
    "clusterIdentifier": "abcdef0123",
    "computeNodeGroupConfigurations": [
        {
            "computeNodeId": "abcdef0123"
        }
    ],
    "queueName": "all"
},
"responseElements": {
    "queue": {
        "arn": "arn:aws:pcs:us-east-1:609783872011:cluster/abcdef0123/queue/
abcdef0123",
        "clusterId": "abcdef0123",
        "computeNodeGroupConfigurations": [
            {
                "computeNodeId": "abcdef0123"
            }
        ],
        "createdAt": "2024-07-16T17:13:09.276069393Z",
        "id": "abcdef0123",
        "modifiedAt": "2024-07-16T17:13:09.276069393Z",
        "name": "all",
        "status": "CREATING"
    }
}
```

```
    }  
  },  
  "requestID": "a9df46d7-3f6d-43a0-9e3f-example",  
  "eventID": "7ab18f88-0040-47f5-8388-example",  
  "readOnly": false,  
  "eventType": "AwsApiCall",  
  "managementEvent": true,  
  "recipientAccountId": "012345678910",  
  "eventCategory": "Management",  
  "tlsDetails": {  
    "tlsVersion": "TLSv1.3",  
    "cipherSuite": "TLS_AES_128_GCM_SHA256",  
    "clientProvidedHostHeader": "pcs.us-east-1.amazonaws.com"  
  },  
  "sessionCredentialFromConsole": "true"  
}
```

# Puntos finales y cuotas de servicio para PCS AWS

En las siguientes secciones se describen los puntos finales y las cuotas de servicio de AWS Parallel Computing Service (AWS PCS). Las cuotas de servicio, anteriormente denominadas límites, son la cantidad máxima de recursos u operaciones de servicio para usted Cuenta de AWS.

Cuenta de AWS Tiene cuotas predeterminadas para cada AWS servicio. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para obtener más información, consulte [AWS service quotas](#) en la Referencia general de AWS .

## Contenido

- [Puntos de conexión de servicio](#)
- [Service Quotas](#)
  - [Cuotas internas](#)
  - [Cuotas relevantes para otros servicios AWS](#)

## Puntos de conexión de servicio

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Norte de Virginia)	us-east-1	pcs.us-east-1.amazonaws.com	HTTPS
Este de EE. UU. (Ohio)	us-east-2	pcs.us-east-2.amazonaws.com	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	pcs.us-west-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	pcs.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	pcs.ap-southeast-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Tokio)	ap-northeast-1	pcs.ap-northeast-1 .amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	pcs.eu-central-1.a mazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	pcs.eu-west-1.amaz onaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	pcs.eu-north-1.ama zonaws.com	HTTPS

## Service Quotas

Nombre	Predeterminado	Ajustable	Descripción
Clústeres	5	Sí	El número máximo de clústeres por Región de AWS.

### Note

Los valores predeterminados son las cuotas iniciales establecidas por AWS. Estos valores predeterminados son independientes de los valores reales de la cuota aplicada y de las cuotas de servicio máximas posibles. Para obtener más información, consulte [Terminología de Service Quotas](#) en la Guía del usuario de Service Quotas.

Estas cuotas de servicio se enumeran en AWS Parallel Computing Service (PCS) en el [AWS Management Console](#). Para solicitar un aumento de cuota para los valores que se muestran como ajustables, consulte [Solicitar un aumento de cuota](#) en la Guía del usuario de Service Quotas.

**⚠ Important**

Recuerde comprobar la Región de AWS configuración actual en AWS Management Console.

## Cuotas internas

Las siguientes cuotas son internas y no ajustables.

Nombre	Predeterminado	Ajustable	Descripción
Creación simultánea de clústeres	1	No	El número máximo de clústeres en el <code>Creating</code> estado por. Región de AWS
Calcule los grupos de nodos por clúster	10	No	El número máximo de grupos de nodos de procesamiento por clúster.
Colas por clúster	10	No	El número máximo de colas por clúster.

