aws

Guía del usuario de

Red Hat OpenShift Service en AWS

Red Hat OpenShift Service en AWS: Guía del usuario de

Table of Contents

¿Qué es Red Hat OpenShift Service en AWS?

Red Hat OpenShift Service en AWS (ROSA) es un servicio gestionado que puede utilizar para crear, escalar e implementar aplicaciones en contenedores con la plataforma OpenShift empresarial Kubernetes de Red Hat. AWS ROSA agiliza el traslado de las OpenShift cargas de trabajo de Red Hat locales a AWS otras y ofrece una estrecha integración con ellas. Servicios de AWS

Características

ROSA cuenta con el apoyo y la gestión conjuntos de Red AWS Hat. Cada ROSA clúster cuenta con el apoyo de un ingeniero de confiabilidad de sitios (SRE) de Red Hat las 24 horas del día para la administración de clústeres, respaldado por el acuerdo de nivel de servicio (SLA) de Red Hat con un tiempo de actividad del 99,95%. Para obtener más información sobre el modelo de soporte del servicio, consulte. the section called “Cómo obtener asistencia”

ROSA también proporciona las siguientes funciones:

- Instalación de clústeres, mantenimiento de clústeres y actualizaciones de clústeres compatibles con la SRE de Red Hat.
- Servicio de AWS Las integraciones incluyen AWS computación, bases de datos, análisis, aprendizaje automático, redes y dispositivos móviles.
- Ejecute y escale el plano de control de Kubernetes en varias zonas de disponibilidad para garantizar una alta AWS disponibilidad.
- Opere los clústeres con OpenShift APIs herramientas de productividad para desarrolladores, como Service Mesh, CodeReady Workspaces y Serverless.

Acceder ROSA

Puede definir y configurar las implementaciones ROSA de servicios mediante las siguientes interfaces.

AWS

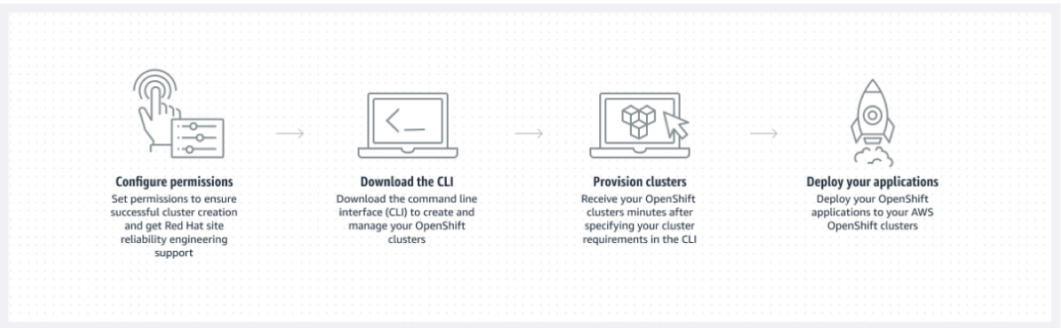
- ROSA consola: proporciona una interfaz web para permitir la ROSA suscripción y la compra de un contrato de ROSA software.

- AWS Command Line Interface (AWS CLI): proporciona comandos para un amplio conjunto de sistemas Servicios de AWS y es compatible con Windows, macOS y Linux. Para obtener más información, consulte AWS Command Line Interface.

Red Hat OpenShift

- Red Hat Hybrid Cloud Console: proporciona una interfaz web para crear, actualizar y gestionar ROSA clústeres, instalar complementos para clústeres y crear e implementar aplicaciones en un ROSA clúster.
- ROSA CLI (rosa): proporciona comandos para crear, actualizar y administrar ROSA clústeres.
- OpenShift CLI (oc): proporciona comandos para crear aplicaciones y administrar proyectos de OpenShift Container Platform.
- Knative CLI (kn): proporciona comandos que se pueden usar para interactuar con componentes OpenShift sin servidor, como Knative Serving y Eventing.
- Pipelines CLI (tkn): proporciona comandos para interactuar con OpenShift Pipelines mediante el terminal.
- opm CLI: proporciona comandos que ayudan a los desarrolladores de operadores y administradores de clústeres a crear y mantener los catálogos de OpenShift operadores desde la terminal.
- CLI del SDK para operadores: proporciona comandos que un desarrollador de operadores puede usar para crear, probar e implementar un OpenShift operador.

¿Cómo empezar con ROSA



A continuación se resume el proceso de introducción de ROSA. Para obtener instrucciones de introducción detalladas, consulteComience con ROSA .

Consola de administración de AWS/AWS CLI

1. Configure los permisos en los Servicios de AWS que ROSA se basa la prestación de la funcionalidad del servicio. Para obtener más información, consulte the section called “Requisitos previos”.
2. Instale y configure la AWS CLI herramienta más reciente. Para obtener más información, consulte Instalación o actualización de la última versión de AWS CLI en la Guía del AWS CLI usuario.
3. ROSA Actívela en la ROSA consola.

ROSA Consola/CLI de Red Hat Hybrid Cloud

1. Descargue la última versión de la ROSA CLI y la OpenShift CLI desde Red Hat Hybrid Cloud Console. Para obtener más información, consulte Introducción a la ROSA CLI en la documentación de Red Hat.
2. Cree ROSA clústeres en la consola Red Hat Hybrid Cloud Console o con la ROSA CLI.
3. Cuando el clúster esté listo, configure un proveedor de identidades para conceder acceso al clúster a los usuarios.
4. Implemente y gestione las cargas de trabajo en su ROSA clúster de la misma forma que lo haría en cualquier otro OpenShift entorno.

Precios

El costo total de ROSA consta de dos componentes: tarifas de ROSA servicio y tarifas de AWS infraestructura. Para obtener más información sobre los precios, consulte Precios de Red Hat OpenShift Service en AWS.

ROSA tarifas de servicio

De forma predeterminada, las tarifas de ROSA servicio se acumulan bajo demanda a una tarifa por hora por cada 4 vCPU utilizadas por los nodos de trabajo. Las tarifas de servicio son uniformes en todas las regiones AWS estándar compatibles. Además de la tarifa de servicio del nodo trabajador, ROSA con clústeres de planes de control alojados (HCP) conlleva una tarifa de clúster por hora.

ROSA ofrece contratos de tarifas de servicio de 1 y 3 años que puede adquirir para ahorrar en las tarifas de servicio bajo demanda para los nodos de trabajo. Para obtener más información, consulte the section called “Comprar un ROSA contrato”.

AWS tarifas de infraestructura

AWS las tarifas de infraestructura se aplican a los nodos de trabajo subyacentes, los nodos de infraestructura, los nodos del plano de control, el almacenamiento y los recursos de red alojados en la infraestructura AWS global. AWS las tarifas de infraestructura varían según Región de AWS.

Resumen de las responsabilidades de ROSA

Esta documentación describe las responsabilidades de Amazon Web Services (AWS), Red Hat y los clientes en relación con el Red Hat OpenShift Service en AWS (ROSA) servicio gestionado. Para obtener más información sobre las políticas ROSA y sus componentes, consulte las políticas y la definición del servicio en la documentación de Red Hat.

El modelo de responsabilidad AWS compartida define la AWS responsabilidad de proteger la infraestructura en la que se ejecutan todos los servicios que se ofrecen en él Nube de AWS, incluidos ROSA los siguientes: AWS la infraestructura incluye el hardware, el software, las redes y las instalaciones que ejecutan Nube de AWS los servicios. Esta AWS responsabilidad se denomina comúnmente «seguridad de la nube». Para funcionar ROSA como un servicio totalmente gestionado, Red Hat y el cliente son responsables de los elementos del servicio que el modelo de AWS responsabilidad define como «seguridad en la nube».

Red Hat es responsable de la administración y la seguridad continuas de la infraestructura del ROSA clúster, la plataforma de aplicaciones subyacente y el sistema operativo. Si bien ROSA los clústeres se alojan en AWS los recursos del cliente Cuentas de AWS, los componentes de ROSA servicio y los ingenieros de confiabilidad del sitio de Red Hat (SREs) acceden a ellos de forma remota mediante IAM funciones que el cliente crea. Red Hat utiliza este acceso para administrar la implementación y la capacidad de todos los nodos del plano de control y de la infraestructura del clúster, y para mantener las versiones de los nodos del plano de control, los nodos de la infraestructura y los nodos de trabajo.

Red Hat y el cliente comparten la responsabilidad de la administración de la ROSA red, el registro de clústeres, el control de versiones de los clústeres y la administración de la capacidad. Si bien Red Hat administra el ROSA servicio, el cliente es totalmente responsable de administrar y proteger las aplicaciones, las cargas de trabajo y los datos en los que se desplieguen. ROSA

Descripción general de

La siguiente tabla proporciona una descripción general de las AWS responsabilidades de Red Hat y del cliente al respecto. Red Hat OpenShift Service en AWS

> **Note**
>
> Si el rol de `cluster-admin` se agrega a un usuario, consulte las notas sobre responsabilidades y exclusiones en el Anexo 4 del contrato de Red Hat Enterprise (Servicios de suscripción en línea).

Resource	Administración de incidentes y operaciones	Administración de cambios	Autorización de identidad y acceso	Seguridad y conformidad con las regulaciones	Recuperación de desastres
Datos del cliente	Cliente	Cliente	Cliente	Cliente	Cliente
Aplicaciones del cliente	Cliente	Cliente	Cliente	Cliente	Cliente
Servicios para desarrolladores	Cliente	Cliente	Cliente	Cliente	Cliente
Monitoreo de la plataforma	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Registro	Red Hat	Red Hat y el cliente	Red Hat y el cliente	Red Hat y el cliente	Red Hat
Redes de aplicaciones	Red Hat y el cliente	Red Hat y el cliente	Red Hat y el cliente	Red Hat	Red Hat
Redes de clústeres	Red Hat	Red Hat y el cliente	Red Hat y el cliente	Red Hat	Red Hat
Administración de redes virtuales	Red Hat y el cliente	Red Hat y el cliente	Red Hat y el cliente	Red Hat y el cliente	Red Hat y el cliente

Resource	Administración de incidentes y operaciones	Administración de cambios	Autorización de identidad y acceso	Seguridad y conformidad con las regulaciones	Recuperación de desastres
Administración de computación virtual (plano de control, infraestructura y nodos de trabajo)	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Versión del clúster	Red Hat	Red Hat y el cliente	Red Hat	Red Hat	Red Hat
Administración de la capacidad	Red Hat	Red Hat y el cliente	Red Hat	Red Hat	Red Hat
Administración del almacenamiento virtual	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS software (público Servicios de AWS)	AWS	AWS	AWS	AWS	AWS
Hardware/ infraestructura global AWS	AWS	AWS	AWS	AWS	AWS

Tareas de responsabilidades compartidas por área

AWS, Red Hat y los clientes comparten la responsabilidad de la supervisión y el mantenimiento de los ROSA componentes. Esta documentación define las responsabilidades de ROSA servicio por área y tarea.

Administración de incidentes y operaciones

AWS es responsable de proteger la infraestructura de hardware en la que se ejecutan todos los servicios que se ofrecen en Nube de AWS. Red Hat es responsable de administrar los componentes de servicio necesarios para la red de plataformas predeterminadas. El cliente es responsable de la administración de los incidentes y las operaciones de los datos de las aplicaciones del cliente y de cualquier red personalizada que el cliente haya configurado.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Redes de aplicaciones	Red Hat • Supervise OpenShift el servicio del router nativo y responda a las alertas.	Cliente • Monitorear el estado de las rutas de las aplicaciones y los puntos de conexión detrás de ellas. • Informe las interrupciones a Red Hat AWS y a Red Hat.
Administración de redes virtuales	Red Hat • Supervise los balanceadores de AWS carga, Amazon VPC las subredes y Servicio de AWS los componentes necesarios para la red de plataforma predeterminada. Responder a alertas.	Cliente • Supervise el estado de los puntos finales del AWS equilibrador de carga. • Supervise el tráfico de red que se configura opcionalmente mediante Amazon VPC una conexión a una VPC, Site-to-Site VPN una conexión o Direct Connect para detectar posibles

Resource	Responsabilidades del servicio	Responsabilidades del cliente
		problemas o amenazas de seguridad.
Administración del almacenamiento virtual	Red Hat • Supervise Amazon EBS los volúmenes que se utilizan para los nodos del clúster y los Amazon S3 depósitos que se utilizan para el registro de imágenes de contenedores integrado en el ROSA servicio. Responder a alertas.	Cliente • Monitorear el estado de los datos de la aplicación. • Si AWS KMS keys se utilizan sistemas gestionados por el cliente, cree y controle el ciclo de vida de las claves y las políticas de Amazon EBS cifrado.
AWS software (público Servicios de AWS)	AWS • Para obtener información sobre la gestión de AWS incidentes y operaciones, consulte Cómo se AWS mantiene la resiliencia operativa y la continuidad del servicio en el AWS documento técnico.	Cliente • Supervise el estado de AWS los recursos de la cuenta del cliente. • Utilice IAM las herramientas para aplicar los permisos adecuados a AWS los recursos de la cuenta del cliente.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Hardware/infraestructura global AWS	AWS • Para obtener información sobre la gestión de AWS incidentes y operaciones, consulte Cómo se AWS mantiene la resiliencia operativa y la continuidad del servicio en el AWS documento técnico.	Cliente • Configurar, administrar y monitorear las aplicaciones y los datos de los clientes para garantizar que los controles de seguridad de las aplicaciones y los datos se apliquen correctamente.

Administración de cambios

AWS es responsable de proteger la infraestructura de hardware en la que se ejecutan todos los servicios que se ofrecen en el. Nube de AWS Red Hat es responsable de permitir los cambios en la infraestructura y los servicios del clúster que el cliente controlará, así como de mantener las versiones para los nodos del plano de control, los nodos de la infraestructura y los nodos de trabajo. El cliente es responsable de iniciar los cambios en la infraestructura. El cliente también es responsable de instalar y mantener los servicios opcionales, las configuraciones de las redes en el clúster, y los cambios en los datos y las aplicaciones del cliente.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Registro	Red Hat • Agregar y monitorear de forma centralizada los registros de auditoría de la plataforma. • Proporcionar y mantener un operador de registro para que el cliente pueda implementar una pila de	Cliente • Instalar el operador de registro de aplicaciones predeterminado opcional en el clúster. • Instalar, configurar y mantener cualquier solución de registro de aplicaciones opcional, como contenedo

Resource	Responsabilidades del servicio	Responsabilidades del cliente
	registro para el registro predeterminado de las aplicaciones. • Proporcionar registros de auditoría a pedido del cliente.	res laterales de registro o aplicaciones de registro de terceros. • Ajustar el tamaño y la frecuencia de los registros de aplicaciones que generan las aplicaciones de los clientes si afectan a la estabilidad de la pila de registros o del clúster. • Solicitar los registros de auditoría de la plataform a a través de un caso de asistencia para investigar incidentes específicos.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Redes de aplicaciones	Red Hat • Configurar equilibradores de carga públicos. Ofrecer la posibilidad de configurar equilibradores de carga privados y hasta un equilibrador de carga adicional cuando sea necesario. • Configure el servicio de OpenShift router nativo. Ofrecer la posibilidad de configurar el enrutador como privado y añadir hasta una partición adicional del enrutador. • Instale, configure y mantenga los componentes de OpenShift SDN para el tráfico del pod interno predeterminado. • Brindarle al cliente la posibilidad de administrar objetos de `NetworkPolicy` y `EgressNetworkPolicy` (firewall).	Cliente • Configurar los permisos de red de los pods no predeterminados para las redes de proyectos y de pods, así como para la entrada y salida de pods mediante objetos de la `NetworkPolicy` . • Usa OpenShift Cluster Manager para solicitar un balanceador de cargas privado para las rutas de aplicaciones predeterminadas. • Use OpenShift Cluster Manager para configurar hasta un fragmento de router público o privado adicional y el balanceador de carga correspondiente. • Solicitar y configurar cualquier equilibrador de carga de servicios adicional para servicios específicos. • Configurar las reglas de reenvío del DNS necesarias.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Redes de clústeres	Red Hat • Configure los component es de administración de clústeres, como los puntos finales de servicios públicos o privados y la integraci ón necesaria con los componentes. Amazon VPC • Configurar los component es de red internos necesario s para la comunicación interna del clúster entre los nodos de trabajo, de la infraestructura y del plano de control.	Cliente • Proporcione rangos de direcciones IP opcionales no predeterminados para el CIDR de máquina, el CIDR de servicio y el CIDR de pod si es necesario a través de OpenShift Cluster Manager cuando se aprovisione el clúster. • Solicita que el punto final del servicio de API se haga público o privado al crear el clúster o después de crearlo mediante Cluster Manager. OpenShift

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Administración de redes virtuales	Red Hat • Configure y configure Amazon VPC los componentes necesarios para aprovisionar el clúster, como subredes, balancead ores de carga, puertas de enlace de Internet y puertas de enlace NAT. • Proporcione al cliente la capacidad de administrar la Site-to-Site VPN conectivi dad con recursos locales, la conectividad a la Amazon VPC VPC y, Direct Connect según sea necesario, a través OpenShift de Cluster Manager. • Permita a los clientes crear e implementar balancead ores de AWS carga para usarlos con balanceadores de carga de servicios.	Cliente • Configure y mantenga Amazon VPC los componentes opcionales, como la conexión Amazon VPC a VPC, la Site-to-S ite VPN conexión o. Direct Connect • Solicitar y configurar cualquier equilibrador de carga adicional para servicios específicos.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Administración de computación virtual	Red Hat • Configure y configure el plano de ROSA control y el plano de datos para usar Amazon EC2 instancias para la computación en clústeres. • Supervise y gestione el despliegue del plano de Amazon EC2 control y los nodos de infraestructura en el clúster.	Cliente • Supervise y administre los Amazon EC2 nodos de trabajo mediante la creación de un grupo de máquinas mediante el administrador de OpenShift clústeres o la ROSA CLI. • Administrar los cambios en las aplicaciones y los datos de las aplicacio nes implementadas por el cliente.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Versión del clúster	Red Hat • Habilitar el proceso de programación de actualizaciones. • Supervisar el progreso de la actualización y solucionar los problemas encontrados. • Publicar los registros de cambios y las notas de la versión para las actualizaciones secundarias y de mantenimiento.	Cliente • Programar las actualizaciones de las versiones de mantenimiento de forma inmediata, para el futuro, o realizar actualizaciones automáticas. • Reconocer y programar las actualizaciones de las versiones secundarias. • Garantizar que la versión del clúster permanezca en una versión secundaria compatible. • Probar las aplicaciones del cliente en versiones secundarias y de mantenimiento para garantizar la compatibilidad.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Administración de la capacidad	Red Hat • Monitorear el uso del plano de control. Los planos de control incluyen nodos del plano de control y nodos de la infraestructura. • Escalar y cambiar el tamaño de los nodos del plano de control para mantener la calidad del servicio.	Cliente • Supervisar la utilización de los nodos de trabajo y, si corresponde, habilitar la característica de escalado automático. • Determinar la estrategia de escalado del clúster. • Utilice los controles del administrador de OpenShift clústeres proporcionados para añadir o eliminar nodos de trabajo adicionales según sea necesario. • Responder a las notificac iones de Red Hat relaciona das con los requisitos de recursos del clúster.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Administración del almacenamiento virtual	Red Hat • Configúrelo y Amazon EBS configúrelo para aprovisionar el almacenamiento de nodos locales y el almacenamiento de volumen persistente para el clúster. • Configure y configure el registro de imágenes integrado para usar el almacenamiento en Amazon S3 cubos. • Reduzca periódicamente los recursos de registro de imágenes Amazon S3 para optimizar el Amazon S3 uso y el rendimiento del clúster.	Cliente • Si lo desea, configure el controlador Amazon EBS CSI o el controlador Amazon EFS CSI para aprovisionar volúmenes persistentes en el clúster.

Resource	Responsabilidades del servicio	Responsabilidades del cliente

AWS software (servicios públicos AWS)	AWS
	
	Computación
	
	• Proporcione el Amazon EC2 servicio, que se utiliza para ROSA el plano de control, la infraestructura y los nodos de trabajo.
	
	Almacenamiento
	
	• Se proporciona Amazon EBS para permitir que el ROSA servicio aprovisione almacenamiento en nodos locales y almacenamiento en volumen persistente para el clúster.
	
	Redes
	
	• Proporcione los siguiente s Nube de AWS servicios para satisfacer las necesidades de infraestr uctura de redes ROSA virtuales:
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• Proporcione las siguientes Servicio de AWS integraci
		Cliente
		
		• Firme las solicitudes con un identificador de clave de acceso y una clave de acceso secreta asociadas a una credencial de seguridad IAM principal o AWS STS temporal.
		• Especificar las subredes de VPC para que el clúster las utilice durante la creación del clúster.
		• Si lo desea, configure una VPC administrada por el cliente para usarla con clústeres. ROSA

Resource	Responsabilidades del servicio	Responsabilidades del cliente
	ones opcionales para ROSA: • Site-to-Site VPN • Direct Connect • AWS PrivateLink • AWS Transit Gateway	
Hardware/infraestructura global AWS	AWS • Para obtener informaci ón sobre los controles de administración de AWS los centros de datos, consulte Nuestros controles en la página de Nube de AWS seguridad. • Para obtener información sobre las mejores prácticas de gestión de cambios, consulte la Guía para la gestión de cambios AWS en la biblioteca de AWS soluciones.	Cliente • Implementar las prácticas recomendadas de administr ación de cambios para las aplicaciones y los datos de los clientes alojados en la Nube de AWS.

Autorización de identidad y acceso

La autorización de identidad y acceso incluye las responsabilidades de administrar el acceso autorizado a los clústeres, las aplicaciones y los recursos de infraestructura. Esto incluye tareas como proporcionar mecanismos de control de acceso, autenticación, autorización y administrar el acceso a los recursos.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Registro	Red Hat • Adherirse a un proceso de acceso interno por niveles basado en los estándares del sector para los registros de auditoría de la plataform a. • Proporcione capacidades de OpenShift RBAC nativas.	Cliente • Configure el OpenShift RBAC para controlar el acceso a los proyectos y, por extensión, a los registros de las aplicaciones de un proyecto. • En el caso de las solucione s de registro de aplicacio nes personalizadas o de terceros, el cliente es responsable de la administr ación del acceso.
Redes de aplicaciones	Red Hat • Proporcione capacidades y OpenShift RBAC nativos. `dedicated-admin`	Cliente • Configure un OpenShift `dedicated-admin` RBAC para controlar el acceso a la configuración de la ruta según sea necesario. • Administre a los administr adores de la organizac ión de Red Hat para que Red Hat conceda acceso a OpenShift Cluster Manager. El administrador de clústeres se utiliza para configurar las opciones del enrutador y proporcio nar una service quota del equilibrador de carga.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Redes de clústeres	Red Hat • Proporcione controles de acceso a los clientes a través de OpenShift Cluster Manager. Proporcione capacidades y OpenShift `dedicated-admin` RBAC nativos.	Cliente • Configure un OpenShift `dedicated-admin` RBAC para controlar el acceso a la configuración de la ruta según sea necesario. • Administrar la membresía de la organización de Red Hat de cuentas de Red Hat. • Administre a los administr adores de la organización para que Red Hat conceda acceso a OpenShift Cluster Manager.
Administración de redes virtuales	Red Hat • Proporcione controles de acceso a los clientes a través de OpenShift Cluster Manager.	Cliente • Gestione el acceso opcional de los usuarios a AWS los componentes a través de OpenShift Cluster Manager.
Administración de computaci ón virtual	Red Hat • Proporcione controles de acceso a los clientes a través de OpenShift Cluster Manager.	Cliente • Gestione el acceso opcional de los usuarios a AWS los componentes a través de OpenShift Cluster Manager. • Cree las IAM funciones y las políticas adjuntas necesaria s para permitir el acceso al ROSA servicio.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Administración del almacenamiento virtual	Red Hat • Proporcione controles de acceso a los clientes a través de OpenShift Cluster Manager.	Cliente • Gestione el acceso opcional de los usuarios a AWS los componentes a través de OpenShift Cluster Manager. • Cree las IAM funciones y las políticas adjuntas necesarias para permitir el acceso al ROSA servicio.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
AWS software (AWS servicios públicos)	AWS Computación • Proporcione el Amazon EC2 servicio, que se utiliza para ROSA el plano de control, la infraestructura y los nodos de trabajo. Almacenamiento • Provide Amazon EBS, que se utiliza ROSA para permitir el aprovisionamiento de almacenamiento en nodos locales y almacenamiento de volumen persistente para el clúster. • Provide Amazon S3, que se utiliza para el registro de imágenes integrado en el servicio. Redes • Provide AWS Identity and Access Management (IAM), que utilizan los clientes para controlar el acceso a ROSA los recursos que se encuentran en las cuentas de los clientes.	Cliente • Cree las IAM funciones y las políticas adjuntas necesarias para permitir el acceso al ROSA servicio. • Utilice IAM las herramientas para aplicar los permisos adecuados a AWS los recursos de la cuenta del cliente. • Para activarlos ROSA en toda AWS la organización, el cliente es responsable de administrar AWS Organizations los administradores. • Para ROSA activarlo en toda su AWS organización, el cliente es responsable de distribuir la subvención de ROSA prestaciones mediante. AWS License Manager

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Hardware/infraestructura global AWS	AWS • Para obtener informaci ón sobre los controles de acceso físico a AWS los centros de datos, consulte Nuestros controles en la página de Nube de AWS seguridad.	Cliente • El cliente no es responsab le de la infraestructura AWS global.

Seguridad y conformidad con las regulaciones

A continuación, se detallan las responsabilidades y los controles relacionados con la conformidad:

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Registro	Red Hat • Enviar los registros de auditoría del clúster a una SIEM de Red Hat para analizarlos en busca de eventos de seguridad . Retener los registros de auditoría durante un período de tiempo definido para respaldar el análisis forense.	Cliente • Analizar los registros de las aplicaciones para detectar eventos de seguridad. • Enviar los registros de las aplicaciones a un punto de conexión externo mediante contenedores auxiliares de registro o aplicaciones de registro de terceros si es necesario conservar los durante más tiempo que el que ofrece la pila de registros predeterminada.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Administración de redes virtuales	Red Hat • Monitorear los componentes de la red virtual para detectar posibles problemas y amenazas de seguridad. • Utilice AWS herramientas públicas para una supervisión y protección adicionales.	Cliente • Monitorear los componentes de la red virtual configurada para detectar posibles problemas y amenazas de seguridad. • Configurar las reglas de firewall necesarias o las protecciones del centro de datos del cliente según sea necesario.
Administración de computación virtual	Red Hat • Supervisar los componentes virtuales de computación para detectar posibles problemas y amenazas de seguridad. • Utilice AWS herramientas públicas para una supervisión y protección adicionales.	Cliente • Monitorear los componentes de la red virtual configurada para detectar posibles problemas y amenazas de seguridad. • Configurar las reglas de firewall necesarias o las protecciones del centro de datos del cliente según sea necesario.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Administración del almacenamiento virtual	Red Hat • Supervisar los componentes del almacenamiento virtual para detectar posibles problemas y amenazas de seguridad. • Utilice AWS herramientas públicas para una supervisión y protección adicionales. • Configure el ROSA servicio para cifrar los datos del plano de control, la infraestructura y el volumen de los nodos de trabajo de forma predeterminada mediante la clave KMS AWS administrada que se Amazon EBS proporciona. • Configure el ROSA servicio para cifrar los volúmenes persistentes de los clientes que utilizan la clase de almacenamiento predeterminada con la clave de KMS AWS administrada que se Amazon EBS proporciona. • Proporcione al cliente la posibilidad de utilizar un sistema gestionado por el cliente KMS key para cifrar los volúmenes persistentes.	Cliente • Amazon EBS Volúmenes de aprovisionamiento. • Administre Amazon EBS el almacenamiento por volumen para garantizar que haya suficiente espacio de almacenamiento disponible para montarlo como volumen ROSA. • Cree la declaración de volumen persistente y genere un volumen persistente a través de OpenShift Cluster Manager.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
	• Configure el registro de imágenes del contenedor para cifrar los datos de registro de imágenes en reposo mediante el cifrado del lado del servidor con claves Amazon S3 administradas (SSE-3). • Ofrezca al cliente la posibilidad de crear un registro de imágenes público o privado para proteger las Amazon S3 imágenes del contenedor del acceso de usuarios no autorizados.	

Resource	Responsabilidades del servicio	Responsabilidades del cliente
AWS software (AWS servicios públicos)	AWS Computación • Proporcione Amazon EC2, que se utiliza para ROSA el plano de control, la infraestructura y los nodos de trabajo. Para obtener más información, consulte Seguridad de la infraestructura Amazon EC2 en la Guía del Amazon EC2 usuario. Almacenamiento • Proporcione Amazon EBS, que se utiliza para los volúmenes del plano de ROSA control, la infraestructura y los nodos de trabajo, así como para los volúmenes persistentes de Kubernetes. Para obtener más información, consulte Protección de datos Amazon EC2 en la Guía del Amazon EC2 usuario. • Provide AWS KMS, que se ROSA utiliza para cifrar los volúmenes del plano de control, la infraestructura y	Cliente • Asegúrese de seguir las mejores prácticas de seguridad y el principio del privilegio mínimo para proteger los datos de la Amazon EC2 instancia. Para obtener más información, consulte Seguridad de la infraestructura en Amazon EC2 y Protección de los datos en Amazon EC2. • Monitorear los componentes de la red virtual configurada para detectar posibles problemas y amenazas de seguridad. • Configurar las reglas de firewall necesarias o las protecciones del centro de datos del cliente según sea necesario. • Cree una clave KMS opcional administrada por el cliente y cifre el volumen Amazon EBS persistente con la clave KMS. • Monitorear los datos del cliente en el almacenamiento virtual para detectar posibles problemas y amenazas de seguridad.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
	los nodos de trabajo y los volúmenes persistentes. Para obtener más informaci ón, consulte el Amazon EBS cifrado en la Guía del Amazon EC2 usuario. • Provide Amazon S3, que se utiliza para el registro de imágenes de contenedo res integrado en el servicio ROSA. Para obtener más información, consulte la Amazon S3 sección de seguridad en la Guía Amazon S3 del usuario. Redes • Proporcione capacidades y servicios de seguridad para aumentar la privacidad y controlar el acceso a la red en la infraestructura AWS global, incluidos los firewalls de red integrados Amazon VPC, las conexiones de red privadas o dedicadas y el cifrado automático de todo el tráfico de las redes AWS globales y regionale s entre instalaciones AWS seguras. Para obtener más información, consulte el modelo de responsab	Para obtener más informaci ón, consulte Modelo de responsabilidad compartida de AWS.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
	ilidad AWS compartida y la seguridad de la infraestructura en el documento técnico Introducción a la AWS seguridad.	
Hardware/infraestructura global AWS	AWS • Proporcione la infraestructura AWS global que se ROSA utiliza para ofrecer la funcionalidad del servicio. Para obtener más información sobre los controles de AWS seguridad, consulte Seguridad de la AWS infraestructura en el AWS documento técnico. • Proporcione documentación para que el cliente gestione las necesidades de cumplimiento y compruebe su estado de seguridad AWS mediante herramientas como AWS Artifact AWS Security Hub.	Cliente • Configurar, administrar y monitorear las aplicaciones y los datos de los clientes para garantizar que los controles de seguridad de las aplicaciones y los datos se apliquen correctamente. • Utilice IAM las herramientas para aplicar los permisos adecuados a AWS los recursos de la cuenta del cliente.

Recuperación ante desastres

La recuperación de desastres incluye las copias de seguridad de los datos y la configuración, la replicación de datos y la configuración del entorno de recuperación de desastres, y la conmutación por error en caso de desastre.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
Administración de redes virtuales	Red Hat • Restaurar o volver a crear los componentes de la red virtual afectados que son necesarios para que la plataforma funcione.	Cliente • Configurar las conexiones de redes virtuales con más de un túnel siempre que sea posible para protegerse contra las interrupciones. • Mantener el DNS de conmutación por error y el equilibrio de carga si se utiliza un equilibrador de carga global con varios clústeres.
Administración de computación virtual	Red Hat • Supervise el clúster y sustituya los nodos de infraestructura o del plano de Amazon EC2 control que hayan fallado. • Ofrecer al cliente la posibilidad de reemplazar de forma manual o automática los nodos de trabajo defectuosos.	Cliente • Reemplace los Amazon EC2 nodos de trabajo defectuosos editando la configuración del grupo de máquinas mediante OpenShift Cluster Manager o la ROSA CLI.
Administración del almacenamiento virtual	Red Hat • En el ROSA caso de los clústeres creados con credenciales de AWS IAM usuario, haga una copia de seguridad de todos los	Cliente • Realizar copias de seguridad de las aplicaciones y los datos de las aplicaciones de los clientes.

Resource	Responsabilidades del servicio	Responsabilidades del cliente
	objetos de Kubernetes del clúster mediante instantán eas de los volúmenes por hora, día y semana.	

Resource	Responsabilidades del servicio	Responsabilidades del cliente
AWS software (servicios públicos) AWS	AWS Computación • Proporcione Amazon EC2 funciones que respalden la resiliencia de los datos, como Amazon EBS instantáneas y. Amazon EC2 Auto Scaling Para obtener más informaci ón, consulte Resiliencia Amazon EC2 en la Guía del Amazon EC2 usuario. Almacenamiento • Ofrezca al ROSA servicio y a los clientes la posibilid ad de hacer copias de seguridad del Amazon EBS volumen del clúster mediante instantáneas del Amazon EBS volumen. • Para obtener informaci ón sobre Amazon S3 las funciones que respaldan la resiliencia de los datos, consulte Resiliencia en. Amazon S3 Redes	Cliente • Configure los clústeres ROSA Multi-AZ para mejorar la tolerancia a errores y la disponibilidad de los clústeres. • Aprovisione volúmenes persistentes mediante el controlador Amazon EBS CSI para habilitar las instantáneas de los volúmenes. • Cree instantáneas de volúmenes persistentes en CSI. Amazon EBS

Resource	Responsabilidades del servicio	Responsabilidades del cliente
	• Para obtener información sobre Amazon VPC las funciones que respaldan la resiliencia de los datos, consulte Resiliencia Amazon Virtual Private Cloud en la Guía del Amazon VPC usuario.	
Hardware/infraestructura global AWS	AWS • Proporcione una infraestructura AWS global que permita ROSA escalar el plano de control, la infraestructura y los nodos de trabajo en todas las zonas de disponibilidad. Esta funcionalidad permite ROSA organizar la conmutación por error automática entre zonas sin interrupciones. • Para obtener más información sobre las prácticas recomendadas de recuperación ante desastres, consulte Opciones de recuperación ante desastres en la nube en AWS Well-Architected Framework.	Cliente • Configure los clústeres ROSA Multi-AZ para mejorar la tolerancia a errores y la disponibilidad de los clústeres.

Responsabilidades del cliente en relación con los datos y las aplicaciones

El cliente es responsable de las aplicaciones, las cargas de trabajo y los datos en los que se despliegan. Red Hat OpenShift Service en AWS Sin embargo, AWS Red Hat proporciona varias herramientas para ayudar al cliente a gestionar los datos y las aplicaciones en la plataforma.

Resource	¿Cómo AWS ayuda Red Hat?	Responsabilidades del cliente
Datos del cliente	Red Hat • Mantener los estándares de cifrado de datos a nivel de plataforma, tal como se definen en los estándares de seguridad y conformidad del sector. • Proporcione OpenShift componentes que ayuden a gestionar los datos de las aplicaciones, como los secretos. • Habilite la integración con los servicios de datos, por ejemplo, Amazon RDS para almacenar y administrar datos fuera del clúster y/o AWS. AWS • Permiten a los clientes almacenar y gestionar los datos fuera del clúster. Amazon RDS	Cliente • Ser responsable de todos los datos de los clientes almacenados en la plataforma y de la forma en que las aplicaciones de los clientes consumen y exponen estos datos.
Aplicaciones del cliente	Red Hat	Cliente

Resource	¿Cómo AWS ayuda Red Hat?	Responsabilidades del cliente
	• Aprovisione los clústeres con OpenShift los componentes instalados para que los clientes puedan acceder a ellos OpenShift y a Kubernetes APIs para implementar y administrar las aplicaciones en contenedores. • Crear clústeres con secretos sobre la extracción de imágenes para que las implementaciones de los clientes puedan extraer imágenes del registro del catálogo contenedor de Red Hat. • Proporcione un acceso OpenShift APIs que un cliente pueda usar para configurar los operadores y añadir servicios comunitarios, de terceros y de Red Hat al clúster. AWS • Proporcionar complementos y clases de almacenamiento para admitir volúmenes persistentes y utilizarlos con las aplicaciones de los clientes. • Proporcionar un registro de imágenes de contenedores para que los clientes puedan almacenar de forma	• Ser responsable de las aplicaciones, los datos y todo el ciclo de vida de las aplicaciones de clientes y terceros. • Si un cliente agrega al clúster servicios de Red Hat, comunitarios, de terceros, propios o de otro tipo mediante operadores o imágenes externas, el cliente es responsable de estos servicios y de trabajar con el proveedor correspondiente (incluido Red Hat) para solucionar cualquier problema. • Utilizar las herramientas y las características proporcionadas para configurar e implementar; mantenerse actualizado; configurar las solicitudes y los límites de recursos; dimensionar el clúster para tener suficientes recursos para ejecutar aplicaciones; configurar permisos; integrarse con otros servicios; administrar cualquier flujo de imágenes o plantillas que el cliente implemente; servir externamente; hacer copias de seguridad

Resource	¿Cómo AWS ayuda Red Hat?	Responsabilidades del cliente
	segura las imágenes de los contenedores de aplicacio nes en el clúster para implementar y administrar las aplicaciones. AWS • Amazon EBS Permiten admitir volúmenes persisten tes para su uso con las aplicaciones de los clientes. • Amazon S3 Permiten respaldar el aprovisio namiento por Red Hat del registro de imágenes de contenedores.	, guardar y restaurar datos; y administrar sus cargas de trabajo resilientes y de alta disponibilidad. • Mantenga la responsab ilidad de monitorear las aplicaciones en las que se ejecutan Red Hat OpenShift Service en AWS, incluida la instalación y el funcionam iento del software para recopilar métricas, crear alertas y proteger los secretos de la aplicación.

ROSA arquitectura

Red Hat OpenShift Service en AWS (ROSA) tiene las siguientes topologías de clúster:

- Plano de control hospedado (HCP): el plano de control se aloja en Red Hat Cuenta de AWS y es administrado por Red Hat. Los nodos de trabajo se implementan en los del Cuenta de AWS cliente.
- Clásico: el plano de control y los nodos de trabajo se despliegan en el plano de control y los nodos de trabajo del cliente Cuenta de AWS.

ROSA con HCP ofrece una arquitectura de plano de control más eficiente que ayuda a reducir las tarifas de AWS infraestructura que se deben pagar al ejecutarse ROSA y permite crear clústeres más rápidamente. Tanto ROSA con HCP como ROSA classic se pueden habilitar en la AWS ROSA consola. Tiene la opción de seleccionar la arquitectura que quiere usar al aprovisionar ROSA clústeres mediante la ROSA CLI.

Note

- ROSA ofrece certificaciones de cumplimiento FedRAMP High y HIPAA AWS GovCloud en arquitecturas de plano de control clásicas y alojadas. Para más información, consulte Conformidad en la documentación de Red Hat.
- ROSA ofrece terminales con el estándar federal de procesamiento de información (FIPS) tanto en arquitecturas de plano de control clásicas como AWS GovCloud alojadas.

Comparación de ROSA con HCP y ROSA classic

En la siguiente tabla se compara ROSA con los modelos de arquitectura clásica de HCP y ROSA.

	ROSA con HCP	ROSA clásico
Alojamiento de la infraestructura de clústeres	Los componentes del plano de control, como etcd, el servidor API y oauth, están alojados en un servidor propiedad de Red Hat. Cuenta de AWS	Los componentes del plano de control, como etcd, el servidor API y oauth, se alojan en una propiedad del cliente. Cuenta de AWS
Amazon VPC	Los nodos trabajadores se comunican directamente con el plano de control. AWS PrivateLink	Los nodos de trabajo y los nodos del plano de control se implementan en la VPC del cliente.
AWS Identity and Access Management	Utiliza políticas AWS administradas.	Utiliza políticas administradas por el cliente definidas por el servicio.
Despliegue multizona	El plano de control se implementa en varias zonas de disponibilidad (AZs).	El plano de control se puede implementar en una única zona de disponibilidad o en varias AZs.
Nodos de infraestructura	No utiliza nodos de infraestructura dedicados. Los	Utiliza dos nodos dedicados en una sola zona de disponibi

	ROSA con HCP	ROSA clásico
	componentes de la plataforma se implementan en los nodos de trabajo.	lidad o tres en zonas de disponibilidad múltiples para alojar los componentes de la plataforma.
OpenShift capacidades	La supervisión de la plataform a, el registro de imágenes y el controlador de entrada se implementan en los nodos de trabajo.	La supervisión de la plataform a, el registro de imágenes y el controlador de entrada se implementan en nodos de infraestructura dedicados.
Actualizaciones de clústeres	El plano de control y cada grupo de máquinas se pueden actualizar por separado.	Se debe actualizar todo el clúster al mismo tiempo.
Espacio Amazon EC2 mínimo	Se necesitan dos Amazon EC2 instancias para crear un clúster.	Se necesitan siete instancia s Single-AZ o nueve Amazon EC2 instancias Multi-AZ para crear un clúster.
Regiones de AWS	Para conocer la Región de AWS disponibilidad, consulte los Red Hat OpenShift Service en AWS puntos finales y las cuotas en la Guía de referenci a AWS general.	Para conocer Región de AWS la disponibilidad, consulte los Red Hat OpenShift Service en AWS puntos finales y las cuotas en la Guía de referenci a AWS general.

Comience con ROSA

Red Hat OpenShift Service en AWS (ROSA) es un servicio gestionado que puede utilizar para crear, escalar e implementar aplicaciones en contenedores con la plataforma OpenShift empresarial Kubernetes de Red Hat activada. AWS

Puede utilizar las siguientes guías para crear su primer ROSA clúster, conceder acceso a los usuarios, implementar su primera aplicación y aprender a revocar el acceso de los usuarios y eliminar su clúster.

- the section called “Crear un clúster ROSA de HCP: CLI”- Cree su primera ROSA con un clúster de HCP mediante AWS STS la ROSA CLI.
- the section called “Crea un clúster clásico de ROSA - AWS PrivateLink ”- Cree su primer clúster ROSA clásico con AWS PrivateLink.
- the section called “Cree un clúster clásico de ROSA - CLI”- Cree su primer clúster clásico de ROSA con AWS STS la ROSA CLI.

Configurar para usar ROSA

Para preparar el entorno para la creación de un ROSA clúster, debe realizar las siguientes acciones.

Requisitos previos

Se deben cumplir los siguientes requisitos previos para permitir la creación de ROSA clústeres.

- Instale y configure la versión más reciente AWS CLI. Para obtener más información, consulte Instalación o actualización de la versión de AWS CLI más reciente.
- Instale y configure la CLI y la ROSA CLI de OpenShift Container Platform más recientes. Para obtener más información, consulte Introducción a la ROSA CLI.
- Debe tener establecidas las cuotas de servicio requeridas para Amazon EC2 Amazon VPC, Amazon EBS, y Elastic Load Balancing. AWS o Red Hat puede solicitar en su nombre el aumento de la cuota de servicio según sea necesario para resolver el problema. Para ver las cuotas de servicio requeridas ROSA, consulte los Red Hat OpenShift Service en AWS puntos finales y las cuotas en la Referencia AWS general.
- Para recibir AWS soporte ROSA, debe habilitar los planes de soporte AWS Business, Enterprise On-Ramp o Enterprise. Red Hat puede solicitar AWS asistencia en su nombre según sea

necesario para la resolución de problemas. Para obtener más información, consulte the section called “Cómo obtener asistencia”. Para habilitarlo Soporte, consulte la Soporte página.

- Si utiliza AWS Organizations para administrar el servidor Cuentas de AWS que aloja el ROSA servicio, la política de control de servicios (SCP) de la organización debe configurarse para permitir que Red Hat lleve a cabo las acciones políticas que figuran en la SCP sin restricciones. Para obtener más información, consulte la the section called “AWS Organizations la política de control de servicios deniega AWS Marketplace los permisos necesarios”. Para obtener más información SCPs, consulte las políticas de control de servicios () SCPs.
- Si implementas un ROSA clúster with AWS STS en uno habilitado Región de AWS que está deshabilitado de forma predeterminada, debes actualizar el token de seguridad a la versión 2 para todas las regiones del Cuenta de AWS mismo con el siguiente comando.

```
aws iam set-security-token-service-preferences --global-endpoint-token-version
 v2Token
```

Para obtener más información sobre cómo habilitar las regiones, consulta el enlace: accounts/latest/reference/manage

Habilite ROSA y configure los AWS requisitos previos

Para crear una ROSA clúster, debe habilitar el ROSA servicio en la AWS ROSA consola. La AWS ROSA consola comprueba si Cuenta de AWS tiene los AWS Marketplace permisos necesarios, las cuotas de servicio y la función vinculada al servicio Elastic Load Balancing (ELB) nombrada. `AWSServiceRoleForElasticLoadBalancing` Si falta alguno de estos requisitos previos, la consola proporcionará instrucciones sobre cómo configurar la cuenta para que cumpla con los requisitos previos.

1. Diríjase a la consola de ROSA.
2. Seleccionar Comenzar.
3. En la página Verificar los ROSA requisitos previos, seleccione Acepto compartir mi información de contacto con Red Hat.
4. Seleccione Habilitar ROSA .
5. Una vez que la página haya verificado que sus cuotas de servicio cumplen ROSA los requisitos previos y se haya creado el rol vinculado al servicio del ELB, abra una nueva sesión de terminal para crear la primera mediante ROSA clúster la CLI. ROSA

Cree un clúster ROSA con HCP mediante la ROSA CLI

En las siguientes secciones se describe cómo empezar a utilizar ROSA con planos de control alojados (ROSA con HCP) mediante AWS STS la ROSA CLI. Para conocer los pasos para crear un ROSA con un clúster de HCP mediante Terraform, consulte la documentación de Red Hat. Para obtener más información sobre el proveedor de Terraform para crear ROSA clústeres, consulte la documentación de Terraform.

La ROSA CLI utiliza el `auto` modo o el `manual` modo para crear los IAM recursos y la configuración de OpenID Connect (OIDC) necesarios para crear un. ROSA clúster`auto`el modo crea automáticamente las IAM funciones y políticas requeridas y el proveedor de OIDC. `manual`El modo genera los AWS CLI comandos necesarios para crear los IAM recursos manualmente. Al usar `manual` el modo, puede revisar los AWS CLI comandos generados antes de ejecutarlos manualmente. Con el modo `manual`, también puede pasar los comandos a otro administrador o grupo de su organización para que pueda crear los recursos.

Los procedimientos de este documento utilizan el `auto` modo de la ROSA CLI para crear los IAM recursos necesarios y la configuración OIDC para ROSA con HCP. Para ver más opciones para empezar, consulte. Comience con ROSA

Temas

- Eliminar un clúster y sus AWS STS recursos

Requisitos previos

Complete las acciones previas que se enumeran enthe section called “Configuración”.

Cree una Amazon VPC arquitectura

El siguiente procedimiento crea una Amazon VPC arquitectura que se puede utilizar para alojar un clúster. Todos clúster los recursos están alojados en la subred privada. La subred pública enruta el tráfico saliente de la subred privada a través de una puerta de enlace NAT a la Internet pública. En este ejemplo, se utiliza `10.0.0.0/16` con bloque de CIDR para la Amazon VPC. Sin embargo, puede elegir otro bloque de CIDR. Para obtener más información, consulte Tamaño de la VPC.

> **Important**
>
> Si no se Amazon VPC cumplen los requisitos, se produce un error en la creación del clúster.