## Cuotas relevantes para otros servicios AWS

AWS PCS utiliza otros AWS servicios. Sus cuotas de servicio para esos servicios afectan al uso de AWS PCS.

Cuotas EC2 de servicio de Amazon que afectan a AWS PCS

- Solicitudes de instancias puntuales
- Ejecución de instancias bajo demanda
- Plantillas de inicialización
- Versiones de plantillas de lanzamiento
- Solicitudes EC2 de API de Amazon

Para obtener más información, consulta [las cuotas de EC2 servicio de Amazon](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

# Solución de problemas en AWS Parallel Computing Service

Los siguientes temas proporcionan orientación para solucionar algunos problemas que pueden surgir en el AWS PCS.

## Temas

- [Una EC2 instancia en AWS PCS se termina y se reemplaza después del reinicio](#)

## Una EC2 instancia en AWS PCS se termina y se reemplaza después del reinicio

### Descripción general del problema

Tras reiniciar una EC2 instancia de un grupo de nodos de cómputo, AWS PCS finaliza y reemplaza automáticamente la instancia.

### ¿Por qué sucede esto

AWS PCS no admite el re arranque de instancias. Si se reinicia una EC2 instancia, AWS PCS considera que la instancia está en mal estado y la reemplaza. Si AWS PCS termina y reemplaza las instancias de forma continua, puede que se deba a que algo las reinicie después del lanzamiento. Algunos ejemplos incluyen el reinicio automático de la EC2 instancia (por ejemplo, un reinicio automático después de aplicar los parches), la automatización externa a la EC2 instancia (como una aplicación de administración de red), otro AWS servicio (por ejemplo AWS Systems Manager) o el reinicio manual realizado por una persona.

### Solución

Puedes comprobar tus `slurmd` registros `slurmctld` o registros para comprobar si la instancia se ha reiniciado. Para obtener más información, consulte [AWS Registros del programador PCS](#) y [Supervisión de instancias de AWS PCS mediante Amazon CloudWatch](#). El siguiente ejemplo de entrada de `slurmctld` registro indica que la instancia se reinició:

### Example

```
[2024-09-12T06:42:50.393+00:00] validate_node_specs: Node Login-1 unexpectedly rebooted  
boot_time=1726123354 last_response=1726123285
```

## Se está reiniciando debido a un parche

A menudo es necesario reiniciar el equipo después de aplicar los parches. No aplique los parches directamente a una EC2 instancia que forme parte de un grupo de nodos de cómputo de AWS PCS. Si debe aplicar parches a EC2 las instancias, debe aplicarlos a una Amazon Machine Image (AMI) actualizada y actualizar los grupos de nodos de cómputo para usar la AMI actualizada. EC2 Las nuevas instancias que AWS PCS lance para esos grupos de nodos de cómputo utilizarán la AMI actualizada (parcheada). Para obtener más información, consulte [Imágenes personalizadas de Amazon Machine \(AMIs\) para AWS PCS](#).

# Historial de documentos de la Guía del usuario de AWS PCS

En la siguiente tabla se describen los cambios importantes en la documentación del AWS PCS.