Example

Terraform

1. Instale la CLI de Terraform. Para obtener más información, consulte las instrucciones de instalación en la documentación de Terraform.
2. Abra una sesión de terminal y clone el repositorio de VPC de Terraform.

   ```
   git clone https://github.com/openshift-cs/terraform-vpc-example
   ```

3. Navegue hasta el directorio creado.

   ```
   cd terraform-vpc-example
   ```

4. Inicie el archivo Terraform.

   ```
   terraform init
   ```

   Una vez completado, la CLI devuelve un mensaje que indica que Terraform se ha inicializado correctamente.

5. Para crear un plan de Terraform basado en la plantilla existente, ejecute el siguiente comando. Región de AWS Debe especificarse el. Si lo desea, puede especificar un nombre de clúster.

```
terraform plan -out rosa.tfplan -var region=<region>
```

   Una vez ejecutado el comando, se añade un `rosa.tfplan` archivo al `hypershift-tf` directorio. Para ver opciones más detalladas, consulta el archivo README del repositorio de VPC de Terraform.

6. Aplique el archivo del plan para crear la VPC.

```
terraform apply rosa.tfplan
```

   Una vez completado, la CLI devolvió un mensaje de éxito que verifica los recursos agregados.

   a. (Opcional) Cree variables de entorno para la subred privada, pública y de grupo de máquinas aprovisionada por Terraform IDs para utilizarlas al crear su clúster ROSA con HCP.

```
export SUBNET_IDS=$(terraform output -raw cluster-subnets-string)
```

   b. (Opcional) Compruebe que las variables de entorno se hayan establecido correctamente.

```
echo $SUBNET_IDS
```

Amazon VPC console

1. Abra la consola de Amazon VPC.
2. En el panel de VPC, elija Create VPC (Crear VPC).
3. En Recursos para crear, elija VPC y más.
4. Mantenga seleccionada la opción Generación automática de etiquetas de nombre para crear etiquetas de nombre para los recursos de la VPC, o desactívela para proporcionar sus propias etiquetas de nombre para los recursos de la VPC.
5. Para el bloque IPv4 CIDR, introduzca un rango de IPv4 direcciones para la VPC. Una VPC debe tener un rango de IPv4 direcciones.
6. (Opcional) Para admitir IPv6 el tráfico, elige el bloque IPv6 CIDR, el bloque CIDR proporcionado por Amazon IPv6 .

7. Deje Tenancy como. `Default`
8. En Número de zonas de disponibilidad (AZs), elija el número que necesite. Para las implementaciones en zonas de disponibilidad múltiples (Multi-AZ), ROSA requiere tres zonas de disponibilidad. Para elegir una AZs para sus subredes, expanda Personalizar. AZs

> **Note**
>
> Algunos tipos de ROSA instancias solo están disponibles en determinadas zonas de disponibilidad. Puede usar el `rosa list instance-types` comando ROSA CLI para enumerar todos los tipos de ROSA instancias disponibles. Para comprobar si un tipo de instancia está disponible para una zona de disponibilidad determinada, usa el AWS CLI comando`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

9. Para configurar las subredes, elija valores para Cantidad de subredes públicas y Cantidad de subredes privadas. Para elegir los rangos de direcciones IP para las subredes, expanda Personalizar bloques CIDR de subredes.

> **Note**
>
> ROSA con HCP requiere que los clientes configuren al menos una subred pública y privada por cada zona de disponibilidad utilizada para crear clústeres.

10. Para conceder a los recursos de la subred privada acceso a Internet pública a través de las puertas de enlace NAT IPv4, elija el número de puertas de enlace NAT AZs en las que desee crear las puertas de enlace NAT. En producción, se recomienda implementar una puerta de enlace de NAT en cada AZ con recursos que necesiten acceso a la Internet pública.
11. (Opcional) Si necesita acceder Amazon S3 directamente desde su VPC, elija los puntos de enlace de la VPC, S3 Gateway.
12. Deje seleccionadas las opciones de DNS predeterminadas. ROSA requiere compatibilidad con nombres de host DNS en la VPC.
13. Expanda Etiquetas adicionales, elija Agregar nueva etiqueta y agregue las siguientes claves de etiqueta. ROSA utiliza comprobaciones previas automatizadas que verifican que se utilizan estas etiquetas.

- Clave: `kubernetes.io/role/elb`
- Clave: `kubernetes.io/role/internal-elb`

14. Seleccione Creación de VPC.

AWS CLI

1. Cree una VPC con un bloque de CIDR `10.0.0.0/16`.

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

El comando anterior devuelve el ID de VPC. El siguiente es un ejemplo de salida.

```
vpc-1234567890abcdef0
```

2. Guarde el ID de VPC en una variable de entorno.

```
export VPC_ID=vpc-1234567890abcdef0
```

3. Cree una `Name` etiqueta para la VPC mediante la variable de `VPC_ID` entorno.

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. Habilite la compatibilidad con nombres de host DNS en la VPC.

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. Cree una subred pública y privada en la VPC, especificando las zonas de disponibilidad en las que se deben crear los recursos.

> **Important**
>
> ROSA con HCP requiere que los clientes configuren al menos una subred pública y privada por cada zona de disponibilidad utilizada para crear clústeres. Para las implementaciones en zonas de disponibilidad múltiples (Multi-AZ), se requieren tres

zonas de disponibilidad. Si no se cumplen estos requisitos, se producirá un error en la creación del clúster.

> **Note**
>
> Algunos tipos de ROSA instancias solo están disponibles en determinadas zonas de disponibilidad. Puede usar el `rosa list instance-types` comando ROSA CLI para enumerar todos los tipos de ROSA instancias disponibles. Para comprobar si un tipo de instancia está disponible para una zona de disponibilidad determinada, usa el AWS CLI comando`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. Guarde la subred pública y privada IDs en variables de entorno.

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. Cree las siguientes etiquetas para las subredes de VPC. ROSA utiliza comprobaciones previas automatizadas que verifican el uso de estas etiquetas.

> **Note**
>
> Debe etiquetar al menos una subred privada y, si corresponde, una subred pública.

```
aws ec2 create-tags --resources $PUBLIC_SUB --tags Key=kubernetes.io/role/
elb,Value=1
aws ec2 create-tags --resources $PRIVATE_SUB --tags Key=kubernetes.io/role/
internal-elb,Value=1
```

8. Cree una puerta de enlace a Internet y una tabla de enrutamiento para el tráfico saliente. Cree una tabla de enrutamiento y una dirección IP elástica para el tráfico privado.

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

9. Almacene IDs las variables de entorno.

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

10. Adjunte la puerta de enlace de Internet a la VPC.

```
aws ec2 attach-internet-gateway \
    --vpc-id $VPC_ID \
```

```
    --internet-gateway-id $IGW
```

11. Asocie la tabla de rutas públicas a la subred pública y configure el tráfico para que se dirija a la puerta de enlace de Internet.

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

12. Cree la puerta de enlace NAT y asóciela a la dirección IP elástica para permitir el tráfico a la subred privada.

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

13. Asocie la tabla de rutas privadas a la subred privada y configure el tráfico para que se dirija a la puerta de enlace NAT.

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

14. (Opcional) Para las implementaciones Multi-AZ, repita los pasos anteriores para configurar otras dos zonas de disponibilidad con subredes públicas y privadas.

Cree los IAM roles necesarios y la configuración de OpenID Connect

Antes de crear un clúster ROSA con HCP, debe crear las IAM funciones y políticas necesarias y la configuración de OpenID Connect (OIDC). Para obtener más información sobre las IAM funciones y políticas de ROSA con HCP, consulte. the section called “ AWS políticas gestionadas”

Este procedimiento utiliza el `auto` modo de la ROSA CLI para crear automáticamente la configuración OIDC necesaria para crear un ROSA con un clúster de HCP.

1. Cree las políticas y funciones de IAM cuenta necesarias. El `--force-policy-creation` parámetro actualiza todos los roles y políticas existentes que estén presentes. Si no hay roles ni políticas, el comando crea estos recursos en su lugar.

   ```
   rosa create account-roles --force-policy-creation
   ```

   > **Note**
   >
   > Si el token de acceso sin conexión ha caducado, la ROSA CLI muestra un mensaje de error que indica que el token de autorización debe actualizarse. Para ver los pasos para solucionar problemas, consultethe section called “Solucionar problemas con los tokens de acceso sin conexión caducados por ROSA CLI”.

2. Cree la configuración de OpenID Connect (OIDC) que permita la autenticación de los usuarios en el clúster. Esta configuración está registrada para usarse con OpenShift Cluster Manager (OCM).

   ```
   rosa create oidc-config --mode=auto
   ```

3. Copie el ID de configuración del OIDC que se proporciona en la salida de la ROSA CLI. El ID de configuración de OIDC debe proporcionarse más adelante para crear el clúster de ROSA con HCP.
4. Para verificar las configuraciones OIDC disponibles para los clústeres asociados a su organización de usuarios, ejecute el siguiente comando.

   ```
   rosa list oidc-config
   ```

5. Cree los roles de IAM operador necesarios y sustitúyalos por `<OIDC_CONFIG_ID>` el ID de configuración del OIDC copiado anteriormente.

   Example

   > **Important**
   >
   > Debe proporcionar un prefijo en `<PREFIX_NAME>` al crear los roles de operador. Si no se realiza esta acción, se producirá un error.

```
rosa create operator-roles --prefix <PREFIX_NAME> --oidc-config-id <OIDC_CONFIG_ID>
 --hosted-cp
```

6. Para comprobar que se crearon las funciones de IAM operador, ejecute el siguiente comando:

```
rosa list operator-roles
```

Cree un clúster ROSA con HCP mediante la ROSA CLI y AWS STS

Puede crear una ROSA con HCP clúster mediante AWS Security Token Service (AWS STS) y el `auto` modo que se proporciona en la ROSA CLI. Tiene la opción de crear un clúster con una API pública e Ingress o una API privada e Ingress.

Puede crear una clúster con una única zona de disponibilidad (Single-AZ) o múltiples zonas de disponibilidad (Multi-AZ). En cualquier caso, el valor de CIDR de su máquina debe coincidir con el valor de CIDR de su VPC.

El siguiente procedimiento utiliza el `rosa create cluster --hosted-cp` comando para crear una ROSA en una única zona de disponibilidad con HCP. clúster Para crear una zona de disponibilidad múltiple clúster, especifique `multi-az` en el comando y la subred privada de cada subred IDs privada en la que desee realizar el despliegue.

1. Cree un clúster de ROSA con HCP con uno de los siguientes comandos.
   - Cree un clúster ROSA con HCP con una API pública e Ingress, especificando el nombre del clúster, el prefijo del rol del operador, el ID de configuración del OIDC y la subred pública y privada. IDs

     ```
     rosa create cluster --cluster-name=<CLUSTER_NAME> --sts --mode=auto --hosted-cp --
     operator-roles-prefix <OPERATOR_ROLE_PREFIX> --oidc-config-id <OIDC_CONFIG_ID> --
     subnet-ids=<PUBLIC_SUBNET_ID>,<PRIVATE_SUBNET_ID>
     ```

   - Cree un clúster ROSA con HCP con una API privada e Ingress, especificando el nombre del clúster, el prefijo del rol de operador, el ID de configuración del OIDC y la subred privada. IDs

     ```
     rosa create cluster --private --cluster-name=<CLUSTER_NAME> --sts --mode=auto --
     hosted-cp --subnet-ids=<PRIVATE_SUBNET_ID>
     ```

2. Comprueba el estado de tu. clúster

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> Si el proceso de creación falla o el `State` campo no cambia a un estado listo después de 10 minutos, consulte Resolución de problemas.
> Para ponerse en contacto con Soporte el servicio de asistencia de Red Hat, consulte the section called “Cómo obtener asistencia”.

3. Realice un seguimiento del progreso de la clúster creación observando los registros del OpenShift instalador.

```
rosa logs install -c <CLUSTER_NAME> --watch
```

Configure un proveedor de identidades y conceda el clúster acceso

ROSA incluye un OAuth servidor integrado. Una vez creado clúster el suyo, debe configurarlo OAuth para usar un proveedor de identidades. A continuación, puede añadir usuarios a su proveedor de identidad configurado para concederles acceso a su clúster. Puede otorgarles permisos de `cluster-admin` o `dedicated-admin` a estos usuarios según sea necesario.

Puede configurar diferentes tipos de proveedores de identidad para su clúster de ROSA . Los tipos compatibles incluyen GitHub Enterprise GitHub, Google GitLab, LDAP, OpenID Connect y proveedores de identidad. HTPasswd

> **Important**
>
> El proveedor de HTPasswd identidad se incluye solo para permitir la creación de un único usuario administrador estático. HTPasswd no se admite como proveedor de identidades de uso general para. ROSA

El siguiente procedimiento configura un proveedor de GitHub identidades como ejemplo. Para obtener instrucciones sobre cómo configurar cada uno de los tipos de proveedores de identidad compatibles, consulte Configuración de proveedores de identidad para AWS STS.

1. Ve a github.com e inicia sesión en tu cuenta. GitHub
2. Si no tienes una GitHub organización que puedas usar para el aprovisionamiento de identidades, crea una. clúster Para obtener más información, consulta los pasos de la GitHub documentación.
3. Con el modo interactivo de la ROSA CLI, configure un proveedor de identidades para el clúster.

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. Siga las instrucciones de configuración del resultado para restringir el clúster acceso a los miembros de su GitHub organización.

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. Abre la URL en el resultado y <GITHUB_ORG_NAME> sustitúyela por el nombre de tu GitHub organización.
6. En la página GitHub web, elija Registrar aplicación para registrar una nueva OAuth aplicación en su GitHub organización.
7. Utilice la información de la GitHub OAuth página para rellenar el resto de las solicitudes `rosa create idp` interactivas ejecutando el siguiente comando. Sustituya <GITHUB_CLIENT_ID> y por <GITHUB_CLIENT_SECRET> las credenciales de su aplicación. GitHub OAuth

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
```

```
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> La configuración del proveedor de identidad puede tardar aproximadamente dos minutos en activarse. Si configuraste un `cluster-admin` usuario, puedes correr `oc get pods -n openshift-authentication --watch` para ver cómo se vuelven a implementar los OAuth pods con la configuración actualizada.

8. Compruebe que el proveedor de identidad esté configurado correctamente.

```
rosa list idps --cluster=<CLUSTER_NAME>
```

Conceda al usuario acceso a un clúster

Puede conceder acceso a un usuario al suyo clúster agregándolo al proveedor de identidades configurado.

El siguiente procedimiento agrega un usuario a una GitHub organización que está configurada para el aprovisionamiento de identidades en el clúster.

1. Ve a github.com e inicia sesión en tu cuenta. GitHub
2. Invita a los usuarios que necesiten clúster acceder a tu organización. GitHub Para obtener más información, consulte Invitar a los usuarios a unirse a su organización en la GitHub documentación.

Configuración de permisos de **`cluster-admin`**

1. Otorgue los permisos de `cluster-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su nombre de usuario y clúster.

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario aparezca como miembro del grupo de `cluster-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Configuración de permisos de **`dedicated-admin`**

1. Otorgue los permisos de `dedicated-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su clúster nombre de usuario mediante la ejecución del siguiente comando.

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario aparezca como miembro del grupo de `cluster-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Acceda a a clúster a través de la consola Red Hat Hybrid Cloud

Inicie sesión en su consola a clúster través de Red Hat Hybrid Cloud Console.

1. Obtenga la URL de su consola clúster mediante el siguiente comando. `<CLUSTER_NAME>`Reemplácela por el nombre de su clúster.

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. Navegue hasta la URL de la consola en la salida e inicie sesión.

   En el cuadro de diálogo Iniciar sesión con..., seleccione el nombre del proveedor de identidad y complete las solicitudes de autorización de su proveedor.

Implemente una aplicación del catálogo para desarrolladores

Desde la consola de la nube híbrida de Red Hat, puede implementar una aplicación de prueba del catálogo de desarrolladores y exponerla con una ruta.

1. Diríjase a la Consola de la nube híbrida de Red Hat y seleccione el clúster en el que desea implementar la aplicación.
2. En la página del clúster, seleccione Abrir consola.
3. Desde la perspectiva Administrador, seleccione Inicio > Proyectos > Crear proyecto.
4. Introduzca un nombre para el proyecto y, si lo desea, añada un Nombre de visualización y una Descripción.
5. Seleccione Crear para crear el proyecto.
6. Cambie a la perspectiva Desarrollador y seleccione +Añadir. Asegúrese de que el proyecto seleccionado sea el que se acaba de crear.
7. En el cuadro de diálogo del Catálogo de desarrolladores, seleccione Todos los servicios.
8. En la página del catálogo para desarrolladores, seleccione Idiomas > en el JavaScriptmenú.
9. Elija Node.js y, a continuación, elija Crear aplicación para abrir la página Crear Source-to-Image aplicación.

> **Note**
>
> Puede que tenga que seleccionar Eliminar todos los filtros para que aparezca la opción Node.js.

10. En la sección Git, seleccione Probar ejemplo.
11. En el campo Nombre, agregue un nombre único.
12. Seleccione Crear.

> **Note**
>
> La nueva aplicación tarda varios minutos en implementarse.

13. Una vez finalizada la implementación, elija la URL de la ruta para la aplicación.

    Se abre una nueva pestaña en el navegador con un mensaje similar al siguiente.

```
Welcome to your Node.js application on OpenShift
```

14. (Opcional) Elimine la aplicación y limpie los recursos:
    a. Desde la perspectiva de Administrador, seleccione Inicio > Proyectos.
    b. Abra el menú de acciones del proyecto y seleccione Eliminar proyecto.

Revoque los permisos de **`cluster-admin`** de un usuario

1. Otorgue los permisos de `cluster-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su clúster nombre de usuario.

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario no figure como miembro del grupo de `cluster-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revoque los permisos de **`dedicated-admin`** de un usuario

1. Revoque los permisos de `dedicated-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su clúster nombre de usuario.

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario no figure como miembro del grupo `dedicated-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revocar el acceso del usuario a un clúster

Puede revocar el clúster acceso de un usuario del proveedor de identidades quitándolo del proveedor de identidades configurado.

Puede configurar diferentes tipos de proveedores de identidad para su clúster. El siguiente procedimiento revoca el clúster acceso de un miembro de una GitHub organización.

1. Ve a github.com e inicia sesión en tu cuenta. GitHub
2. Elimina al usuario de tu organización. GitHub Para obtener más información, consulte Eliminar a un miembro de su organización en la GitHub documentación.

Eliminar un clúster y sus AWS STS recursos

Puede usar la ROSA CLI para eliminar una clúster que use AWS Security Token Service (AWS STS). También puede usar la ROSA CLI para eliminar las IAM funciones y el proveedor de OIDC creados por. ROSA Para eliminar las IAM políticas creadas por ROSA, puede utilizar la IAM consola.

> **Note**
>
> IAM las funciones y políticas creadas por ROSA pueden ser utilizadas por otros ROSA clústeres de la misma cuenta.

1. Elimine los registros clúster y observe los mismos. Sustituya `<CLUSTER_NAME>` por el nombre o ID del clúster.

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> Debe esperar clúster a que se eliminen por completo antes de eliminar las IAM funciones, las políticas y el proveedor de OIDC. Los roles de IAM de la cuenta son necesarios para eliminar los recursos creados por el instalador. Las funciones de IAM de los operadores son necesarias para limpiar los recursos creados por los operadores. OpenShift Los operadores utilizan el proveedor de OIDC para autenticar.

2. Elimine el proveedor de OIDC que utilizan los clúster operadores para autenticarse ejecutando el siguiente comando.

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. Elimine las funciones de operador específicas del clúster. IAM

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. Elimine los roles de IAM de la cuenta mediante el siguiente comando. Sustituya `<PREFIX>` por el prefijo de los roles de IAM de la cuenta que desea eliminar. Si especificó un prefijo personalizado al crear los roles de IAM de la cuenta, especifique el prefijo predeterminado de `ManagedOpenShift`.

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. Elimine las IAM políticas creadas por. ROSA
   a. Inicie sesión en la consola de IAM.
   b. En el menú Administración de acceso de la izquierda, seleccione Políticas.
   c. Seleccione la política que desea eliminar y elija Acciones > Eliminar.
   d. Introduzca el nombre de la política y seleccione Eliminar.
   e. Repita este paso para eliminar cada una de las políticas de IAM para el clúster.

Cree un clúster clásico de ROSA mediante la ROSA CLI

En las siguientes secciones se describe cómo empezar a utilizar ROSA classic AWS STS y la ROSA CLI. Para conocer los pasos para crear un clúster ROSA clásico con Terraform, consulte la documentación de Red Hat. Para obtener más información sobre el proveedor de Terraform para crear ROSA clústeres, consulte la documentación de Terraform.

La ROSA CLI usa el `auto` modo o `manual` el modo para crear los IAM recursos necesarios para aprovisionar un ROSA clúster. `auto`El modo crea inmediatamente las IAM funciones y políticas necesarias y un proveedor de OpenID Connect (OIDC). `manual`el modo genera los AWS CLI comandos necesarios para crear los recursos. IAM Al usar `manual` el modo, puede revisar los AWS CLI comandos generados antes de ejecutarlos manualmente. Con el modo `manual`, también puede pasar los comandos a otro administrador o grupo de su organización para que pueda crear los recursos.

Para ver más opciones para empezar, consulteComience con ROSA .

Temas

- Requisitos previos
- Cree un clúster clásico de ROSA mediante la ROSA CLI y AWS STS
- Configure un proveedor de identidades y conceda el clúster acceso
- Conceda al usuario acceso a un clúster
- Configuración de permisos de cluster-admin
- Configuración de permisos de dedicated-admin
- Acceda a a clúster a través de la consola Red Hat Hybrid Cloud

- Implemente una aplicación del catálogo para desarrolladores
- Revoque los permisos de cluster-admin de un usuario
- Revoque los permisos de dedicated-admin de un usuario
- Revocar el acceso del usuario a un clúster
- Eliminar un clúster y sus AWS STS recursos

Requisitos previos

Complete las acciones previas que se enumeran enthe section called “Configuración”.

Cree un clúster clásico de ROSA mediante la ROSA CLI y AWS STS

Puede crear un clásico de ROSA clúster mediante la ROSA CLI y AWS STS.

1. Cree las funciones y políticas de IAM cuenta requeridas utilizando `--mode auto` o`--mode manual`.
   -
     ```
     rosa create account-roles --classic --mode auto
     ```
   -
     ```
     rosa create account-roles --classic --mode manual
     ```

     > **Note**
     >
     > Si el token de acceso sin conexión ha caducado, la ROSA CLI muestra un mensaje de error que indica que el token de autorización debe actualizarse. Para ver los pasos para solucionar problemas, consultethe section called “Solucionar problemas con los tokens de acceso sin conexión caducados por ROSA CLI”.
2. Cree un clúster utilizando `--mode auto` o. `--mode manual` `auto`el modo le permite crear un clúster más rápidamente. `manual`el modo le pide que especifique una configuración personalizada para su clúster.
   -
     ```
     rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode auto
     ```

> **Note**
>
> Cuando lo especificas `--mode auto`, el `rosa create cluster` comando crea automáticamente las IAM funciones de operador específicas del clúster y el proveedor de OIDC. Los operadores utilizan el proveedor de OIDC para autenticar.

> **Note**
>
> Si se utilizan los `--mode auto` valores predeterminados, se instala la última versión estable. OpenShift

- ```
  rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode manual
  ```

> **Important**
>
> Si habilita el cifrado etcd en el `manual` modo, incurrirá en una sobrecarga de rendimiento de aproximadamente un 20%. La sobrecarga se debe a la introducción de esta segunda capa de cifrado, además del cifrado predeterminado de Amazon EBS, que cifra los volúmenes etcd.

> **Note**
>
> Después de ejecutar el `manual` modo para crear el clúster, debe crear manualmente las funciones de IAM de los operadores específicos del clúster y el proveedor de OpenID Connect que los operadores del clúster utilizan para autenticarse.

3. Compruebe el estado de su. clúster

```
rosa describe cluster -c <CLUSTER_NAME>
```
```

> **Note**
>
> Si el proceso de aprovisionamiento falla o el `State` campo no cambia a un estado listo después de 40 minutos, consulteResolución de problemas. Para ponerse en contacto con Soporte el soporte de Red Hat para obtener asistencia, consultethe section called “Cómo obtener asistencia”.

4. Realice un seguimiento del progreso de la clúster creación observando los registros del OpenShift instalador.

```
rosa logs install -c <CLUSTER_NAME> --watch
```

Configure un proveedor de identidades y conceda el clúster acceso

ROSA incluye un OAuth servidor integrado. Una vez creado clúster el suyo, debe configurarlo OAuth para usar un proveedor de identidades. A continuación, puede añadir usuarios a su proveedor de identidad configurado para concederles acceso a su clúster. Puede otorgarles permisos de `cluster-admin` o `dedicated-admin` a estos usuarios según sea necesario.

Puede configurar diferentes tipos de proveedores de identidad para su clúster de ROSA . Los tipos compatibles incluyen GitHub Enterprise GitHub, Google GitLab, LDAP, OpenID Connect y proveedores de identidad. HTPasswd

> **Important**
>
> El proveedor de HTPasswd identidad se incluye solo para permitir la creación de un único usuario administrador estático. HTPasswd no se admite como proveedor de identidades de uso general para. ROSA

El siguiente procedimiento configura un proveedor de GitHub identidades como ejemplo. Para obtener instrucciones sobre cómo configurar cada uno de los tipos de proveedores de identidad compatibles, consulte Configuración de proveedores de identidad para AWS STS.

1. Ve a github.com e inicia sesión en tu cuenta. GitHub
2. Si no tienes una GitHub organización que puedas usar para el aprovisionamiento de identidades, crea una. clúster Para obtener más información, consulta los pasos de la GitHub documentación.

3. Con el modo interactivo de la ROSA CLI, configure un proveedor de identidades para el clúster.

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. Siga las instrucciones de configuración del resultado para restringir el clúster acceso a los miembros de su GitHub organización.

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. Abre la URL en el resultado y <GITHUB_ORG_NAME> sustitúyela por el nombre de tu GitHub organización.
6. En la página GitHub web, elija Registrar aplicación para registrar una nueva OAuth aplicación en su GitHub organización.
7. Utilice la información de la GitHub OAuth página para rellenar el resto de las solicitudes `rosa create idp` interactivas ejecutando el siguiente comando. Sustituya <GITHUB_CLIENT_ID> y por <GITHUB_CLIENT_SECRET> las credenciales de su aplicación. GitHub OAuth

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
```

```
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> La configuración del proveedor de identidad puede tardar aproximadamente dos minutos en activarse. Si configuraste un `cluster-admin` usuario, puedes correr `oc get pods -n openshift-authentication --watch` para ver cómo se vuelven a implementar los OAuth pods con la configuración actualizada.

8. Compruebe que el proveedor de identidad esté configurado correctamente.

```
rosa list idps --cluster=<CLUSTER_NAME>
```

Conceda al usuario acceso a un clúster

Puede conceder acceso a un usuario al suyo clúster agregándolo al proveedor de identidades configurado.

El siguiente procedimiento agrega un usuario a una GitHub organización que está configurada para el aprovisionamiento de identidades en el clúster.

1. Ve a github.com e inicia sesión en tu cuenta. GitHub
2. Invita a los usuarios que necesiten clúster acceder a tu organización. GitHub Para obtener más información, consulte Invitar a los usuarios a unirse a su organización en la GitHub documentación.

Configuración de permisos de **`cluster-admin`**

1. Otorgue los permisos de `cluster-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su nombre de usuario y clúster.

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario aparezca como miembro del grupo de `cluster-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Configuración de permisos de **`dedicated-admin`**

1. Otorgue los permisos de `dedicated-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su clúster nombre de usuario mediante la ejecución del siguiente comando.

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario aparezca como miembro del grupo de `cluster-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Acceda a a clúster a través de la consola Red Hat Hybrid Cloud

Tras crear un usuario clúster administrador o añadir un usuario a su proveedor de identidad configurado, puede iniciar sesión en él a clúster través de la consola de Red Hat Hybrid Cloud.

1. Obtenga la URL de la consola para clúster usted mediante el siguiente comando. `<CLUSTER_NAME>`Sustitúyala por el nombre de tu clúster.

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. Navegue hasta la URL de la consola en la salida e inicie sesión.
   - Si ha creado un usuario de `cluster-admin`, inicie sesión con las credenciales proporcionadas.
   - Si configuró un proveedor de identidad para usted clúster, elija el nombre del proveedor de identidad en el cuadro de diálogo Iniciar sesión con... y complete las solicitudes de autorización que presente su proveedor.

Implemente una aplicación del catálogo para desarrolladores

Desde la consola de la nube híbrida de Red Hat, puede implementar una aplicación de prueba del catálogo de desarrolladores y exponerla con una ruta.

1. Diríjase a la Consola de la nube híbrida de Red Hat y seleccione el clúster en el que desea implementar la aplicación.
2. En la página del clúster, seleccione Abrir consola.
3. Desde la perspectiva Administrador, seleccione Inicio > Proyectos > Crear proyecto.
4. Introduzca un nombre para el proyecto y, si lo desea, añada un Nombre de visualización y una Descripción.
5. Seleccione Crear para crear el proyecto.
6. Cambie a la perspectiva Desarrollador y seleccione +Añadir. Asegúrese de que el proyecto seleccionado sea el que se acaba de crear.
7. En el cuadro de diálogo del Catálogo de desarrolladores, seleccione Todos los servicios.
8. En la página del catálogo para desarrolladores, seleccione Idiomas > en el JavaScriptmenú.
9. Elija Node.js y, a continuación, elija Crear aplicación para abrir la página Crear Source-to-Image aplicación.

> **Note**
>
> Puede que tenga que seleccionar Eliminar todos los filtros para que aparezca la opción Node.js.

10. En la sección Git, seleccione Probar ejemplo.
11. En el campo Nombre, agregue un nombre único.
12. Seleccione Crear.

> **Note**
>
> La nueva aplicación tarda varios minutos en implementarse.

13. Una vez finalizada la implementación, elija la URL de la ruta para la aplicación.

    Se abre una nueva pestaña en el navegador con un mensaje similar al siguiente.

```
Welcome to your Node.js application on OpenShift
```

14. (Opcional) Elimine la aplicación y limpie los recursos:
    a. Desde la perspectiva de Administrador, seleccione Inicio > Proyectos.
    b. Abra el menú de acciones del proyecto y seleccione Eliminar proyecto.

Revoque los permisos de **`cluster-admin`** de un usuario

1. Otorgue los permisos de `cluster-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su clúster nombre de usuario.

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario no figure como miembro del grupo de `cluster-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revoque los permisos de **`dedicated-admin`** de un usuario

1. Revoque los permisos de `dedicated-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su clúster nombre de usuario.

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario no figure como miembro del grupo `dedicated-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revocar el acceso del usuario a un clúster

Puede revocar el clúster acceso de un usuario del proveedor de identidades quitándolo del proveedor de identidades configurado.

Puede configurar diferentes tipos de proveedores de identidad para su clúster. El siguiente procedimiento revoca el clúster acceso de un miembro de una GitHub organización.

1. Ve a github.com e inicia sesión en tu cuenta. GitHub
2. Elimina al usuario de tu organización. GitHub Para obtener más información, consulte Eliminar a un miembro de su organización en la GitHub documentación.

Eliminar un clúster y sus AWS STS recursos

Puede usar la ROSA CLI para eliminar una clúster que use AWS Security Token Service (AWS STS). También puede usar la ROSA CLI para eliminar las IAM funciones y el proveedor de OIDC creados por. ROSA Para eliminar las IAM políticas creadas por ROSA, puede utilizar la IAM consola.

> **Important**
>
> IAM las funciones y políticas creadas por ROSA pueden ser utilizadas por otros ROSA clústeres de la misma cuenta.

1. Elimine los registros clúster y observe los mismos. Sustituya `<CLUSTER_NAME>` por el nombre o ID del clúster.

   ```
   rosa delete cluster --cluster=<CLUSTER_NAME> --watch
   ```

   > **Important**
   >
   > Debe esperar clúster a que se eliminen por completo antes de eliminar las IAM funciones, las políticas y el proveedor de OIDC. Los roles de IAM de la cuenta son necesarios para eliminar los recursos creados por el instalador. Las funciones de IAM de los operadores son necesarias para limpiar los recursos creados por los operadores. OpenShift Los operadores utilizan el proveedor de OIDC para autenticar.

2. Elimine el proveedor de OIDC que utilizan los clúster operadores para autenticarse ejecutando el siguiente comando.

   ```
   rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
   ```

3. Elimine las funciones de operador específicas del clúster. IAM

   ```
   rosa delete operator-roles -c <CLUSTER_ID> --mode auto
   ```

4. Elimine los roles de IAM de la cuenta mediante el siguiente comando. Sustituya `<PREFIX>` por el prefijo de los roles de IAM de la cuenta que desea eliminar. Si especificó un prefijo personalizado al crear los roles de IAM de la cuenta, especifique el prefijo predeterminado de `ManagedOpenShift`.

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. Elimine las IAM políticas creadas por. ROSA
   a. Inicie sesión en la consola de IAM.
   b. En el menú Administración de acceso de la izquierda, seleccione Políticas.
   c. Seleccione la política que desea eliminar y elija Acciones > Eliminar.
   d. Introduzca el nombre de la política y seleccione Eliminar.
   e. Repita este paso para eliminar cada una de las políticas de IAM para el clúster.

Cree un clúster clásico de ROSA que utilice AWS PrivateLink

Los clústeres ROSA classic se pueden implementar de diferentes maneras: públicos, privados o privados con. AWS PrivateLink Para obtener más información sobre ROSA classic, consultethe section called “Arquitectura”. Tanto para clúster las configuraciones públicas como privadas, OpenShift clúster tiene acceso a Internet y la privacidad se establece en las cargas de trabajo de la aplicación en la capa de aplicación.

Si necesita que tanto las cargas clúster de trabajo como las de la aplicación sean privadas, puede configurarlas AWS PrivateLink con ROSA classic. AWS PrivateLink es una tecnología escalable y de alta disponibilidad que se ROSA utiliza para crear una conexión privada entre el ROSA servicio y los recursos del clúster en la cuenta del AWS cliente. Con AWS PrivateLink ella, el equipo de ingeniería de confiabilidad de sitios (SRE) de Red Hat puede acceder al clúster con fines de soporte y reparación mediante una subred privada conectada al punto final del AWS PrivateLink clúster.

Para obtener más información al respecto AWS PrivateLink, consulte ¿Qué es? AWS PrivateLink

Temas

- Requisitos previos
- Cree una Amazon VPC arquitectura
- Cree un clúster clásico de ROSA mediante la ROSA CLI y AWS PrivateLink
- Configure el reenvío de AWS PrivateLink DNS
- Configure un proveedor de identidades y conceda el acceso clúster
- Conceda al usuario acceso a un clúster
- Configuración de permisos de cluster-admin

- Configuración de permisos de dedicated-admin
- Acceda a a clúster través de la consola Red Hat Hybrid Cloud
- Implemente una aplicación del catálogo para desarrolladores
- Revoque los permisos de cluster-admin de un usuario
- Revoque los permisos de dedicated-admin de un usuario
- Revocar el acceso del usuario a un clúster
- Eliminar un clúster y sus AWS STS recursos

Requisitos previos

Complete las acciones previas que se enumeran enthe section called “Configuración”.

Cree una Amazon VPC arquitectura

El siguiente procedimiento crea una Amazon VPC arquitectura que se puede utilizar para alojar un clúster. Todos clúster los recursos están alojados en la subred privada. La subred pública enruta el tráfico saliente de la subred privada a través de una puerta de enlace NAT a la Internet pública. En este ejemplo, se utiliza `10.0.0.0/16` con bloque de CIDR para la Amazon VPC. Sin embargo, puede elegir otro bloque de CIDR. Para obtener más información, consulte Tamaño de la VPC.

> **Important**
>
> Si no se Amazon VPC cumplen los requisitos, se produce un error en la creación del clúster.

Example

Amazon VPC console

1. Abra la consola de Amazon VPC.
2. En el panel de VPC, elija Create VPC (Crear VPC).
3. En Recursos para crear, elija VPC y más.
4. Mantenga seleccionada la opción Generación automática de etiquetas de nombre para crear etiquetas de nombre para los recursos de la VPC, o desactívela para proporcionar sus propias etiquetas de nombre para los recursos de la VPC.

5. Para el bloque IPv4 CIDR, introduzca un rango de IPv4 direcciones para la VPC. Una VPC debe tener un rango de IPv4 direcciones.
6. (Opcional) Para admitir IPv6 el tráfico, elige el bloque IPv6 CIDR, el bloque CIDR proporcionado por Amazon IPv6 .
7. Deje Tenancy como. `Default`
8. En Número de zonas de disponibilidad (AZs), elija el número que necesite. Para las implementaciones en zonas de disponibilidad múltiples (Multi-AZ), ROSA requiere tres zonas de disponibilidad. Para elegir una AZs para sus subredes, expanda Personalizar. AZs

> **Note**
>
> Algunos tipos de ROSA instancias solo están disponibles en determinadas zonas de disponibilidad. Puede usar el `rosa list instance-types` comando ROSA CLI para enumerar todos los tipos de ROSA instancias disponibles. Para comprobar si un tipo de instancia está disponible para una zona de disponibilidad determinada, usa el AWS CLI comando`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

9. Para configurar las subredes, elija valores para Cantidad de subredes públicas y Cantidad de subredes privadas. Para elegir los rangos de direcciones IP para las subredes, expanda Personalizar bloques CIDR de subredes.

> **Note**
>
> ROSA requiere que los clientes configuren al menos una subred privada por cada zona de disponibilidad utilizada para crear clústeres.

10. Para conceder a los recursos de la subred privada acceso a Internet pública, en el caso de las puertas de enlace NAT IPv4, elija el número de puertas de enlace NAT AZs en las que desee crear las puertas de enlace NAT. En producción, se recomienda implementar una puerta de enlace de NAT en cada AZ con recursos que necesiten acceso a la Internet pública.
11. (Opcional) Si necesita acceder Amazon S3 directamente desde su VPC, elija los puntos de enlace de la VPC, S3 Gateway.

12. Deje seleccionadas las opciones de DNS predeterminadas. ROSA requiere compatibilidad con nombres de host DNS en la VPC.
13. Seleccione Creación de VPC.

AWS CLI

1. Cree una VPC con un bloque de CIDR `10.0.0.0/16`.

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

El comando anterior devuelve el ID de VPC. El siguiente es un ejemplo de salida.

```
vpc-1234567890abcdef0
```

2. Guarde el ID de VPC en una variable de entorno.

```
export VPC_ID=vpc-1234567890abcdef0
```

3. Cree una `Name` etiqueta para la VPC mediante la variable de `VPC_ID` entorno.

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. Habilite la compatibilidad con nombres de host DNS en la VPC.

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. Cree una subred pública y privada en la VPC, especificando las zonas de disponibilidad en las que se deben crear los recursos.

> **Important**
>
> ROSA requiere que los clientes configuren al menos una subred privada por cada zona de disponibilidad utilizada para crear clústeres. Para las implementaciones Multi-AZ, se

requieren tres zonas de disponibilidad. Si no se cumplen estos requisitos, se producirá un error en la creación del clúster.

> **Note**
>
> Algunos tipos de ROSA instancias solo están disponibles en determinadas zonas de disponibilidad. Puede usar el `rosa list instance-types` comando ROSA CLI para enumerar todos los tipos de ROSA instancias disponibles. Para comprobar si un tipo de instancia está disponible para una zona de disponibilidad determinada, usa el AWS CLI comando`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. Almacene la subred pública y privada IDs en variables de entorno.

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. Cree una puerta de enlace a Internet y una tabla de rutas para el tráfico saliente. Cree una tabla de enrutamiento y una dirección IP elástica para el tráfico privado.

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
```

```
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

8. Almacene IDs las variables de entorno.

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

9. Adjunte la puerta de enlace de Internet a la VPC.

```
aws ec2 attach-internet-gateway \
    --vpc-id $VPC_ID \
    --internet-gateway-id $IGW
```

10. Asocie la tabla de rutas públicas a la subred pública y configure el tráfico para que se dirija a la puerta de enlace de Internet.

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

11. Cree la puerta de enlace NAT y asóciela a la dirección IP elástica para permitir el tráfico a la subred privada.

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
```

```
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

12. Asocie la tabla de rutas privadas a la subred privada y configure el tráfico para que se dirija a la puerta de enlace NAT.

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

13. (Opcional) Para las implementaciones Multi-AZ, repita los pasos anteriores para configurar otras dos zonas de disponibilidad con subredes públicas y privadas.

Cree un clúster clásico de ROSA mediante la ROSA CLI y AWS PrivateLink

Puede usar la ROSA CLI y AWS PrivateLink crear una clúster con una sola zona de disponibilidad (Single-AZ) o varias zonas de disponibilidad (Multi-AZ). En cualquier caso, el valor de CIDR de su máquina debe coincidir con el valor de CIDR de su VPC.

El siguiente procedimiento utiliza el `rosa create cluster` comando para crear un ROSA classic. clúster Para crear una zona de disponibilidad múltiple clúster, especifique `--multi-az` en el comando y, a continuación, seleccione la subred privada IDs que desee utilizar cuando se le solicite.

> **Note**
>
> Si utiliza un firewall, debe configurarlo para que ROSA pueda acceder a los sitios que necesita para funcionar.
> Para obtener más información, consulte los requisitos para el uso de AWS PrivateLink clústeres en la documentación de Red Hat.

1. Cree los roles y políticas de IAM cuenta necesarios utilizando `--mode auto` o `--mode manual`.

- ```
  rosa create account-roles --classic --mode auto
  ```
  ```

- ```
  rosa create account-roles --classic --mode manual
  ```

  > **Note**
  >
  > Si el token de acceso sin conexión ha caducado, la ROSA CLI muestra un mensaje de error que indica que el token de autorización debe actualizarse. Para ver los pasos para solucionar problemas, consultethe section called “Solucionar problemas con los tokens de acceso sin conexión caducados por ROSA CLI”.

2. Cree un clúster mediante la ejecución de uno de los siguientes comandos.
   - Single-AZ

     ```
     rosa create cluster --private-link --cluster-name=<CLUSTER_NAME> --machine-
     cidr=10.0.0.0/16 --subnet-ids=<PRIVATE_SUBNET_ID>
     ```

   - Multi-AZ

     ```
     rosa create cluster --private-link --multi-az --cluster-name=<CLUSTER_NAME> --
     machine-cidr=10.0.0.0/16
     ```

     > **Note**
     >
     > Para crear un clúster que utilice credenciales de corta duración AWS PrivateLink con AWS Security Token Service (AWS STS), añada `--sts --mode auto` o `--sts --mode manual` al final del `rosa create cluster` comando.

3. Cree los IAM roles de clúster operador siguiendo las instrucciones interactivas.

   ```
   rosa create operator-roles --interactive -c <CLUSTER_NAME>
   ```

4. Cree el proveedor de OpenID Connect (OIDC) que los clúster operadores utilizan para autenticarse.

   ```
   rosa create oidc-provider --interactive -c <CLUSTER_NAME>
   ```

5. Compruebe el estado de su. clúster
   ```

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> El clúster `State` campo puede tardar hasta 40 minutos en mostrar el `ready` estado. Si se produce un error en el aprovisionamiento o no aparece `ready` después de 40 minutos, consulteResolución de problemas. Para ponerse en contacto con Soporte el servicio de asistencia de Red Hat para obtener asistencia, consultethe section called “Cómo obtener asistencia”.

6. Realice un seguimiento del progreso de la clúster creación observando los registros del OpenShift instalador.

```
rosa logs install -c <CLUSTER_NAME> --watch
```

Configure el reenvío de AWS PrivateLink DNS

Los clústeres que se utilizan AWS PrivateLink crean una zona alojada pública y una zona alojada privada en Route 53. Los registros de la zona alojada Route 53 privada solo se pueden resolver desde la VPC a la que están asignados.

La validación DNS-01 de Let’s Encrypt requiere una zona pública para poder emitir certificados válidos y de confianza pública para el dominio. Los registros de validación se eliminan una vez finalizada la validación de Let's Encrypt. La zona sigue siendo necesaria para emitir y renovar estos certificados, que normalmente se requieren cada 60 días. Si bien estas zonas suelen aparecer vacías, una zona pública desempeña un rol fundamental en el proceso de validación.

Para obtener más información sobre las zonas alojadas AWS privadas, consulte Trabajar con zonas privadas. Para obtener más información acerca de las zonas alojadas públicas, consulte Uso de zonas alojadas públicas.

Configure un punto Route 53 Resolver final de entrada

1. Para permitir registros como, por ejemplo, la VPC `api.<cluster_domain>` y `*.apps.<cluster_domain>` resolverlos fuera de ella, configure un punto final de Route 53 Resolver entrada.

> **Note**
>
> Al configurar un punto final de entrada, debe especificar un mínimo de dos direcciones IP para garantizar la redundancia. Le recomendamos que especifique direcciones IP que se encuentren al menos en dos zonas de disponibilidad. Opcionalmente, puede especificar direcciones IP adicionales en estas u otras zonas de disponibilidad.

2. Al configurar el punto final de entrada, selecciona la VPC y las subredes privadas que se usaron al crear el clúster.

Configure el reenvío de DNS para el clúster

Una vez que el punto final Route 53 Resolver interno esté asociado y en funcionamiento, configure el reenvío de DNS para que los servidores designados de la red puedan gestionar las consultas de DNS.

1. Configure su red corporativa para que reenvíe las consultas de DNS a las direcciones IP del dominio de nivel superior, por ejemplo `drow-pl-01.htno.p1.openshiftapps.com`.
2. Para reenviar consultas de DNS de una VPC a otra VPC, siga las instrucciones de Administración de reglas de reenvío.
3. Para configurar el servidor DNS de su red remota, consulte la documentación específica del servidor DNS para configurar el reenvío de DNS selectivo para el dominio del clúster instalado.

Configure un proveedor de identidades y conceda el acceso clúster

ROSA incluye un OAuth servidor integrado. Una vez creado ROSA clúster el suyo, debe configurarlo OAuth para usar un proveedor de identidades. A continuación, puede añadir usuarios a su proveedor de identidad configurado para concederles acceso a su clúster. Puede otorgarles permisos de `cluster-admin` o `dedicated-admin` a estos usuarios según sea necesario.

Puede configurar diferentes tipos de proveedores de identidad para su clúster. Los tipos compatibles incluyen GitHub Enterprise GitHub, Google GitLab, LDAP, OpenID Connect y proveedores de identidad. HTPasswd

> **Important**
>
> El proveedor de HTPasswd identidad se incluye solo para permitir la creación de un único usuario administrador estático. HTPasswd no se admite como proveedor de identidades de uso general para. ROSA

El siguiente procedimiento configura un proveedor de GitHub identidades como ejemplo. Para obtener instrucciones sobre cómo configurar cada uno de los tipos de proveedores de identidad compatibles, consulte Configuración de proveedores de identidad para AWS STS.

1. Ve a github.com e inicia sesión en tu cuenta. GitHub
2. Si no tienes una GitHub organización que puedas usar para el aprovisionamiento de identidades, crea una. ROSA clúster Para obtener más información, consulta los pasos de la GitHub documentación.
3. Con el modo interactivo de la ROSA CLI, configure un proveedor de identidades para su clúster ejecutando el siguiente comando.

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. Siga las instrucciones de configuración del resultado para restringir el clúster acceso a los miembros de su GitHub organización.

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. Abre la URL en el resultado y `<GITHUB_ORG_NAME>` sustitúyela por el nombre de tu GitHub organización.
6. En la página GitHub web, elija Registrar aplicación para registrar una nueva OAuth aplicación en su GitHub organización.
7. Utilice la información de la GitHub OAuth página para rellenar el resto de las solicitudes `rosa create idp` interactivas, sustituyendo `<GITHUB_CLIENT_ID>` y `<GITHUB_CLIENT_SECRET>` utilizando las credenciales GitHub OAuth de la aplicación.