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
15 de mayo de 2025	Nueva función: contabilidad	La contabilidad de Slurm ahora es compatible con Slurm 24.11 o versiones posteriores. Para obtener más información, consulte <a href="#">Contabilidad de barrios bajos en PCS AWS</a> .	SDK DE AWS: 15 DE MAYO DE 2020
15 de mayo de 2025	Actualizado para Slurm 24.11	Se actualizó la guía del usuario para la compatibilidad con Slurm 24.11.5. Para obtener más información, consulte los siguientes temas: <ul style="list-style-type: none"> <li>• <a href="#">Versiones Slurm en PCS AWS</a></li> <li>• <a href="#">Instaladores de software para crear PCS personalizados AMIs AWS</a></li> <li>• <a href="#">Notas de publicación para un ejemplo de AWS PCS AMIs</a></li> </ul>	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
5 de mayo de 2025	Preguntas frecuentes sobre las versiones actualizadas de Slurm	Se actualizaron las preguntas frecuentes (FAQ) de las versiones de Slurm sobre las versiones de Slurm que se acercan o superan el final de su vida útil (EOL). Para obtener más información, consulte <a href="#">Preguntas frecuentes sobre las versiones de Slurm en PCS AWS</a> .	N/A
17 de abril de 2025	Tema nuevo: cómo obtener los detalles de un grupo de nodos de cómputo	Aprenda a obtener detalles de un grupo de nodos de cómputo de AWS PCS, como su ID, ARN e ID de AMI. Para obtener más información, consulte <a href="#">Obtenga detalles del grupo de nodos de cómputo en AWS PCS</a> .	N/A
2 de abril de 2025	Instalador de Slurm actualizado	Se actualizó el tema de AMI para el instalador Slurm 24.05.7-1. Para obtener más información, consulte <a href="#">Instaladores de software para crear PCS personalizados AMIs AWS</a> .	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
28 de marzo de 2025	Se agregaron cuotas para el número máximo de colas y grupos de nodos de cómputo	Se agregaron cuotas internas no ajustables para el número máximo de grupos de nodos de cómputo por clúster y el número máximo de colas por clúster. Para obtener más información, consulte <a href="#">Cuotas internas</a> .	N/A
14 de marzo de 2025	Se ha modificado una clave de propiedad en la plantilla CloudFormation	Idahora es <code>TemplateId</code> para la <code>CustomLaunchTemplate</code> propiedad de la CloudFormation plantilla. Para obtener más información, consulta <a href="#">Recursos</a> en <a href="#">Partes de una CloudFormation plantilla para AWS PCS</a> .	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
13 de marzo de 2025	Se agregó información sobre la versión del agente AWS PCS y Slurm	<p>Se agregó un tema nuevo que describe los cambios para cada versión del agente AWS PCS. Para obtener más información, consulte <a href="#">AWS Versiones del agente PCS</a>.</p> <p>Se agregó más información al tema sobre las versiones de Slurm, que describe las fechas de soporte importantes y las notas de lanzamiento detalladas sobre el soporte de AWS PCS para Slurm. Para obtener más información, consulte <a href="#">Versiones Slurm en PCS AWS</a>.</p>	N/A
7 de marzo de 2025	Agente de PCS actualizado	Se actualizó el tema de AMI para el agente AWS PCS 1.2.0-1. Para obtener más información, consulte <a href="#">Instaladores de software para crear PCS personalizados AMIs AWS</a> .	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
3 de febrero de 2025	Se agregó un tema sobre el uso con PCS AWS CloudFormation AWS	Se agregó un tema a la guía del usuario que proporciona un ejemplo de cómo usarlo AWS CloudFormation con AWS PCS. En este tema se proporciona un procedimiento para utilizar una CloudFormation plantilla de ejemplo para crear el clúster de AWS PCS de muestra y se describen brevemente las secciones de esa plantilla. Para obtener más información, consulte <a href="#">Comience con un AWS CloudFormationAWS PCS</a> .	N/A
18 de diciembre de 2024	Actualizado para Slurm 24.05	Se actualizó la guía del usuario para la compatibilidad con Slurm 24.05. Para obtener más información, consulte <a href="#">Instaladores de software para crear PCS personalizados AMIs AWS</a> y <a href="#">Notas de publicación para un ejemplo de AWS PCS AMIs</a> .	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
18 de diciembre de 2024	Ejemplo de versiones actualizadas de NVIDIA para Slurm 23.11 AMIs	Se actualizaron las versiones CUDA y del controlador NVIDIA en la muestra de Slurm 23.11. AMIs Para obtener más información, consulte <a href="#">Notas de publicación para un ejemplo de AWS PCS AMIs</a> .	N/A