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> La configuración del proveedor de identidad puede tardar aproximadamente dos minutos en activarse. Si configuraste un `cluster-admin` usuario, puedes ejecutar el `oc get pods -n openshift-authentication --watch` comando para ver cómo se vuelven a implementar los OAuth pods con la configuración actualizada.

8. Compruebe que el proveedor de identidad esté configurado correctamente.

```
rosa list idps --cluster=<CLUSTER_NAME>
```

Conceda al usuario acceso a un clúster

Puede conceder acceso a un usuario al suyo clúster agregándolo al proveedor de identidades configurado.

El siguiente procedimiento agrega un usuario a una GitHub organización que está configurada para el aprovisionamiento de identidades en el clúster.

1. Ve a github.com e inicia sesión en tu cuenta. GitHub
2. Invita a los usuarios que necesiten clúster acceder a tu organización. GitHub Para obtener más información, consulte Invitar a los usuarios a unirse a su organización en la GitHub documentación.

Configuración de permisos de `cluster-admin`

1. Otorgue los permisos de `cluster-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su nombre de usuario y clúster.

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario aparezca como miembro del grupo de `cluster-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Configuración de permisos de `dedicated-admin`

1. Otorgue los permisos de `dedicated-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su clúster nombre de usuario.

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario aparezca como miembro del grupo de `cluster-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Acceda a a clúster través de la consola Red Hat Hybrid Cloud

Tras crear un usuario clúster administrador o añadir un usuario a su proveedor de identidad configurado, puede iniciar sesión en su cuenta a clúster través de la consola de Red Hat Hybrid Cloud.

1. Obtenga la URL de la consola para clúster usted mediante el siguiente comando. `<CLUSTER_NAME>`Sustitúyala por el nombre de tu clúster.

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. Navegue hasta la URL de la consola en la salida e inicie sesión.
   - Si ha creado un usuario de `cluster-admin`, inicie sesión con las credenciales proporcionadas.
   - Si configuró un proveedor de identidad para usted clúster, elija el nombre del proveedor de identidad en el cuadro de diálogo Iniciar sesión con... y complete cualquier solicitud de autorización que presente su proveedor.

Implemente una aplicación del catálogo para desarrolladores

Desde la consola de la nube híbrida de Red Hat, puede implementar una aplicación de prueba del catálogo de desarrolladores y exponerla con una ruta.

1. Diríjase a la Consola de la nube híbrida de Red Hat y seleccione el clúster en el que desea implementar la aplicación.
2. En la página del clúster, seleccione Abrir consola.
3. Desde la perspectiva Administrador, seleccione Inicio > Proyectos > Crear proyecto.
4. Introduzca un nombre para el proyecto y, si lo desea, añada un Nombre de visualización y una Descripción.
5. Seleccione Crear para crear el proyecto.
6. Cambie a la perspectiva Desarrollador y seleccione +Añadir. Asegúrese de que el proyecto seleccionado sea el que se acaba de crear.
7. En el cuadro de diálogo del Catálogo de desarrolladores, seleccione Todos los servicios.
8. En la página del catálogo para desarrolladores, seleccione Idiomas > en el JavaScriptmenú.
9. Elija Node.js y, a continuación, elija Crear aplicación para abrir la página Crear Source-to-Image aplicación.

> **Note**
>
> Puede que tenga que seleccionar Eliminar todos los filtros para que aparezca la opción Node.js.

10. En la sección Git, seleccione Probar ejemplo.
11. En el campo Nombre, agregue un nombre único.
12. Seleccione Crear.

> **Note**
>
> La nueva aplicación tarda varios minutos en implementarse.

13. Una vez finalizada la implementación, elija la URL de la ruta para la aplicación.

    Se abre una nueva pestaña en el navegador con un mensaje similar al siguiente.

```
Welcome to your Node.js application on OpenShift
```

14. (Opcional) Elimine la aplicación y limpie los recursos.
    a. Desde la perspectiva de Administrador, seleccione Inicio > Proyectos.
    b. Abra el menú de acciones del proyecto y seleccione Eliminar proyecto.

Revoque los permisos de **`cluster-admin`** de un usuario

1. Otorgue los permisos de `cluster-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su clúster nombre de usuario.

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario no figure como miembro del grupo de `cluster-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revoque los permisos de **`dedicated-admin`** de un usuario

1. Otorgue los permisos de `dedicated-admin` mediante el siguiente comando. Sustituya `<IDP_USER_NAME>` y `<CLUSTER_NAME>` por su clúster nombre de usuario.

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Compruebe que el usuario no figure como miembro del grupo `dedicated-admins`.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revocar el acceso del usuario a un clúster

Puede revocar el clúster acceso de un usuario del proveedor de identidades quitándolo del proveedor de identidades configurado.

Puede configurar diferentes tipos de proveedores de identidad para su clúster. El siguiente procedimiento revoca el clúster acceso de un miembro de una GitHub organización.

1. Ve a github.com e inicia sesión en tu cuenta. GitHub
2. Elimina al usuario de tu organización. GitHub Para obtener más información, consulte Eliminar a un miembro de su organización en la GitHub documentación.

Eliminar un clúster y sus AWS STS recursos

Puede usar la ROSA CLI para eliminar una clúster que use AWS Security Token Service (AWS STS). También puede usar la ROSA CLI para eliminar las IAM funciones y el proveedor de OIDC creados por. ROSA Para eliminar las IAM políticas creadas por ROSA, puede utilizar la IAM consola.

> **Important**
>
> IAM las funciones y políticas creadas por ROSA pueden ser utilizadas por otros ROSA clústeres de la misma cuenta.

1. Elimine los registros clúster y observe los mismos. Sustituya <CLUSTER_NAME> por el nombre o ID del clúster.

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> Debe esperar clúster a que se eliminen por completo antes de eliminar las IAM funciones, las políticas y el proveedor de OIDC. Los roles de IAM de la cuenta son necesarios para eliminar los recursos creados por el instalador. Las funciones de IAM de los operadores

son necesarias para limpiar los recursos creados por los operadores. OpenShift Los operadores utilizan el proveedor de OIDC para autenticar.

2. Elimine el proveedor de OIDC que utilizan los clúster operadores para autenticarse ejecutando el siguiente comando.

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. Elimine las funciones de operador específicas del clúster. IAM

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. Elimine los roles de IAM de la cuenta mediante el siguiente comando. Sustituya `<PREFIX>` por el prefijo de los roles de IAM de la cuenta que desea eliminar. Si especificó un prefijo personalizado al crear los roles de IAM de la cuenta, especifique el prefijo predeterminado de `ManagedOpenShift`.

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. Elimine las IAM políticas creadas por. ROSA
   a. Inicie sesión en la consola de IAM.
   b. En el menú Administración de acceso de la izquierda, seleccione Políticas.
   c. Seleccione la política que desea eliminar y elija Acciones > Eliminar.
   d. Introduzca el nombre de la política y seleccione Eliminar.
   e. Repita este paso para eliminar cada una de las políticas de IAM para el clúster.

Seguridad en ROSA

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada 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. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de cumplimiento a los que se aplica ROSA, consulte Servicios de AWS Alcance by Compliance Program.
- Seguridad en la nube: su responsabilidad viene determinada por lo Servicio de AWS que utilice. También es 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 cuando se utiliza ROSA. Le muestra cómo configurarlo para ROSA cumplir sus objetivos de seguridad y conformidad. También aprenderá a usar otros Servicios de AWS que le ayuden a monitorear y proteger sus ROSA recursos.

Contenido

Protección de datos en ROSA

La the section called “Responsabilidades” documentación y el modelo de responsabilidad AWS compartida definen la protección de datos en ROSA. AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Red Hat es responsable

de proteger la infraestructura del clúster y la plataforma de servicios subyacente. El cliente es responsable de mantener el control sobre el contenido que se aloja en esta infraestructura. Este contenido incluye las tareas de configuración y administración de la seguridad Servicios de AWS que utilice. Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos. Para obtener más información sobre la protección de datos en Europa, consulte la publicación de blog AWS Shared Responsibility Model and 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 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.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad gestionados avanzados Amazon Macie, como los que ayudan a descubrir y proteger los datos confidenciales almacenados en ellos Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un terminal FIPS. Para obtener más información acerca de los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, números de cuenta de sus clientes, en los campos de formato libre, como el campo Nombre. Esto incluye cuando trabaja con ROSA o Servicios de AWS utiliza la consola, la API o. AWS CLI AWS SDKs Todos los datos que introduzcas ROSA o cualquier otro servicio podrían recogerse para incluirlos en los registros de diagnóstico. Cuando le proporcione una URL a un servidor externo, no incluya información sobre las credenciales en la URL para validar la solicitud en ese servidor.

Temas

- Protección de datos mediante cifrado

Protección de datos mediante cifrado

La protección de datos se refiere a la protección de los datos mientras están en tránsito (mientras viajan hacia y desde ROSA) y en reposo (mientras están almacenados en los discos de los centros de AWS datos).

Red Hat OpenShift Service en AWS proporciona acceso seguro a Amazon Elastic Block Store (Amazon EBS) los volúmenes de almacenamiento conectados a Amazon EC2 las instancias para el plano de ROSA control, la infraestructura y los nodos de trabajo, así como a los volúmenes persistentes de Kubernetes para el almacenamiento persistente. ROSA cifra los datos de volumen en reposo y en tránsito, y utiliza AWS Key Management Service (AWS KMS) para ayudar a proteger los datos cifrados. El servicio utiliza Amazon S3 como contenedor el almacenamiento del registro de imágenes, que está cifrado en reposo de forma predeterminada.

Important

Porque ROSA es un servicio gestionado, AWS y Red Hat gestiona la infraestructura que ROSA utiliza. Los clientes no deben intentar cerrar manualmente las Amazon EC2 instancias que ROSA utilizan desde la AWS consola o la CLI. Esta acción puede provocar que se pierdan datos de los clientes.

Cifrado de datos para Amazon EBS volúmenes de almacenamiento respaldados

Red Hat OpenShift Service en AWS utiliza el marco de volúmenes persistentes (PV) de Kubernetes para permitir a los administradores de clústeres aprovisionar un clúster con almacenamiento persistente. Los volúmenes persistentes, así como el plano de control, la infraestructura y los nodos de trabajo, están respaldados por Amazon Elastic Block Store (Amazon EBS) volúmenes de almacenamiento adjuntos a las instancias. Amazon EC2

En el caso de los volúmenes ROSA persistentes y los nodos respaldados por Amazon EBS, las operaciones de cifrado se realizan en los servidores que alojan las instancias de EC2, lo que garantiza la seguridad tanto de los datos en reposo como de los datos en tránsito entre una instancia y su almacenamiento adjunto. Para obtener más información, consulte el Amazon EBS cifrado en la Guía del Amazon EC2 usuario.

Cifrado de datos para el controlador Amazon EBS CSI y el controlador Amazon EFS CSI

ROSA de forma predeterminada, utiliza el controlador Amazon EBS CSI para aprovisionar el almacenamiento. Amazon EBS El controlador Amazon EBS CSI y el operador del controlador Amazon EBS CSI se instalan en el clúster de forma predeterminada, en el espacio de nombres. `openshift-cluster-csi-drivers` El controlador y el operador Amazon EBS CSI le permiten aprovisionar volúmenes persistentes de forma dinámica y crear instantáneas de los volúmenes.

ROSA también es capaz de aprovisionar volúmenes persistentes mediante el controlador CSI y Amazon EFS el Amazon EFS operador del controlador CSI. El Amazon EFS controlador y el operador también permiten compartir los datos del sistema de archivos entre módulos o con otras aplicaciones dentro o fuera de Kubernetes.

Los datos de volumen están protegidos en tránsito tanto para el controlador CSI como para el controlador Amazon EBS CSI. Amazon EFS Para obtener más información, consulte Uso de la interfaz de almacenamiento de contenedores (CSI) en la documentación de Red Hat.

> **Important**
>
> Al aprovisionar volúmenes ROSA persistentes de forma dinámica mediante el controlador Amazon EFS CSI, tenga en Amazon EFS cuenta el ID de usuario, el ID de grupo (GID) y el grupo secundario del punto de acceso al evaluar los permisos IDs del sistema de archivos. Amazon EFS reemplaza el usuario y el grupo de los archivos IDs por el usuario y el grupo IDs del punto de acceso e ignora el cliente NFS. IDs Como resultado, ignora la configuración de Amazon EFS forma silenciosa. `fsGroup` ROSA no puede reemplazar los archivos mediante el GIDs uso de. `fsGroup` Cualquier módulo que pueda acceder a un punto de Amazon EFS acceso montado podrá acceder a cualquier archivo del volumen. Para obtener más información, consulte Trabajar con puntos de Amazon EFS acceso en la Guía del Amazon EFS usuario.

Cifrado ETCD

ROSA ofrece la opción de habilitar el cifrado de los valores `etcd` clave del `etcd` volumen durante la creación del clúster, añadiendo una capa de cifrado adicional. Tras cifrar `etcd`, se incurrirá en una sobrecarga de rendimiento adicional de aproximadamente un 20 %. Le recomendamos que habilite el cifrado de `etcd` solo si lo necesita específicamente para su caso. Para obtener más información, consulte el cifrado etcd en la definición del ROSA servicio.

Administración de claves

ROSA KMS keys se utiliza para gestionar de forma segura los volúmenes de datos del plano de control, la infraestructura y los volúmenes de datos de los trabajadores y los volúmenes persistentes para las aplicaciones de los clientes. Durante la creación del clúster, tiene la opción de utilizar la clave AWS gestionada por defecto KMS key proporcionada por Amazon EBS el cliente o especificar su propia clave gestionada por el cliente. Para obtener más información, consulte the section called "Administración de claves".

Cifrado de datos para el registro de imágenes integrado

ROSA proporciona un registro de imágenes de contenedores integrado para almacenar, recuperar y compartir imágenes de contenedores mediante almacenamiento en Amazon S3 cubos. El operador de registro de OpenShift imágenes configura y administra el registro. Proporciona una out-of-the-box solución para que los usuarios administren las imágenes que ejecutan sus cargas de trabajo y se ejecuta sobre la infraestructura de clústeres existente. Para obtener más información, consulte Registro en la documentación de Red Hat.

ROSA ofrece registros de imágenes públicos y privados. En el caso de las aplicaciones empresariales, se recomienda utilizar un registro privado para prevenir el uso de las imágenes por parte de usuarios no autorizados. Para proteger los datos inactivos de su registro, ROSA utiliza de forma predeterminada el cifrado del lado del servidor con claves Amazon S3 administradas (SSE-S3). Esto no requiere ninguna acción de su parte y no conlleva ningún cargo adicional. Para obtener más información, consulte Protección de datos mediante el cifrado del lado del servidor con claves de cifrado Amazon S3 administradas (SSE-S3) en la Guía del usuario. Amazon S3

ROSA utiliza el protocolo Transport Layer Security (TLS) para proteger los datos en tránsito hacia y desde el registro de imágenes. Para obtener más información, consulte Registro en la documentación de Red Hat.

Privacidad del tráfico entre redes

Red Hat OpenShift Service en AWS usa Amazon Virtual Private Cloud (Amazon VPC) para crear límites entre los recursos ROSA del clúster y controlar el tráfico entre ellos, la red local e Internet. Para obtener más información sobre Amazon VPC la seguridad, consulte la privacidad del tráfico entre redes Amazon VPC en la Guía del Amazon VPC usuario.

Dentro de la VPC, puede configurar sus ROSA clústeres para que usen un servidor proxy HTTP o HTTPS para denegar el acceso directo a Internet. Si es administrador de clústeres, también puede

definir políticas de red a nivel de pod que restrinjan el tráfico entre redes a los pods de su ROSA clúster. Para obtener más información, consulte the section called “Seguridad de la infraestructura”.

Cifrado de datos mediante KMS

ROSA utiliza AWS KMS para gestionar de forma segura las claves de los datos cifrados. Los volúmenes del plano de control, la infraestructura y los nodos de trabajo se cifran de forma predeterminada mediante la AWS gestión KMS key proporcionada por Amazon EBS. KMS key Tiene el alias`aws/ebs`. Los volúmenes persistentes que utiliza la clase de almacenamiento gp3 predeterminada también se cifran de forma predeterminada con esta KMS key.

Los ROSA clústeres recién creados están configurados para usar la clase de almacenamiento gp3 predeterminada para cifrar los volúmenes persistentes. Los volúmenes persistentes creados con cualquier otra clase de almacenamiento solo se cifran si la clase de almacenamiento está configurada para cifrarse. Para obtener más información sobre las clases de almacenamiento ROSA prediseñadas, consulte Configuración del almacenamiento persistente en la documentación de Red Hat.

Durante la creación del clúster, puede optar por cifrar los volúmenes persistentes del clúster con la clave Amazon EBS proporcionada por defecto o especificar su propia simetría gestionada por el cliente. KMS keyPara obtener más información sobre la creación de claves, consulte Creación de claves KMS de cifrado simétrico en la Guía para desarrolladores. AWS KMS

También puede cifrar los volúmenes persistentes de los contenedores individuales de un clúster al definir una KMS key. Esto resulta útil cuando se utilizan directrices explícitas de conformidad y seguridad a AWS la hora de realizar la implementación en. Para obtener más información, consulte Cifrar volúmenes persistentes de contenedores AWS con a KMS key en la documentación de Red Hat.

Tenga en cuenta lo siguiente al cifrar volúmenes persistentes con su propia KMS keys:

- Si utiliza el cifrado KMS con el suyo propio KMS key, la clave debe estar en el mismo lugar Región de AWS que su clúster.
- La creación y el uso del tuyo propio conllevan un coste KMS keys. Para obtener más información, consulte Precios de AWS Key Management Service.

Gestión de identidad y acceso para ROSA

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAM los administradores controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar ROSA los recursos. IAM es una Servicio de AWS que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice ROSA.

Usuario del servicio: si utiliza el ROSA servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más ROSA funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función en ROSA, consultethe section called “Resolución de problemas”.

Administrador de servicios: si está a cargo de ROSA los recursos de su empresa, probablemente tenga acceso total a ellos ROSA. Su trabajo consiste en determinar a qué ROSA funciones y recursos deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos de IAM.

IAM administrador: si es IAM administrador, puede que desee obtener más información sobre las políticas que se utilizan para administrar el acceso a ROSA. Para ver ejemplos de políticas ROSA basadas en la identidad que puede utilizar IAM, consulte. the section called “ ROSA ejemplos de políticas basadas en la identidad”

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 Cuenta de AWS raíz Usuario de IAM, o asumiendo un IAM rol.

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center (IAM Identity Center) los usuarios, 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, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal Consola de administración de AWS 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 usuario de AWS inicio de sesión.

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 cómo usar el método recomendado para firmar las solicitudes tú mismo, consulta Cómo firmar las solicitudes de la AWS API en la Guía del IAM usuario.

Independientemente del método de autenticación que utilice, es posible que también 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 multifactorial en la Guía del usuario del AWS IAM Identity Center (sucesor del inicio de sesión AWS único) y Uso de la autenticación multifactorial (MFA) AWS 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 única 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 utilice el usuario raíz para sus tareas diarias. Proteja sus credenciales de usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren

que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía del IAM usuario.

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 información sobre el Centro de identidades de IAM, consulte ¿Qué es el Centro de identidades de IAM? en la guía del AWS usuario del IAM Identity Center (sucesor del AWS Single Sign-On).

Usuarios de IAM y grupos

Una Usuario de IAMes una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, te recomendamos Usuarios de IAM que utilices credenciales temporales en lugar de crearlas con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales de larga duración Usuarios de IAM, le recomendamos que rote 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 IAM grupo es una identidad que especifica una colección de Usuarios de IAM. No puede iniciar sesión como grupo. Puede usar 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 IAM los recursos.

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 Cuándo crear un rol Usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

IAM roles

Un IAM rol es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos. Es similar a un Usuario de IAM, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el Consola de administración de AWS cambiando de rol. Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para obtener más información sobre los métodos de uso de roles, consulte Uso de IAM roles en la Guía del usuario de IAM.

IAM los roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuarios federados: para asignar permisos a una identidad federada, debe crear un rol y definir los permisos para el rol. 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 para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del 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 sobre los conjuntos de permisos, consulte los conjuntos de permisos en la Guía del usuario del AWS IAM Identity Center (sucesor del AWS Single Sign-On).
- Usuario de IAM Permisos temporales: An Usuario de IAM puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso a varias cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte En qué se diferencian las IAM funciones de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones Amazon EC2 o almacene objetos en Amazon S3él. Es posible que un servicio

haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a un servicio.

- Sesiones de acceso directo (FAS): cuando utilizas un rol Usuario de IAM o 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 del solicitante 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.
- Función de servicio: una función de servicio es una IAM función que asume un servicio para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro 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 a un 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 su IAM cuenta y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

- Aplicaciones en ejecución Amazon EC2 : puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una Amazon EC2 instancia y que realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la Amazon EC2 instancia. Para asignar un AWS rol a una Amazon 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 Amazon EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a las aplicaciones que se ejecutan en Amazon EC2 instancias en la Guía del usuario de IAM.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del usuario de IAM.

Administración del acceso con 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 de las políticas determinan si la solicitud está permitida o denegada. 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. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAM las políticas definen los permisos para una acción independientemente del método que se utilice 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 Consola de administración de AWS AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en la identidad son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un Usuario de IAM rol o un grupo. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte Creación de políticas en la Guía IAM del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas integradas están integradas directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para 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 políticas JSON que se asocian a un recurso. 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 basada en 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 puede usar políticas AWS administradas desde una política IAM 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, AWS WAF, y Amazon VPC son ejemplos de servicios que admiten. ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía del usuario 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 función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (Usuario de IAM o función). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en 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 anula la autorización. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para IAM las entidades 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 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, incluido cada usuario Cuenta de AWS raíz. Para obtener más información sobre Organizations SCPs, consulte Políticas de control de servicios (SCPs) 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 identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política basada en 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.

ROSA ejemplos de políticas basadas en la identidad

De forma predeterminada, Usuarios de IAM los roles no tienen permiso para crear o modificar AWS recursos. Tampoco pueden realizar tareas con la AWS API Consola de administración de AWS AWS CLI, o. IAM El administrador debe crear IAM políticas que concedan permiso a los usuarios y roles para realizar operaciones de API específicas en los recursos específicos que necesitan. A continuación, el administrador debe adjuntar esas políticas a los Usuarios de IAM grupos que requieran esos permisos.

Para obtener información sobre cómo crear una política IAM basada en la identidad con estos ejemplos de documentos de política de JSON, consulte Creación de políticas en la pestaña JSON de la Guía del usuario de IAM.

Uso de la consola ROSA

Para suscribirse ROSA desde la consola, su director de IAM debe tener los AWS Marketplace permisos necesarios. Los permisos permiten al director suscribirse y cancelar la suscripción a la lista de ROSA productos AWS Marketplace y ver AWS Marketplace las suscripciones. Para añadir los permisos necesarios, ve a la ROSA consola y adjunta la política AWS gestionada `ROSAManageSubscription` a tu cuenta principal de IAM. Para obtener más información acerca de `ROSAManageSubscription`, consulte the section called “AWS política gestionada: ROSAManage suscripción”.

Autorizar a ROSA con HCP a administrar los recursos AWS

ROSA, con planes de control alojados (HCP), utiliza políticas AWS administradas con los permisos necesarios para la operación y el soporte del servicio. Utiliza la ROSA CLI o la IAM consola para adjuntar estas políticas a las funciones de servicio de su Cuenta de AWS.

Para obtener más información, consulte the section called “ AWS políticas gestionadas”.

¿Autorizar a ROSA classic a administrar los recursos AWS

ROSA classic utiliza políticas de IAM administradas por el cliente con permisos predefinidos por el servicio. Utiliza la ROSA CLI para crear estas políticas y adjuntarlas a las funciones de servicio de su Cuenta de AWS. ROSA requiere que estas políticas estén configuradas según lo definido por el servicio para garantizar el funcionamiento continuo y el soporte del servicio.

> **Note**
>
> No debe modificar las políticas clásicas de ROSA sin antes consultar a Red Hat. Si lo hace, podría invalidar el acuerdo de nivel de servicio de Red Hat con un tiempo de actividad de los clústeres del 99,95%. ROSA, con planes de control alojados, utiliza políticas AWS administradas con un conjunto de permisos más limitado. Para obtener más información, consulte the section called “ AWS políticas gestionadas”.

Existen dos tipos de políticas administradas por el cliente ROSA: políticas de cuentas y políticas de operador. Las políticas de cuentas están asociadas a las IAM funciones que el servicio utiliza para establecer una relación de confianza con Red Hat en lo que respecta al soporte del ingeniero de confiabilidad del sitio (SRE), la creación de clústeres y la funcionalidad de procesamiento. Las

políticas de los operadores están vinculadas a las IAM funciones que OpenShift los operadores utilizan para las operaciones de clúster relacionadas con la entrada, el almacenamiento, el registro de imágenes y la administración de nodos. Las políticas de cuentas se crean una vez por clúster Cuenta de AWS, mientras que las políticas de operador se crean una vez por clúster.

Para obtener más información, consulte the section called “Políticas de cuentas ROSA classic” y the section called “Pólizas de operador clásicas de ROSA”.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo se puede crear una política que Usuarios de IAM permita ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante. AWS CLI

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Effect": "Allow",
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

Políticas de cuentas clásicas de ROSA

En esta sección se proporcionan detalles sobre las políticas de cuenta que se requieren para ROSA classic. Estos permisos son necesarios para que ROSA classic gestione AWS los recursos en los que se ejecutan los clústeres y permita el soporte de los clústeres por parte de los ingenieros de confiabilidad de sitios de Red Hat. Puede asignar un prefijo personalizado a los nombres de las políticas, pero, de lo contrario, estas políticas deberían tener el nombre definido en esta página (por ejemplo,`ManagedOpenShift-Installer-Role-Policy`).

Las políticas de la cuenta son específicas de una versión OpenShift secundaria y son compatibles con versiones anteriores. Antes de crear o actualizar un clúster, debe comprobar que la versión de la política y la versión del clúster son las mismas`rosa list account-roles`. Si la versión de la política es inferior a la versión del clúster, `rosa upgrade account-roles` ejecútela para actualizar las funciones y las políticas asociadas. Puede usar las mismas políticas y roles de cuenta para varios clústeres de la misma versión secundaria.

[Prefijo] -Política de roles del instalador

Puede adjuntar `[Prefix]-Installer-Role-Policy` a sus entidades de IAM. Antes de poder crear un clúster clásico de ROSA, primero debe adjuntar esta política a un rol de IAM denominado. `[Prefix]-Installer-Role` Esta política concede los permisos necesarios que permiten al ROSA instalador gestionar los AWS recursos necesarios para la creación del clúster.

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:AssociateDhcpOptions",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
```

```
                "ec2:AttachNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CopyImage",
                "ec2:CreateDhcpOptions",
                "ec2:CreateInternetGateway",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteDhcpOptions",
                "ec2:DeleteInternetGateway",
                "ec2:DeleteNatGateway",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteSubnet",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeleteVpc",
                "ec2:DeleteVpcEndpoints",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNatGateways",
```

```
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:DetachInternetGateway",
                "ec2:DisassociateRouteTable",
                "ec2:GetConsoleOutput",
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVpcAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
```

```
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:GetInstanceProfile",
                "iam:TagInstanceProfile",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:ListInstanceProfiles",
                "iam:ListInstanceProfilesForRole",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:ListUserPolicies",
                "iam:ListUsers",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:SimulatePrincipalPolicy",
                "iam:TagRole",
                "iam:UntagRole",
                "route53:ChangeResourceRecordSets",
                "route53:ChangeTagsForResource",
                "route53:CreateHostedZone",
                "route53:DeleteHostedZone",
                "route53:GetAccountLimit",
                "route53:GetChange",
                "route53:GetHostedZone",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
```

```
                "route53:ListTagsForResource",
                "route53:UpdateHostedZoneComment",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketAcl",
                "s3:GetBucketCORS",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListAWSDefaultServiceQuotas",
                "sts:AssumeRole",
                "sts:AssumeRoleWithWebIdentity",
                "sts:GetCallerIdentity",
                "tag:GetResources",
                "tag:UntagResources",
                "ec2:CreateVpcEndpointServiceConfiguration",
                "ec2:DeleteVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServiceConfigurations",
```

```
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:ModifyVpcEndpointServicePermissions",
                "kms:DescribeKey",
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

[Prefijo] - ControlPlane -Role-Policy

Puede adjuntar `[Prefix]-ControlPlane-Role-Policy` a sus entidades de IAM. Antes de poder crear un clúster clásico de ROSA, primero debe adjuntar esta política a un rol de IAM denominado. `[Prefix]-ControlPlane-Role` Esta política otorga a ROSA classic los permisos necesarios para gestionar Amazon EC2 y leer Elastic Load Balancing KMS keys los recursos que alojan el plano de ROSA control.

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
```

```
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteVolume",
                "ec2:Describe*",
                "ec2:DetachVolume",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyVolume",
                "ec2:RevokeSecurityGroupIngress",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerPolicy",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteLoadBalancerListeners",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:Describe*",
                "elasticloadbalancing:DetachLoadBalancerFromSubnets",
                "elasticloadbalancing:ModifyListener",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefijo] -Política de funciones del trabajador

Puede adjuntar `[Prefix]-Worker-Role-Policy` a sus entidades de IAM. Antes de poder crear un clúster clásico de ROSA, primero debe adjuntar esta política a un rol de IAM denominado. `[Prefix]-Worker-Role` Esta política otorga los permisos necesarios a ROSA classic para describir las instancias de EC2 que se ejecutan como nodos de trabajo.

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefijo] -Política de roles de soporte

Puede adjuntar `[Prefix]-Support-Role-Policy` a sus entidades de IAM. Antes de poder crear un clúster clásico de ROSA, primero debe adjuntar esta política a un rol de IAM denominado. `[Prefix]-Support-Role` Esta política otorga los permisos necesarios al departamento de ingeniería de confiabilidad de sitios de Red Hat para observar, diagnosticar y respaldar los AWS recursos que utilizan los clústeres ROSA clásicos, incluida la capacidad de cambiar el estado de los nodos del clúster.

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:LookupEvents",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:CopySnapshot",
                "ec2:CreateNetworkInsightsPath",
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:DeleteTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAddressesAttribute",
                "ec2:DescribeAggregateIdFormat",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeCarrierGateways",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeCoipPools",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeIdFormat",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
```

```
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLocalGatewayRouteTables",
                "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
                "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
                "ec2:DescribeLocalGateways",
                "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
                "ec2:DescribeLocalGatewayVirtualInterfaces",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInsightsAnalyses",
                "ec2:DescribeNetworkInsightsPaths",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePlacementGroups",
                "ec2:DescribePrefixLists",
                "ec2:DescribePrincipalIdFormat",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeRouteTables",
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshotAttribute",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGatewayAttachments",
                "ec2:DescribeTransitGatewayConnectPeers",
                "ec2:DescribeTransitGatewayConnects",
                "ec2:DescribeTransitGatewayMulticastDomains",
                "ec2:DescribeTransitGatewayPeeringAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeVolumeAttribute",
                "ec2:DescribeVolumes",
```

```
                "ec2:DescribeVolumesModifications",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetAssociatedIpv6PoolCidrs",
                "ec2:GetConsoleOutput",
                "ec2:GetManagedPrefixListEntries",
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:GetTransitGatewayAttachmentPropagations",
                "ec2:GetTransitGatewayMulticastDomainAssociations",
                "ec2:GetTransitGatewayPrefixListReferences",
                "ec2:GetTransitGatewayRouteTableAssociations",
                "ec2:GetTransitGatewayRouteTablePropagations",
                "ec2:ModifyInstanceAttribute",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:SearchLocalGatewayRoutes",
                "ec2:SearchTransitGatewayMulticastGroups",
                "ec2:SearchTransitGatewayRoutes",
                "ec2:StartInstances",
                "ec2:StartNetworkInsightsAnalysis",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListenerCertificates",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeRules",
```