17 de diciembre de 2024	Instalador de Slurm actualizado	Se actualizó el tema de AMI para el instalador de Slurm 23.11.10-3. Para obtener más información, consulte <a href="#">Instaladores de software para crear PCS personalizados AMIs AWS</a> .	N/A
13 de diciembre de 2024	Agente PCS actualizado	Se actualizó el tema de AMI para el agente AWS PCS 1.1.1-1. Para obtener más información, consulte <a href="#">Instaladores de software para crear PCS personalizados AMIs AWS</a> .	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
6 de diciembre de 2024	Se actualizaron el agente PCS y el instalador de Slurm	Se actualizó el tema de AMI para el agente AWS PCS 1.1.0-1 y el instalador de Slurm 23.11.10-2. Para obtener más información, consulte <a href="#">Instaladores de software para crear PCS personalizados AMIs AWS</a> .	N/A
6 de diciembre de 2024	Se agregó un tema sobre la compatibilidad con el sistema operativo	Para obtener más información, consulte <a href="#">Sistemas operativos compatibles en AWS PCS</a> .	N/A
8 de noviembre de 2024	Guía de usuario reorganizada	Reorganizamos la guía del usuario para llevar los temas al nivel superior, trasladamos algunos temas a sus propias páginas y agrupamos temas similares.	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
7 de noviembre de 2024	Temas de AMI actualizados	<p>Se actualizó el tema de AMI para Slurm 23.11.10 y libjwt 17.0. Para obtener más información, consulte <a href="#">Instaladores de software para crear PCS personalizados AMIs AWS</a> y <a href="#">Paso 3: Instalar Slurm</a>.</p> <p>Se han simplificado y corregido las notas de la versión de AMIs. Para obtener más información, consulte <a href="#">Notas de publicación para un ejemplo de AWS PCS AMIs</a>.</p>	N/A
7 de noviembre de 2024	Se agregó un tema nuevo sobre el uso de volúmenes de EBS cifrados con AWS PCS	<p>Se agregó un tema que describe la política de claves de KMS requerida para los volúmenes de EBS cifrados en AWS PCS. Para obtener más información, consulte <a href="#">Política de claves de KMS obligatoria para su uso con volúmenes de EBS cifrados en PCS AWS</a>.</p>	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
18 de octubre de 2024	AWS Lanzamiento del agente PCS 1.0.1-1	Se actualizó la documentación relacionada con la AMI para hacer referencia a la versión AWS 1.0.1-1 del agente PCS. Para obtener más información, consulte <a href="#">Instaladores de software para crear PCS personalizados AMIs AWS</a> y <a href="#">Paso 2: Instalar el agente AWS PCS</a> .	N/A
10 de octubre de 2024	Se agregó un capítulo de solución de problemas	Se agregó un capítulo de solución de problemas con un tema sobre el reemplazo automático de las EC2 instancias tras un reinicio. Para obtener más información, consulte <a href="#">Solución de problemas en AWS Parallel Computing Service</a> .	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
23 de septiembre de 2024	Se actualizaron los permisos mínimos para usar las acciones de la API y para un administrador de servicios	Ahora se requiere el <code>ec2:DescribeInstanceTypeOfferings</code> permiso para las acciones de la <code>UpdateComputeNodeGroup</code> API <code>CreateComputeNodeGroup</code> y las de la API. Para obtener más información, consulte <a href="#">Permisos mínimos para PCS AWS</a> .	N/A
5 de septiembre de 2024	Se actualizó el ejemplo de política de IAM para los permisos mínimos para un administrador de servicios	Para obtener más información, consulte <a href="#">Permisos mínimos para un administrador de servicios</a> .	N/A
5 de septiembre de 2024	Se agregó un permiso faltante al JSON en la página de políticas administradas	Se trataba únicamente de una corrección de la documentación. La política gestionada real no se modificó. Para obtener más información, consulte <a href="#">AWS políticas administradas para AWS Parallel Computing Service</a> .	N/A

Date	Cambio	Actualizaciones de la documentación	Versiones de API actualizadas
28 de agosto de 2024	Se agregó la página de políticas administradas	Para obtener más información, consulte <a href="#">AWS políticas administradas para AWS Parallel Computing Service</a> .	N/A
28 de agosto de 2024	AWS Versión de PCS	Versión inicial de la guía del usuario del AWS PCS.	AWS SDK: 28 de agosto de 2020

# AWS Glosario

Para obtener la AWS terminología más reciente, consulte el [AWS glosario](#) de la Glosario de AWS Referencia.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.