```
                "elasticloadbalancing:DescribeSSLPolicies",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GetRole",
                "iam:ListRoles",
                "kms:CreateGrant",
                "route53:GetHostedZone",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "s3:GetBucketTagging",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListAllMyBuckets",
                "sts:DecodeAuthorizationMessage",
                "tiros:CreateQuery",
                "tiros:GetQueryAnswer",
                "tiros:GetQueryExplanation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::managed-velero*",
                "arn:aws:s3:::*image-registry*"
            ]
        }
    ]
}
```

Las políticas de operador clásicas de ROSA

En esta sección se proporcionan detalles sobre las políticas de operador que se requieren para ROSA classic. Antes de poder crear un clúster ROSA classic, primero debe adjuntar estas políticas a

las funciones de operador pertinentes. Se requiere un conjunto único de roles de operador para cada clúster.

Estos permisos son necesarios para que los OpenShift operadores puedan gestionar los nodos de clústeres clásicos de ROSA. Puede asignar un prefijo personalizado a los nombres de las políticas para simplificar la administración de las políticas (por ejemplo,`ManagedOpenShift-openshift-ingress-operator-cloud-credentials`).

[Prefijo] - -credenciales openshift-ingress-operator-cloud

Puede adjuntar `[Prefix]-openshift-ingress-operator-cloud-credentials` a sus entidades de IAM. Esta política otorga los permisos necesarios al operador de ingreso para aprovisionar y administrar los balanceadores de carga y las configuraciones de DNS para el acceso a clústeres externos. La política también permite al operador de entrada leer y filtrar los valores de las etiquetas de Route 53 recursos para detectar las zonas alojadas. Para obtener más información sobre el operador, consulte el Operador OpenShift de entrada en la OpenShift GitHub documentación.

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "elasticloadbalancing:DescribeLoadBalancers",
                "route53:ListHostedZones",
                "route53:ListTagsForResources",
                "route53:ChangeResourceRecordSets",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefijo] - - openshift-cluster-csi-drivers ebs-cloud-credentials

Puede adjuntar `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` a sus entidades de IAM. Esta política otorga los permisos necesarios al operador del controlador Amazon EBS CSI para instalar y mantener el controlador Amazon EBS CSI en un clúster ROSA classic. Para obtener más información sobre el operador, consulte aws-ebs-csi-driver-operator en la documentación. OpenShift GitHub

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateSnapshot",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DetachVolume",
                "ec2:EnableFastSnapshotRestores",
                "ec2:ModifyVolume"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefijo] - -cloud-credentials openshift-machine-api-aws

Puede adjuntar `[Prefix]-openshift-machine-api-aws-cloud-credentials` a sus entidades de IAM. Esta política otorga los permisos necesarios al operador de Machine Config para describir, ejecutar y finalizar Amazon EC2 las instancias administradas como nodos de trabajo. Esta política también otorga permisos para permitir el cifrado del disco del volumen raíz del nodo de trabajo mediante AWS KMS keys. Para obtener más información sobre el operador, consulte machine-config-operatorla OpenShift GitHub documentación.

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
```

```
        {
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

[Prefijo] - -cloud-credentials openshift-cloud-credential-operator

Puede adjuntar `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` a sus entidades de IAM. Esta política otorga los permisos necesarios al operador de credenciales en la nube para recuperar Usuario de IAM detalles, como la clave IDs de acceso, los documentos de política en línea adjuntos, la fecha de creación del usuario, la ruta, el ID de usuario y el nombre de recurso de Amazon (ARN). Para obtener más información sobre el operador, consulte cloud-credential-operatorla documentación. OpenShift GitHub

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetUser",
                "iam:GetUserPolicy",
                "iam:ListAccessKeys"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefijo] - -cloud-credentials openshift-image-registry-installer

Puede adjuntar `[Prefix]-openshift-image-registry-installer-cloud-credentials` a sus entidades de IAM. Esta política otorga al operador de registro de imágenes los permisos necesarios para aprovisionar y administrar los recursos para el registro de imágenes integrado en el clúster de ROSA classic y los servicios dependientes, incluidos los correspondientes. Amazon S3 Esto es necesario para que el operador pueda instalar y mantener el registro interno de un clúster ROSA classic. Para obtener más información sobre el operador, consulte Image Registry Operator en la OpenShift GitHub documentación.

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketTagging",
                "s3:GetBucketTagging",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration",
```

```
                "s3:PutLifecycleConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucketMultipartUploads",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefijo] - - openshift-cloud-network-config controller-cloud-cr

Puede adjuntar `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` a sus entidades de IAM. Esta política otorga los permisos necesarios al operador del controlador Cloud Network Config para aprovisionar y administrar los recursos de red para que los utilice la superposición de redes de clústeres clásica de ROSA. El operador usa estos permisos para administrar las direcciones IP privadas de las Amazon EC2 instancias que forman parte del clúster clásico de ROSA. Para obtener más información sobre el operador, consulte C loud-network-config-controller en la OpenShift GitHub documentación.

Política de permisos

Los permisos definidos en este documento de política especifican qué acciones están permitidas o denegadas.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssignPrivateIpAddresses",
```

```
                "ec2:UnassignIpv6Addresses",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS políticas administradas para ROSA

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, consulta las políticas AWS gestionadas en la Guía del IAM usuario.

AWS política gestionada: ROSAManage suscripción

Puede adjuntar la `ROSAManageSubscription` política a sus IAM entidades. Antes de activarla ROSA en la AWS ROSA consola, primero debe adjuntar esta política a un rol de IAM.

Esta política le concede los AWS Marketplace permisos necesarios para gestionar la ROSA suscripción.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `aws-marketplace:Subscribe`- Otorga permiso para suscribirse al AWS Marketplace producto durante ROSA.
- `aws-marketplace:Unsubscribe`- Permite a los directores eliminar las suscripciones a los AWS Marketplace productos.
- `aws-marketplace:ViewSubscriptions`- Permite a los directores ver las suscripciones desde. AWS Marketplace Esto es necesario para que el IAM director pueda ver las AWS Marketplace suscripciones disponibles.

Para ver el documento de política de JSON completo, consulte ROSAManageSuscripción en la Guía de referencia de políticas AWS gestionadas.

ROSA con políticas de cuentas de HCP

En esta sección se proporcionan detalles sobre las políticas de cuenta que se requieren para ROSA con planes de control alojados (HCP). Estas políticas AWS administradas añaden los permisos utilizados por ROSA con las funciones de IAM de HCP. Los permisos son necesarios para la asistencia técnica de la ingeniería de confiabilidad del sitio (SRE) de Red Hat, la instalación de clústeres, y las funciones informáticas y del plano de control.

> **Note**
>
> AWS Las políticas gestionadas están diseñadas para que ROSA las utilice con planos de control alojados (HCP). Los clústeres clásicos de ROSA utilizan políticas de IAM gestionadas por el cliente. Para obtener más información sobre las políticas clásicas de ROSA, consulte the section called “Políticas de cuentas ROSA classic” ythe section called “Pólizas de operador clásicas de ROSA”.

AWS política gestionada: ROSAWorker InstancePolicy

Puede adjuntarla `ROSAWorkerInstancePolicy` a sus IAM entidades. Antes de crear un clúster, debe tener un rol de IAM con esta política adjunta. Un servicio de ROSA hace llamadas a otras personas Servicios de AWS en su nombre. Lo hacen para administrar los recursos que se utilizan en cada clúster.

Detalles de los permisos

Esta política incluye los siguientes permisos que permiten a los nodos trabajadores de ROSA completar las siguientes tareas:

- `ec2`— Evalúe Región de AWS e Amazon EC2 instancie los detalles como parte de la gestión del ciclo de vida de los nodos de trabajadores del clúster ROSA.
- `ecr`- Evalúe y obtenga las imágenes de los repositorios de ECR gestionados por ROSA que sean necesarias para la instalación del clúster y la gestión del ciclo de vida de los nodos de trabajo.

Para ver el documento de política de JSON completo, consulte la Guía de referencia ROSAWorkerInstancePolicyde políticas AWS gestionadas.

AWS política gestionada: ROSASRESupport Política

Puede adjuntar `ROSASRESupportPolicy` a sus entidades de IAM.

Antes de crear un clúster ROSA con planos de control alojados, primero debe asociar esta política a una función de IAM. Esta política otorga los permisos necesarios a los ingenieros de confiabilidad de sitios de Red Hat (SREs) para que observen, diagnostiquen y brinden soporte directamente a AWS los recursos asociados a los ROSA clústeres, incluida la capacidad de cambiar el estado de los nodos del ROSA clúster.

Detalles de los permisos

Esta política incluye los siguientes permisos que permiten SREs a Red Hat completar las siguientes tareas:

- `cloudtrail`— Lea AWS CloudTrail los eventos y las rutas relevantes para el clúster.
- `cloudwatch`— Lea Amazon CloudWatch las métricas relevantes para el clúster.
- `ec2`— Lea, describa y revise Amazon EC2 los componentes relacionados con el estado del clúster, como los grupos de seguridad, las conexiones de los puntos finales de la VPC y el estado del volumen. Inicie, detenga, reinicie y finalice las Amazon EC2 instancias.
- `elasticloadbalancing`— Lea, describa y revise Elastic Load Balancing los parámetros relacionados con el estado del clúster.
- `iam`— Evaluar IAM las funciones relacionadas con la salud del clúster.
- `route53`: revisar la configuración del DNS relacionada con el estado del clúster.
- `sts`— `DecodeAuthorizationMessage` — Lee IAM los mensajes con fines de depuración.

Para ver el documento de política de JSON completo, consulte la ROSASRESupportPolítica en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: ROSAInstaller Política

Puede adjuntarla `ROSAInstallerPolicy` a sus IAM entidades.

Antes de crear un clúster ROSA con planos de control alojados, primero debe adjuntar esta política a un rol de IAM denominado`[Prefix]-ROSA-Worker-Role`. Esta política permite a las entidades añadir cualquier rol que siga el patrón de `[Prefix]-ROSA-Worker-Role` a un perfil de instancia. Esta política otorga al instalador los permisos necesarios para administrar AWS los recursos que admiten la instalación ROSA del clúster.

Detalles de los permisos

Esta política incluye los siguientes permisos que le permiten al instalador completar las siguientes tareas:

- `ec2`— Ejecute Amazon EC2 instancias AMIs alojadas en servidores Cuentas de AWS propiedad y gestionados por Red Hat. Describa Amazon EC2 las instancias, los volúmenes y los recursos de red asociados a Amazon EC2 los nodos. Este permiso es necesario para que el plano de control de Kubernetes pueda unir instancias a un clúster y el clúster pueda evaluar su presencia en él. Amazon VPC Inspeccione las reservas de capacidad de Amazon EC2 para que sean compatibles con la nueva función de reservas de capacidad de ROSA. Etiquete y elimine las etiquetas de las subredes mediante la combinación de claves de etiquetas. `"kubernetes.io/cluster/*"` Esto es necesario para garantizar que el balanceador de carga utilizado para la entrada de clústeres se cree solo en las subredes aplicables y para administrar las etiquetas de identificación de los clústeres de Kubernetes.
- `elasticloadbalancing`: agregar equilibradores de carga a los nodos de destino de un clúster. Eliminar los equilibradores de carga de los nodos de destino de un clúster. Este permiso es necesario para que el plano de control de Kubernetes pueda aprovisionar dinámicamente los balanceadores de carga solicitados por los servicios de Kubernetes y los servicios de aplicaciones. OpenShift
- `kms`— Lea una AWS KMS clave, cree y gestione las subvenciones y devuelva una clave de datos simétrica única para Amazon EC2 utilizarla fuera de ella. AWS KMS Esto es necesario para el uso de datos cifrados de `etcd` cuando el cifrado de `etcd` está activado en el momento de la creación del clúster.

- `iam`: validar los roles y las políticas de IAM. Aprovisione y gestione de forma dinámica los perfiles de Amazon EC2 instancia relevantes para el clúster. Añadir etiquetas a un perfil de instancia de IAM mediante el permiso de `iam:TagInstanceProfile`. Envíe mensajes de error al instalador cuando la instalación del clúster falle debido a la falta de un proveedor de OIDC de clúster especificado por el cliente.
- `route53`— Gestione Route 53 los recursos necesarios para crear clústeres.
- `servicequotas`: evaluar las service quotas necesarias para crear un clúster.
- `sts`— Crear AWS STS credenciales temporales para ROSA los componentes. Asumir las credenciales para la creación del clúster.
- `secretsmanager`: leer un valor secreto para permitir de forma segura la configuración de OIDC administrada por el cliente como parte del aprovisionamiento de clústeres.

Para ver el documento de política de JSON completo, consulte la ROSAInstallerPolítica en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: ROSAShared VPCRoute53 Política

Puede adjuntarla `ROSASharedVPCRoute53Policy` a sus IAM entidades. Debe adjuntar esta política a una función de IAM para permitir que un clúster ROSA realice llamadas a otros Servicios de AWS en entornos de VPC compartidos.

Esta política permite al instalador de ROSA configurar los registros de Route 53. Esta política está pensada para usarse en una VPC compartida y proporciona un subconjunto de permisos de Route 53 diseñados para los casos de uso de VPC compartidas.

Detalles de los permisos

Esta política incluye los siguientes permisos que permiten al instalador de ROSA completar las siguientes tareas:

- `route53`— Lea la información de la zona DNS y los registros DNS existentes para comprender la configuración DNS actual. Cree, modifique y elimine registros de DNS, pero solo para patrones de dominio específicos relacionados con ROSA`.hypershift.local`, como, `.openshiftapps.com` `.devshift.org.openshiftusgov.com`, y. `.devshiftusgov.com` Agregue, modifique o elimine etiquetas en los recursos de Route 53 para administrar y organizar los recursos.
- `tag`— Descubra y enumere AWS los recursos en función de sus etiquetas, lo que resulta útil para identificar los recursos administrados por ROSA.

Para ver más detalles sobre la política, incluida la última versión del documento de política de JSON, consulte la ROSASharedVPCRoute53Política en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: ROSAShared VPCEndpoint Política

Puede adjuntarla `ROSASharedVPCEndpointPolicy` a sus IAM entidades. Debe adjuntar esta política a una función de IAM para permitir que un clúster ROSA realice llamadas a otros Servicios de AWS en entornos de VPC compartidos.

Esta política permite al instalador de ROSA configurar puntos finales de VPC y grupos de seguridad en entornos de VPC compartidos.

Detalles de los permisos

Esta política incluye los siguientes permisos que permiten al instalador de ROSA completar las siguientes tareas:

- `ec2`— Permisos de solo lectura para describir los recursos relacionados con la VPC, incluidos los puntos finales de la VPC y los grupos de seguridad VPCs, a fin de comprender el entorno de la red. Cree, elimine y modifique grupos de seguridad con restricciones basadas en etiquetas, lo que permitirá a ROSA crear y administrar grupos de seguridad para redes de clústeres y, al mismo tiempo, restringir las operaciones únicamente a los recursos etiquetados por ROSA. Cree, modifique y elimine puntos de enlace de VPC con restricciones basadas en etiquetas, lo que permite a ROSA crear y administrar puntos de enlace de VPC para una conectividad privada en entornos de VPC compartidos. Servicios de AWS Aplique etiquetas a los puntos finales y grupos de seguridad de VPC recién creados durante la creación para una correcta identificación y administración de los recursos.

Para ver más detalles sobre la política, incluida la última versión del documento de política de JSON, consulte la ROSASharedVPCEndpointpolítica en la Guía de referencia de políticas AWS gestionadas.

ROSA con políticas de operadores de HCP

Esta sección proporciona detalles sobre las políticas de operador que se requieren para ROSA con aviones de control alojados (HCP). Puede adjuntar estas políticas AWS gestionadas a las funciones de operador necesarias para utilizar ROSA con el HCP. Los permisos son necesarios para que los OpenShift operadores puedan gestionar ROSA con nodos de clústeres de HCP.

> **Note**
>
> AWS Las políticas gestionadas están diseñadas para que ROSA las utilice con planes de control alojados (HCP). Los clústeres clásicos de ROSA utilizan políticas de IAM gestionadas por el cliente. Para obtener más información sobre las políticas clásicas de ROSA, consulte the section called “Políticas de cuentas ROSA classic” ythe section called “Pólizas de operador clásicas de ROSA”.

AWS política gestionada: ROSAAmazon EBSCSIDriver OperatorPolicy

Puede adjuntarla `ROSAAmazonEBSCSIDriverOperatorPolicy` a sus IAM entidades. Debe adjuntar esta política a la función de IAM de un operador para permitir que un ROSA con un clúster de aviones de control alojado pueda realizar llamadas a otros Servicios de AWS. Se requiere un conjunto único de roles de operador para cada clúster.

Esta política otorga los permisos necesarios al operador del Amazon EBS CSI para instalar y mantener el controlador Amazon EBS CSI en un clúster. ROSA Para obtener más información sobre el operador, consulte el aws-ebs-csi-driver operador en la OpenShift GitHub documentación.

Detalles de los permisos

Esta política incluye los siguientes permisos que permiten al Amazon EBS conductor y operador realizar las siguientes tareas:

- `ec2`— Crear, modificar, adjuntar, separar y eliminar Amazon EBS los volúmenes adjuntos a las Amazon EC2 instancias. Cree y elimine instantáneas de Amazon EBS volúmenes y enumere Amazon EC2 instancias, volúmenes e instantáneas.

Para ver el documento de política de JSON completo, consulte la Guía ROSAAmazonEBSCSIDriverOperatorPolicyde referencia de políticas AWS gestionadas.

AWS política gestionada: ROSAIngress OperatorPolicy

Puede adjuntarla `ROSAIngressOperatorPolicy` a sus IAM entidades. Debe adjuntar esta política a la función de IAM de un operador para permitir que un ROSA con un clúster de aviones de control alojado pueda realizar llamadas a otros Servicios de AWS. Se requiere un conjunto único de roles de operador para cada clúster.

Esta política otorga los permisos necesarios al operador de ingreso para aprovisionar y administrar los balanceadores de carga y las configuraciones de DNS para los clústeres. ROSA La política permite el acceso de lectura a los valores de las etiquetas. A continuación, el operador filtra los valores de las etiquetas de los Route 53 recursos para detectar las zonas alojadas. Para obtener más información sobre el operador, consulte OpenShift Ingress Operator en la OpenShift GitHub documentación.

Detalles de los permisos

Esta política incluye los siguientes permisos que le permiten al operador de entrada completar las siguientes tareas:

- `elasticloadbalancing`: describir el estado de los equilibradores de carga aprovisionados.
- `route53`— Enumere las zonas Route 53 alojadas y edite los registros que administran el DNS controlado por el clúster ROSA.
- `tag`: administrar los recursos etiquetados mediante el permiso de `tag:GetResources`.

Para ver el documento de política de JSON completo, consulte ROSAIngressOperatorPolicyla Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: ROSAImage RegistryOperatorPolicy

Puede adjuntarla `ROSAImageRegistryOperatorPolicy` a sus IAM entidades. Debe adjuntar esta política a la función de IAM de un operador para permitir que un ROSA con un clúster de aviones de control alojado pueda realizar llamadas a otros Servicios de AWS. Se requiere un conjunto único de roles de operador para cada clúster.

Esta política otorga los permisos necesarios al operador de registro de imágenes para aprovisionar y administrar los recursos del registro de imágenes ROSA integrado en el clúster y los servicios dependientes, incluido S3. Esto es necesario para que el operador pueda instalar y mantener el registro interno de un ROSA clúster. Para obtener más información sobre el operador, consulte Image Registry Operator en la OpenShift GitHub documentación.

Detalles de los permisos

Esta política incluye los siguientes permisos que le permiten al operador del registro de imágenes completar las siguientes acciones:

- `s3`— Administre y evalúe los Amazon S3 depósitos como almacenamiento persistente para el contenido de las imágenes del contenedor y los metadatos del clúster.

Para ver el documento de política de JSON completo, consulta ROSAImageRegistryOperatorPolicyla Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: ROSACloud NetworkConfigOperatorPolicy

Puede adjuntarla `ROSACloudNetworkConfigOperatorPolicy` a sus IAM entidades. Debe adjuntar esta política a la función de IAM de un operador para permitir que un ROSA con un clúster de aviones de control alojado pueda realizar llamadas a otros Servicios de AWS. Se requiere un conjunto único de roles de operador para cada clúster.

Esta política otorga los permisos necesarios al operador del controlador Cloud Network Config para aprovisionar y administrar los recursos de red para la superposición de redes del ROSA clúster. El operador usa estos permisos para administrar las direcciones IP privadas de las Amazon EC2 instancias que forman parte del ROSA clúster. Para obtener más información sobre el operador, consulta C loud-network-config-controller en la OpenShift GitHub documentación.

Detalles de los permisos

Esta política incluye los siguientes permisos que le permiten al operador del controlador de configuración de red en la nube completar las siguientes tareas:

- `ec2`— Lea, asigne y describa las configuraciones para conectar Amazon EC2 instancias, Amazon VPC subredes e interfaces de red elásticas en un ROSA clúster.

Para ver el documento de política de JSON completo, consulte ROSACloudNetworkConfigOperatorPolicyla Guía de referencia de políticas AWS administradas.

AWS política gestionada: ROSAKube ControllerPolicy

Puede adjuntarla `ROSAKubeControllerPolicy` a sus IAM entidades. Debe adjuntar esta política a la función de IAM de un operador para permitir que un ROSA con un clúster de aviones de control alojado pueda realizar llamadas a otros Servicios de AWS. Se requiere un conjunto único de roles de operador para cada clúster.

Esta política otorga al controlador kube los permisos necesarios para gestionar Amazon EC2 un clúster ROSA con planos de control alojados y AWS KMS los recursos necesarios para ello. Elastic Load Balancing Para obtener más información sobre este controlador, consulte la arquitectura del controlador en la OpenShift documentación.

Detalles de los permisos

Esta política incluye los siguientes permisos que le permiten al controlador de kube completar las siguientes tareas:

- `ec2`— Cree, elimine y añada etiquetas a los grupos de seguridad de Amazon EC2 instancias. Agregar reglas de entrada a los grupos de seguridad. Describa las zonas de disponibilidad, las Amazon EC2 instancias, las tablas de enrutamiento VPCs, los grupos de seguridad y las subredes.
- `elasticloadbalancing`— Cree y gestione los balanceadores de carga y sus políticas. Cree y gestione los dispositivos de escucha de los balanceadores de carga. Registra y anula el registro de los objetivos con los grupos objetivo y gestiona los grupos objetivo. Registra y anula el registro de Amazon EC2 las instancias con un balanceador de cargas y agrega etiquetas a los balanceadores de cargas.
- `kms`— Recupera información detallada sobre una clave. AWS KMS Esto es necesario para el uso de datos cifrados de `etcd` cuando el cifrado de `etcd` está activado en el momento de la creación del clúster.

Para ver el documento de política de JSON completo, consulte ROSAKubeControllerPolicyla Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: ROSANode PoolManagementPolicy

Puede adjuntarla `ROSANodePoolManagementPolicy` a sus IAM entidades. Debe asociar esta política a la función de IAM de un operador para permitir que un ROSA con un clúster de aviones de control alojado pueda realizar llamadas a otros AWS servicios. Se requiere un conjunto único de roles de operador para cada clúster.

Esta política otorga al NodePool controlador los permisos necesarios para describir, ejecutar y finalizar las Amazon EC2 instancias administradas como nodos de trabajo. Esta política también concede permisos para permitir el cifrado del disco del volumen raíz del nodo de trabajo mediante AWS KMS claves, etiquetar la interfaz de red elástica que está conectada al nodo de trabajo y acceder a Amazon EC2 Capacity Reservations. Para obtener más información sobre este controlador, consulte la arquitectura del controlador en la OpenShift documentación.

Detalles de los permisos

Esta política incluye los siguientes permisos que permiten al NodePool controlador realizar las siguientes tareas:

- `ec2`— Ejecute Amazon EC2 instancias AMIs alojadas en servidores Cuentas de AWS propiedad y gestionados por Red Hat. Gestione los ciclos de vida de EC2 en el clúster. ROSA Cree e integre

dinámicamente nodos de trabajo con Elastic Load Balancing, Amazon VPC Route 53, Amazon EBS y. Amazon EC2 Acceda a las reservas de capacidad y descríbalas para respaldar la función de reserva de capacidad de ROSA.

- `iam`— Úselo Elastic Load Balancing a través del rol vinculado al servicio denominado. `AWSServiceRoleForElasticLoadBalancing` Asigne funciones a los perfiles de Amazon EC2 instancia.
- `kms`— Lea una AWS KMS clave, cree y gestione las subvenciones y devuelva una clave de datos simétrica única para usarla fuera de AWS KMS ella. Amazon EC2 Esto es necesario para permitir el cifrado del disco del volumen raíz del nodo de trabajo.

Para ver el documento de política de JSON completo, consulte ROSANodePoolManagementPolicyla Guía de referencia sobre políticas AWS gestionadas.

AWS política gestionada: ROSAKMSProvider Política

Puede adjuntarla `ROSAKMSProviderPolicy` a sus IAM entidades. Debe adjuntar esta política a la función de IAM de un operador para permitir que un ROSA con un clúster de aviones de control alojado pueda realizar llamadas a otros Servicios de AWS. Se requiere un conjunto único de roles de operador para cada clúster.

Esta política otorga los permisos necesarios al proveedor de AWS cifrado integrado para administrar AWS KMS las claves que admiten el cifrado de `etcd` datos. Esta política permite Amazon EC2 utilizar las claves KMS que proporciona el proveedor de AWS cifrado para cifrar y descifrar `etcd` datos. Para obtener más información sobre este proveedor, consulte Proveedor de AWS cifrado en la documentación de GitHub Kubernetes.

Detalles de los permisos

Esta política incluye los siguientes permisos que permiten al proveedor de AWS cifrado realizar las siguientes tareas:

- `kms`— Cifrar, descifrar y recuperar una AWS KMS clave. Esto es necesario para el uso de datos cifrados de `etcd` cuando el cifrado de `etcd` está activado en el momento de la creación del clúster.

Para ver el documento de política de JSON completo, consulte la ROSAKMSProviderPolítica en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: ROSAControl PlaneOperatorPolicy

Puede adjuntarla `ROSAControlPlaneOperatorPolicy` a sus IAM entidades. Debe adjuntar esta política a la función de IAM de un operador para permitir que un ROSA con un clúster de aviones de control alojado pueda realizar llamadas a otros Servicios de AWS. Se requiere un conjunto único de roles de operador para cada clúster.

Esta política concede al operador del plano de control los permisos necesarios para gestionar los clústeres de planos de control alojados Amazon EC2 y Route 53 los recursos necesarios para ROSA. Para obtener más información sobre este operador, consulte la arquitectura del controlador en la OpenShift documentación.

Detalles de los permisos

Esta política incluye los siguientes permisos que le permiten al operador del plano de control completar las siguientes tareas:

- `ec2`— Cree y gestione Amazon VPC puntos finales.
- `route53`— Listar y cambiar los conjuntos de Route 53 registros y enumerar las zonas alojadas.
- Etiquetas añadidas a RedHatManagedSecurityGroups: Permite al operador del plano de control etiquetar los grupos de seguridad gestionados por Red Hat tras su creación. Esto es necesario para gestionar adecuadamente el ciclo de vida de los recursos y limpiar los grupos de seguridad asociados a ROSA con clústeres de HCP.
- Se agregó un grupo de seguridad* para administrar VPCEndpointWithCondition: corrige los errores de reconciliación del VPCE durante las actualizaciones de los clústeres. El operador necesita permiso para modificar los puntos finales de la VPC que hacen referencia a los grupos de seguridad.

Para ver el documento de política de JSON completo, consulte la Guía ROSAControlPlaneOperatorPolicyde referencia de políticas AWS gestionadas.

ROSA actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas ROSA desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de Historial de revisión.

Cambio	Descripción	Fecha
ROSAControlPlaneOperatorPolicy — Política actualizada	ROSA actualizó la política para permitir el etiquetado de los grupos de seguridad gestionados por Red Hat para una gestión adecuada del ciclo de vida de los recursos y para añadir Security-group/* a Manage para corregir los errores de reconciliación de VPCE durante las actualizaciones de VPCEndpoint WithCondition los clústeres. Para obtener más información, consulte the section called “AWS política gestionada: ROSAControl PlaneOperatorPolicy”.	9 de abril de 2026
ROSAKubeControllerPolicy — Política actualizada	ROSA actualizó la política para aclarar los permisos de Elastic Load Balancing para registrar y anular el registro de objetivos con los grupos objetivo. Para obtener más información, consulte the section called “AWS política gestionada: ROSAKubeControllerPolicy”.	5 de marzo de 2026
ROSANodePoolManagementPolicy — Política actualizada	ROSA actualizó la política para añadir acceso a los recursos para las reservas de capacidad de Amazon EC2. Este cambio permite al NodePool controlador	3 de septiembre de 2025

Cambio	Descripción	Fecha
	acceder a las reservas de capacidad y describirlas para mejorar la administración de los recursos. Para obtener más información, consulte the section called “AWS política gestionada: ROSANode PoolManagementPolicy”.	
ROSASharedVPCEndpointPolítica: se agregó una nueva política	ROSA agregó una nueva política que permite al ROSA instalador configurar puntos finales y grupos de seguridad de VPC en entornos de VPC compartidos. Esta política proporciona un subconjunto de permisos de EC2 diseñados para casos de uso de VPC compartidas. Para obtener más información, consulte the section called “AWS política gestionada: ROSAShared VPCEndpoint Política”.	7 de agosto de 2025

Cambio	Descripción	Fecha
ROSASharedVPCRoute 53Política: se agregó una nueva política	ROSA agregó una nueva política que permite al ROSA instalador configurar los registros de Route 53 en entornos de VPC compartid os. Esta política proporciona un subconjunto de permisos de Route 53 diseñados para casos de uso de VPC compartidas. Para obtener más información, consulte the section called “AWS política gestionada: ROSAShared VPCRoute53 Política”.	7 de agosto de 2025

Cambio	Descripción	Fecha
ROSAInstallerPolítica: política actualizada	ROSA actualizó la política para permitir al ROSA instalador inspeccionar las reservas de capacidad de Amazon EC2 para respaldar la nueva función de reservas de capacidad de ROSA. Esta actualización también permite al instalador eliminar etiquetas en las subredes mediante la coincidencia de claves de etiquetas `"kubernetes.io/cluster/*"` para mejorar la administración de etiquetas de clústeres de Kubernetes. Para obtener más información, consulte the section called “AWS política gestionada: ROSAInstaller Política”.	7 de agosto de 2025

Cambio	Descripción	Fecha
ROSAImageRegistryOperatorPolicy — Política actualizada	ROSA actualizó la política para que los permisos se limitaran al nivel de recursos del bucket S3. Este cambio cumple con los requisitos de almacenamiento de ROSA tanto para el sector AWS comercial como para las GovCloud regiones. Para obtener más información, consulte the section called “AWS política gestionada: ROSAImage RegistryOperatorPolicy”.	19 de mayo de 2025
ROSANodePoolManagementPolicy — Política actualizada	ROSA actualizó la política para permitir el etiquetado de la interfaz de red elástica que está conectada al nodo de trabajo. Para obtener más información, consulte the section called “AWS política gestionada: ROSANodePoolManagementPolicy”.	5 de mayo de 2025

Cambio	Descripción	Fecha
ROSAImageRegistryOperatorPolicy — Política actualizada	ROSA actualizó la política para permitir que el operador de registro de OpenShift imágenes de Red Hat aprovisione y administre buckets y objetos de Amazon S3 en AWS GovCloud las regiones para que los utilice el registro de imágenes integrado en el clúster de ROSA. Este cambio cumple con los requisitos de almacenamiento de ROSA para las regiones. AWS GovCloud Para obtener más información, consulte the section called “AWS política gestionada: ROSAImage RegistryOperatorPolicy”.	16 de abril de 2025
ROSAWorkerInstancePolicy — Política actualizada	ROSA actualizó la política para permitir a los nodos trabajadores evaluar y obtener imágenes de los repositorios de ECR gestionados por ROSA que son necesarias para la instalación de los clústeres y la gestión del ciclo de vida de los nodos trabajadores. Para obtener más información, consulte the section called “AWS política gestionada: ROSAWorker InstancePolicy”.	3 de marzo de 2025

Cambio	Descripción	Fecha
ROSANodePoolManagementPolicy — Política actualizada	ROSA actualizó la política para permitir que las interfaces de red elásticas se etiqueten de forma similar a las instancias de EC2 solo durante las RunInstances llamadas de ec2: cuando la solicitud incluye la etiqueta. `red-hat-managed: true` Estos permisos son necesarios para admitir ROSA con clústeres de HCP 4.17. Para obtener más información, consulte the section called “AWS política gestionada: ROSANodePoolManagementPolicy”.	24 de febrero de 2025
ROSAAmazonEBSCSIDriverOperatorPolicy — Política actualizada	ROSA actualizó la política para admitir la nueva API de autorización de Amazon EBS instantáneas. Para obtener más información, consulte the section called “AWS política gestionada: ROSAAmazon EBSCSIDriver OperatorPolicy”.	17 de enero de 2025

Cambio	Descripción	Fecha
ROSANodePoolManagementPolicy — Política actualizada	ROSA actualizó la política para permitir al administrador del grupo de ROSA nodos describir los conjuntos de opciones de DHCP a fin de establecer los nombres de DNS privados adecuados. Para obtener más información, consulte the section called “AWS política gestionada: ROSANode PoolManagementPolicy”.	2 de mayo de 2024
ROSAInstallerPolítica: política actualizada	ROSA actualizó la política para permitir al ROSA instalador añadir etiquetas a las subredes mediante la coincidencia `"kubernetes.io/cluster/*"` de claves de etiquetas. Para obtener más información, consulte the section called “AWS política gestionada: ROSAInstaller Política”.	24 de abril de 2024
ROSASRESupportPolítica: política actualizada	ROSA actualizó la política para permitir que la función de SRE recupere información sobre los perfiles de instancia etiquetados ROSA como `red-hat-managed` . Para obtener más información, consulte the section called “AWS política gestionada: ROSASRESupport Política”.	10 de abril de 2024

Cambio	Descripción	Fecha
ROSAInstallerPolítica: política actualizada	ROSA actualizó la política para permitir al ROSA instalador validar que las políticas AWS administradas ROSA estén asociadas a las IAM funciones utilizadas por ROSA. Esta actualización también permite al instalado r identificar si las políticas gestionadas por el cliente se han asociado a las ROSA funciones. Para obtener más información, consulte the section called “AWS política gestionada: ROSAInstaller Política”.	10 de abril de 2024

Cambio	Descripción	Fecha
ROSAInstallerPolítica: política actualizada	ROSA actualizó la política para permitir que el servicio envíe mensajes de alerta al instalador cuando la instalaci ón del clúster falte debido a la falta de un proveedor de OIDC de clústeres especificado por el cliente. Esta actualización también permite al servicio recuperar los servidores de nombres DNS existentes para que las operaciones de aprovisionamiento de clústeres sean idempotentes. Para obtener más informaci ón, consulte the section called “AWS política gestionada: ROSAInstaller Política”.	26 de enero de 2024
ROSASRESupportPolítica: política actualizada	ROSA se actualizó la política para permitir que el servicio realice operaciones de lectura en grupos de seguridad mediante la DescribeS ecurityGroups API. Para obtener más información, consulte the section called “AWS política gestionada: ROSASRESupport Política”.	22 de enero de 2024

Cambio	Descripción	Fecha
ROSAImageRegistryOperatorPolicy — Política actualizada	ROSA se actualizó la política para permitir al operador de registro de imágenes tomar medidas en los Amazon S3 depósitos de regiones con nombres de 14 caracteres. Para obtener más información, consulte the section called “AWS política gestionada: ROSAImage RegistryOperatorPolicy”.	12 de diciembre de 2023
ROSAKubeControllerPolicy — Política actualizada	ROSA actualizó la política para poder describir las kube-controller-manager zonas de disponibilidad, las Amazon EC2 instancias, las tablas de enrutamiento VPCs, los grupos de seguridad y las subredes. Para obtener más información, consulte the section called “AWS política gestionada: ROSAKube ControllerPolicy”.	16 de octubre de 2023
ROSAManageSuscripción: política actualizada	ROSA actualizó la política para añadir el ROSA a los aviones de control alojados ProductId. Para obtener más información, consulte the section called “AWS política gestionada: ROSAManage suscripción”.	1 de agosto de 2023

Cambio	Descripción	Fecha
ROSAKubeControllerPolicy — Política actualizada	ROSA se actualizó la política para permitir la kube-controller-manager creación de balanceadores de carga de red como balanceadores de carga de servicios de Kubernetes. Los equilibradores de carga de red ofrecen una mayor capacidad para administrar cargas de trabajo volátiles y admiten direcciones IP estáticas para el equilibrador de carga. Para obtener más información, consulte the section called “AWS política gestionada: ROSAKubeControllerPolicy”.	13 de julio de 2023
ROSANodePoolManagementPolicy — Se agregó una nueva política	ROSA se agregó una nueva política que permite al NodePool controlador describir, ejecutar y terminar Amazon EC2 las instancias administradas como nodos de trabajo. Esta política también permite cifrar el disco del volumen raíz del nodo de trabajo mediante AWS KMS claves. Para obtener más información, consulte the section called “AWS política gestionada: ROSANodePoolManagementPolicy”.	8 de junio de 2023

Cambio	Descripción	Fecha
ROSAInstallerPolítica: se agregó una nueva política	ROSA se agregó una nueva política que permite al instalador administrar AWS los recursos que admiten la instalación del clúster. Para obtener más información, consulte the section called “AWS política gestionada: ROSAInstaller Política”.	6 de junio de 2023
ROSASRESupportPolítica: se agregó una nueva política	ROSA agregó una nueva política que permite a Red Hat observar, diagnosticar y respaldar directamente AWS los recursos asociados SREs a los ROSA clústeres, incluida la capacidad de cambiar el estado de los nodos del ROSA clúster. Para obtener más información, consulte the section called “AWS política gestionada: ROSASRESupport Política”.	1 de junio de 2023
ROSAKMSProviderPolítica: se agregó una nueva política	ROSA se agregó una nueva política que permite al proveedor de AWS cifrado integrado administrar AWS KMS las claves para admitir el cifrado de datos etc/d. Para obtener más información, consulte the section called “AWS política gestionada: ROSAKMSProvider Política”.	27 de abril de 2023

Cambio	Descripción	Fecha
ROSAKubeControllerPolicy — Se ha añadido una nueva política	ROSA se agregó una nueva política para permitir que el controlador Kube administre y Amazon EC2 utilice Elastic Load Balancing AWS KMS recursos para los clústeres ROSA de planos de control alojados. Para obtener más información, consulte the section called “AWS política gestionada: ROSAKube ControllerPolicy”.	27 de abril de 2023
ROSAImageRegistryO peratorPolicy — Se agregó una nueva política	ROSA se agregó una nueva política que permite al operador de registro de imágenes aprovisionar y administrar recursos para el registro ROSA de imágenes del clúster y los servicios dependientes, incluido S3. Para obtener más informaci ón, consulte the section called “AWS política gestionad a: ROSAImage RegistryO peratorPolicy”.	27 de abril de 2023

Cambio	Descripción	Fecha
ROSAControlPlaneOperatorPolicy — Se agregó una nueva política	ROSA se agregó una nueva política que permite al operador del plano de control administrar los clústeres de planos de control alojados Amazon EC2 y los Route 53 recursos necesarios para ROSA ellos. Para obtener más información, consulte the section called “AWS política gestionada: ROSAControlPlaneOperatorPolicy”.	24 de abril de 2023
ROSACloudNetworkConfigOperatorPolicy — Se agregó una nueva política	ROSA agregó una nueva política que permite al operador del controlador de configuración de red en la nube aprovisionar y administrar los recursos de red para la superposición de redes del ROSA clúster. Para obtener más información, consulte the section called “AWS política gestionada: ROSACloudNetworkConfigOperatorPolicy”.	20 de abril de 2023

Cambio	Descripción	Fecha
ROSAIngressOperatorPolicy — Se agregó una nueva política	ROSA se agregó una nueva política que permite al operador de ingreso aprovisionar y administrar los balanceadores de carga y las configuraciones de DNS para ROSA los clústeres. Para obtener más informaci ón, consulte the section called “AWS política gestionada: ROSAIngress OperatorPolicy”.	20 de abril de 2023
ROSAAmazonEBSCSIDr iverOperatorPolicy — Se agregó una nueva política	ROSA se agregó una nueva política que permite al operador del controlador Amazon EBS CSI instalar y mantener el controlador Amazon EBS CSI en un ROSA clúster. Para obtener más información, consulte the section called “AWS política gestionada: ROSAAmazo n EBSCSIDriver OperatorP olicy”.	20 de abril de 2023
ROSAWorkerInstancePolicy — Se agregó una nueva política	ROSA se agregó una nueva política para permitir que el servicio administre los recursos del clúster. Para obtener más información, consulte the section called “AWS política gestionada: ROSAWorker InstancePolicy”.	20 de abril de 2023

Cambio	Descripción	Fecha
ROSAManageSuscripción: se agregó una nueva política	ROSA se agregó una nueva política para conceder los AWS Marketplace permisos necesarios para administrar la ROSA suscripción. Para obtener más información, consulte the section called “AWS política gestionada: ROSAManage suscripción”.	11 de abril de 2022
Red Hat OpenShift Service en AWS comenzó a rastrear los cambios	Red Hat OpenShift Service en AWS comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	2 de marzo de 2022

Solución de problemas ROSA de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con ROSA y IAM.

AWS Organizations la política de control de servicios deniega AWS Marketplace los permisos necesarios

Si tu política de control de AWS Organizations servicios (SCP) no permite los permisos de AWS Marketplace suscripción necesarios cuando intentas habilitarlos ROSA, se produce el siguiente error de consola.

```
An error occurred while enabling ROSA, because a service control policy (SCP) is
 denying required permissions. Contact your management account administrator, and
 consult the documentation for troubleshooting.
```

Si recibe este error, debe ponerse en contacto con el administrador para obtener ayuda. Su administrador es la persona que administra las cuentas de su organización. Pídale a esa persona que haga lo siguiente:

1. Configure el SCP para permitir `aws-marketplace:Subscribe` `aws-marketplace:Unsubscribe` y `aws-marketplace:ViewSubscriptions` permisos. Para obtener más información, consulte Actualización de un SCP en la Guía del AWS Organizations usuario.
2. ROSA Actívela en la cuenta de administración de la organización.
3. Comparta la ROSA suscripción a las cuentas de los miembros que requieren acceso dentro de la organización. Para obtener más información, consulta Cómo compartir las suscripciones en una organización en la Guía del AWS Marketplace comprador.

El usuario o el rol no tienen los AWS Marketplace permisos necesarios

Si tu IAM titular no tiene los permisos de AWS Marketplace suscripción necesarios cuando intentas habilitarlos ROSA, se produce el siguiente error de consola.

```
An error occurred while enabling ROSA, because your user or role does not have the
 required permissions.
```

Para resolver este problema, siga estos pasos:

1. Ve a la IAM consola y adjunta la política AWS gestionada `ROSAManageSubscription` a tu identidad de IAM. Para obtener más información, consulte la sección ROSAManageSuscripción en la Guía de referencia de políticas AWS gestionadas.
2. Siga el procedimiento indicado en the section called “Habilite ROSA y configure los AWS requisitos previos”.

Si no tiene permiso para ver o actualizar su conjunto de permisos IAM o recibe un error, debe ponerse en contacto con su administrador para obtener ayuda. Pídele a esa persona que adjunte `ROSAManageSubscription` tu IAM identidad y sigue el procedimiento indicado enthe section called “Habilite ROSA y configure los AWS requisitos previos”. Cuando un administrador realiza esta acción, la activa ROSA actualizando el conjunto de permisos para todas IAM las identidades incluidas en Cuenta de AWS.

AWS Marketplace Los permisos necesarios están bloqueados por un administrador

Si el administrador de su cuenta bloqueó los permisos de AWS Marketplace suscripción necesarios, se producirá el siguiente error de consola al intentar habilitarlos ROSA.

```
An error occurred while enabling ROSA because required permissions have been blocked by
 an administrator. ROSAManageSubscription includes the permissions required to enable
 ROSA. Consult the documentation and try again.
```

Si recibe este error, debe ponerse en contacto con el administrador para obtener ayuda. Pídale a esa persona que haga lo siguiente:

1. Ve a la ROSA consola y adjunta la política AWS gestionada `ROSAManageSubscription` a tu identidad de IAM. Para obtener más información, consulte la sección ROSAManageSuscripción en la Guía de referencia de políticas AWS gestionadas.
2. Siga el procedimiento indicado the section called “Habilite ROSA y configure los AWS requisitos previos” para activarla ROSA. Este procedimiento se habilita ROSA mediante la actualización del conjunto de permisos para todas IAM las identidades incluidas en Cuenta de AWS.

Error al crear el balanceador de cargas: AccessDenied

Si no has creado un balanceador de cargas, es posible que el rol `AWSServiceRoleForElasticLoadBalacing` vinculado al servicio no exista en tu cuenta. Si intentas crear un rol ROSA clúster sin el `AWSServiceRoleForElasticLoadBalacing` rol en tu cuenta, se produce el siguiente error.

```
Error creating network Load Balancer: AccessDenied
```

Para resolver este problema, siga estos pasos:

1. Compruebe si su cuenta tiene el rol de `AWSServiceRoleForElasticLoadBalancing`.

   ```
   aws iam get-role --role-name "AWSServiceRoleForElasticLoadBalancing"
   ```

2. Si no tiene este rol, siga las instrucciones para crearlo que se encuentran en Crear el rol vinculado al servicio en la Guía del Elastic Load Balancing usuario.

Resiliencia en ROSA

AWS resiliencia de la infraestructura global

La infraestructura AWS global se basa en unas Regiones de AWS zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que se conectan a través de 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.

ROSA ofrece a los clientes la opción de ejecutar el plano de control y el plano de datos de Kubernetes en una única zona de disponibilidad o en varias zonas de AWS disponibilidad. Si bien los clústeres Single-AZ pueden ser útiles para la experimentación, se recomienda a los clientes que ejecuten sus cargas de trabajo en más de una zona de disponibilidad. Esto garantiza que las aplicaciones puedan soportar incluso una falla total en la zona de disponibilidad, lo que en sí mismo es muy poco frecuente.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global AWS .

ROSA resiliencia de clústeres

El plano de ROSA control consta de al menos tres nodos OpenShift del plano de control. Cada nodo del plano de control está compuesto por una instancia de servidor de la API, una instancia de `etcd` y controladores. En caso de que se produzca un error en un nodo del plano de control, todas las solicitudes de la API se redirigen automáticamente a los demás nodos disponibles para garantizar la disponibilidad del clúster.

El plano de ROSA datos consta de al menos dos nodos de OpenShift infraestructura y dos OpenShift nodos de trabajo. Los nodos de infraestructura ejecutan módulos que admiten los componentes de la infraestructura del OpenShift clúster, como el enrutador predeterminado, el OpenShift registro integrado y los componentes para las métricas y la supervisión del clúster. OpenShift los nodos de trabajo ejecutan pods de aplicaciones para usuarios finales.

Los ingenieros de confiabilidad de sitios de Red Hat (SREs) administran completamente el plano de control y los nodos de infraestructura. Red Hat supervisa el ROSA clúster de SREs forma proactiva

y es responsable de reemplazar los nodos del plano de control y los nodos de infraestructura que fallen. Para obtener más información, consulte the section called “Responsabilidades”.

> **Important**
>
> Dado que ROSA se trata de un servicio gestionado, Red Hat es responsable de gestionar la AWS infraestructura subyacente que ROSA utiliza. Los clientes no deben intentar cerrar manualmente las Amazon EC2 instancias que ROSA utilizan desde la AWS consola o AWS CLI. Esta acción puede provocar que se pierdan datos de los clientes.

Si un nodo de trabajo falla en el plano de datos, el plano de control reubica los pods no programados en los nodos de trabajo en funcionamiento hasta que se recupere o sustituya el nodo defectuoso. Los nodos de trabajo defectuosos se pueden reemplazar de forma manual o automática si se permite el escalado automático de las máquinas de un clúster. Para obtener más información, consulte Escalado automático de clústeres en la documentación de Red Hat.

Resiliencia de las aplicaciones implementadas por el cliente

Si bien ROSA ofrece muchas protecciones para garantizar una alta disponibilidad del servicio, los clientes son responsables de crear las aplicaciones implementadas para garantizar una alta disponibilidad a fin de proteger las cargas de trabajo contra el tiempo de inactividad. Para obtener más información, consulte Información sobre disponibilidad de ROSA en la documentación de Red Hat.

La seguridad de la infraestructura en ROSA

Como servicio gestionado, Red Hat OpenShift Service en AWS 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 la infraestructura en el pilar de la seguridad: AWS Well-Architected Framework.

Utiliza las llamadas a la API AWS publicadas para acceder a ROSA través de la AWS 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.

Aislamiento de redes de clúster

Los ingenieros de confiabilidad de sitios de Red Hat (SREs) son responsables de la administración continua y la seguridad de la red del clúster y la plataforma de aplicaciones subyacente. Para obtener más información sobre las responsabilidades de Red Hat ROSA, consultethe section called “Responsabilidades”.

Al crear un clúster nuevo, ROSA ofrece la opción de crear rutas de aplicaciones y puntos de enlace de servidor API de Kubernetes públicos o rutas de aplicaciones y puntos de enlace de API de Kubernetes privados. Esta conexión se utiliza para comunicarse con el clúster (mediante herramientas OpenShift de administración como ROSA CLI y OpenShift CLI). Una conexión privada permite que toda la comunicación entre los nodos y el servidor de la API permanezcan dentro de su VPC. Si habilita el acceso privado al servidor de API y a las rutas de la aplicación, debe usar una VPC existente y conectar la VPC AWS PrivateLink al servicio de backend. OpenShift

El acceso al servidor API de Kubernetes está protegido mediante una combinación de AWS Identity and Access Management (IAM) y un control de acceso basado en roles (RBAC) nativo de Kubernetes. Para obtener más información sobre el RBAC de Kubernetes, consulte Utilización de la autorización del RBAC en la documentación de Kubernetes.

ROSA permite crear rutas de aplicaciones seguras mediante varios tipos de terminación de TLS para entregar los certificados al cliente. Para obtener más información, consulte Rutas seguras en la documentación de Red Hat.

Si crea un ROSA clúster en una VPC existente, debe especificar las subredes de la VPC y las zonas de disponibilidad que utilizará el clúster. También debe definir los rangos de CIDR que debe utilizar la red del clúster y hacer coincidir estos rangos de CIDR con las subredes de la VPC. Para obtener más información, consulte Definiciones de rango de CIDR en la documentación de Red Hat.

En el caso de los clústeres que utilizan el punto de enlace de la API pública, es ROSA necesario que la VPC esté configurada con una subred pública y privada para cada zona de disponibilidad en la que desee implementar el clúster. En el caso de los clústeres que utilizan el punto de conexión de la API privada, solo se requieren subredes privadas.

Si utiliza una VPC existente, puede configurar los ROSA clústeres para que utilicen un servidor proxy HTTP o HTTPS durante o después de la creación del clúster para cifrar el tráfico web del clúster y añadir otra capa de seguridad a sus datos. Al habilitar un proxy, a los componentes principales del clúster se les niega el acceso directo a Internet. El proxy no deniega el acceso a Internet a las cargas de trabajo de los usuarios. Para obtener más información, consulte Configuración del proxy en todo el clúster en la documentación de Red Hat.

Aislamiento de la red de pods

Si es administrador de clústeres, puede definir políticas de red a nivel de pod que restrinjan el tráfico a los pods de su ROSA clúster.

ROSA cuotas de servicio

Red Hat OpenShift Service en AWS (ROSA) usa cuotas de servicio para Amazon EC2 Amazon Virtual Private Cloud Amazon Elastic Block Store, y para Elastic Load Balancing aprovisionar los clústeres. Para obtener más información, consulte los Red Hat OpenShift Service en AWS puntos finales y las cuotas en la Guía de referencia AWS general.

AWS servicios integrados con ROSA

ROSA trabaja con otros Servicios de AWS para ofrecer soluciones adicionales a los desafíos de su empresa. En este tema se identifican los servicios que ROSA se utilizan para añadir funcionalidad o los que se ROSA utilizan para realizar tareas.

Temas

Cómo ROSA funciona con AWS Marketplace

AWS Marketplace es un catálogo digital seleccionado que puede utilizar para buscar, comprar, implementar y administrar el software, los datos y los servicios de terceros que necesita para crear soluciones y administrar su empresa. AWS Marketplace simplifica las licencias y la adquisición de software con opciones de precios flexibles y varios métodos de implementación.

ROSA se utiliza AWS Marketplace para la medición y facturación de servicios. ROSA classic se mide y factura a través de un producto basado en AWS Marketplace Amazon Machine Image (AMI), mientras que ROSA con planos de control alojados (HCP) se mide y factura a través de un producto basado en AWS Marketplace software como servicio (SaaS).

En esta página se explica cómo ROSA funciona con los pagos, la facturación, las suscripciones y las compras AWS Marketplace por contrato.

Terminología

En esta página se utilizan los siguientes términos al analizar la integración de ROSA con AWS Marketplace.

Imagen de máquina de Amazon (AMI)

> Una imagen de un servidor, que incluye un sistema operativo y software adicional, que se ejecuta en AWS.

Suscripciones de AMI

> En AWS Marketplace, los productos de software basados en AMI, como ROSA classic, utilizan un modelo de precios por hora con suscripción anual. El precio por hora es el modelo de precios

predeterminado, pero tienes la opción de comprar por adelantado el equivalente a un año de uso para un tipo de Amazon EC2 instancia.

Suscripción a SaaS

En AWS Marketplace, los productos software-as-a-service (SaaS) como ROSA con HCP adoptan un modelo de suscripción basado en el uso. El vendedor de software realiza un seguimiento de su uso y usted solo paga por lo que usa.

Oferta pública

Las ofertas públicas le permiten comprar AWS Marketplace software y servicios directamente desde. Consola de administración de AWS

Oferta privada

Las ofertas privadas son un programa de compra que permite a los vendedores y compradores negociar precios personalizados y las condiciones del acuerdo de licencia de usuario final (EULA) para realizar compras. AWS Marketplace

Tarifas de servicio de ROSA

Tarifas que ROSA cobran los ingenieros de confiabilidad de sitios de Red Hat por la administración de OpenShift software y clústeres (SREs). ROSA las tarifas de servicio se calculan AWS Marketplace íntegramente y aparecen en su AWS factura.

Tarifas de infraestructura de AWS

Las tarifas estándar que se AWS cobran por los ROSA clústeres Servicios de AWS subyacentes, incluidas Amazon EC2, Amazon EBS Amazon S3, y Elastic Load Balancing. Las tarifas se calculan en función del Servicio de AWS uso y aparecen en tu AWS factura.

ROSA pagos y facturación

ROSA se integra AWS Marketplace para permitir la medición y facturación de las tarifas de ROSA servicio. ROSA las tarifas de servicio cubren el acceso a la administración de OpenShift software y clústeres por parte de los ingenieros de confiabilidad de sitios de Red Hat (SREs). ROSA las tarifas de servicio son uniformes en todas las regiones AWS estándar compatibles. De forma predeterminada, las tarifas de ROSA con los servicios de HCP se acumulan según la demanda, a una tarifa fija por hora que se basa en la cantidad de clústeres en ejecución y en función del número de nodos de trabajo que estén CPUs funcionando en esos clústeres. Las tarifas de servicio de ROSA Classic se acumulan en función de la demanda y se basan en el número de trabajadores del

nodo v. CPUs ROSA classic no cobra tarifas de servicio por el plano de control ni por los nodos de infraestructura necesarios.

ROSA los clientes también pagan tarifas de AWS infraestructura estándar por los ROSA clústeres Servicios de AWS subyacentes Amazon EC2, que incluyen Amazon EBS Amazon S3, y Elastic Load Balancing. AWS las tarifas de infraestructura son un elemento de facturación independiente de las tarifas de ROSA servicio que se calculan. AWS Marketplace AWS De forma predeterminada, las tarifas de infraestructura varían Región de AWS y se basan en el uso por hora. Para ahorrar costes de AWS infraestructura adicionales, puede adquirir planes de Amazon EC2 ahorro o instancias reservadas. Para obtener más información, consulte Compute Savings Plans and Reserved Instances en la Guía del Amazon EC2 usuario.

ROSA no cobra comisiones hasta que cree un ROSA clúster o adquiera un ROSA contrato. Para obtener más información, consulte Precios de Red Hat OpenShift Service en AWS.

Puede ver las tarifas ROSA de servicio y las tarifas de AWS infraestructura y administrar los pagos en la AWS Billing consola. También puede ver sus costos y monitorear el uso mediante la AWS Cost Explorer Service interfaz de forma gratuita. Para obtener más información, consulte Visualización de la factura en la Guía del Administración de facturación y costos de AWS usuario y Análisis de los costes AWS Cost Explorer Service en la Guía del usuario de gestión de AWS costes.

Suscribirse a los listados de ROSA Marketplace a través de la consola

Si lo activas ROSA en la ROSA consola, te Cuenta de AWS suscribes a los listados ROSA classic y ROSA with HCP. AWS Marketplace La activación ROSA de las suscripciones es gratuita.

Para AWS Organizations los usuarios, ROSA permite compartir las suscripciones clásicas de ROSA con otras cuentas de su organización. Para obtener más información, consulte Compartir suscripciones en una organización en la Guía del AWS Marketplace comprador.

Comprar un ROSA contrato

ROSA suele AWS Marketplace ofrecer contratos opcionales para ROSA con HCP y ROSA classic. Los contratos permiten ahorrar en las tarifas de servicio del nodo ROSA obrero. ROSA los contratos no afectan a las tarifas cobradas por la AWS infraestructura.

Contratos de 12 meses

Puedes comprar contratos de oferta pública de 12 meses para ROSA classic y ROSA con HCP desde la ROSA consola.

> **Note**
>
> ROSA clásico debe estar habilitado en su cuenta antes de poder adquirir contratos de 12 meses desde la consola.

> **Note**
>
> Los contratos de 12 meses no se pueden transferir a una oferta privada.

Adquisición de un contrato de 12 meses de ROSA clásico

Al adquirir un contrato de 12 meses de ROSA clásico, usted efectúa un pago por adelantado por un plazo anual y no paga ninguna cuota de servicio por hora durante los 12 meses siguientes por las instancias cubiertas. El costo del contrato se basa en el tipo de Amazon EC2 instancia y la cantidad de instancias que seleccione. El contrato no cubre las tarifas de AWS infraestructura que se ROSA cobran por la infraestructura subyacente Servicios de AWS que se utiliza. Para obtener más información, consulte Red Hat OpenShift Service en AWS Precios.

El contrato solo cubre los tipos de instancia que especifique durante la creación del contrato (p. ej., m5.xlarge). Puede adquirir contratos adicionales de 12 meses para ahorrar costes en más de un tipo de Amazon EC2 instancia. El uso fuera de su contrato de 12 meses implica tarifas de ROSA servicio a la tarifa bajo demanda.

> **Note**
>
> Los contratos ROSA clásicos de 12 meses no se renuevan automáticamente.

Para adquirir un contrato de 12 meses de ROSA clásico

> **Note**
>
> Si utiliza la ROSA consola en una región que aún no admite ROSA con HCP, este flujo de trabajo aún no está disponible. Para obtener una lista de las regiones que admiten ROSA con HCP, consulte. the section called “Comparación de ROSA con HCP y ROSA classic”

Para adquirir contratos ROSA clásicos en regiones sin ROSA con soporte HCP, vaya a la consola de ROSA y seleccione Adquirir un contrato de software y ver los contratos existentes.

1. Vaya a la consola de ROSA.
2. En el panel de navegación izquierdo, seleccione Contratos.
3. Elija Contratos para ROSA clásico.
4. Elija Adquirir contrato.
5. Seleccione el tipo de EC2 instancia y la cantidad de instancias que necesita.
6. Elija Revisar contrato.
7. Revise los detalles del contrato y elija Adquirir contrato.

Note

ROSA Los contratos de 12 meses no se pueden rebajar de categoría ni cancelar una vez creados mediante la consola. Si necesita bajar de categoría o cancelar el contrato durante la duración del contrato activo, vaya a Centro de Soporte y abra un caso de soporte.

Adquisición de un contrato de 12 meses de ROSA con HCP

Al activar ROSA con HCP en la consola, se crea inicialmente en su cuenta un contrato gratuito de ROSA con HCP de 12 meses para facilitar la facturación bajo demanda. Si opta por adquirir un contrato ROSA con HCP para ahorrar en las tarifas de servicio del nodo trabajador, el contrato inicial se modifica para cubrir los costos de uso del nodo trabajador v CPUs y los planos de control que especifique.

Cuando adquiere un contrato de 12 meses con ROSA con HCP, realiza un pago por adelantado durante un período anual y no paga ninguna cuota de uso por hora durante los próximos 12 meses para los aviones Worker Node V CPUs y control cubiertos. El coste del contrato se basa en la cantidad de trabajadores del nodo v CPUs y de los planos de control que seleccione. El contrato cubre únicamente el nodo trabajador v CPUs y los planos de control que especifique durante la creación del contrato. El contrato no cubre las tarifas de AWS infraestructura que se ROSA cobran por el subyacente Servicios de AWS que se utiliza. Para obtener más información, consulte Red Hat OpenShift Service en AWS Precios.

Cuota de uso mensual

Tras la compra, sus aviones v CPUs y de control de prepago se convierten en una cuota de uso mensual. Se aplican tarifas de uso bajo demanda por hora para el uso de vCPU y plano de control que supere la cuota mensual. ROSA con HCP utiliza las siguientes fórmulas para calcular la cuota mensual asociada al contrato:

- Nodo de trabajo vCPUs: número de v CPUs x 24 horas x 365 días/12 meses
- Planos de control: número de planos de control x 24 horas x 365 días/12 meses

Por ejemplo, la compra de 4 000 aviones de control del nodo V CPUs y 8 de control se convertiría en una cuota mensual de 2 920 000 horas de vCPU en el nodo de trabajo y 5 840 horas consumibles en el plano de control al mes.

Para adquirir un contrato de 12 meses de ROSA con HCP

> **Note**
>
> Si utiliza la Red Hat OpenShift Service en AWS consola en una región que aún no admite ROSA con planos de control alojados, este flujo de trabajo aún no está disponible. Para obtener una lista de las regiones que admiten ROSA con HCP, consultethe section called "Comparación de ROSA con HCP y ROSA classic".

1. Vaya a la consola de ROSA.
2. En el panel de navegación izquierdo, seleccione Contratos.
3. Elija Contratos para ROSA con HCP.
4. Elija Adquirir contrato.
5. Introduzca el número de v CPUs que desea comprar. Especifique en múltiplos de 4.
6. Ingrese el número de planos de control que desea adquirir.
7. Elija Revisar contrato.
8. Revise los detalles del contrato y elija Adquirir contrato.

> **Note**
>
> ROSA Los contratos de 12 meses no se pueden rebajar de categoría ni cancelar una vez creados mediante la consola. Si necesita bajar de categoría o cancelar el contrato durante la duración del contrato activo, vaya a Centro de Soporte y abra un caso de soporte.

Actualización de un contrato de 12 meses de ROSA con HCP

Puede actualizar su contrato de 12 meses de ROSA activo con HCP en cualquier momento con más trabajadores en el nodo v y en planos de control. CPUs Al actualizar su contrato de 12 meses de ROSA con HCP, realiza un pago prorrateado por adelantado por los recursos que se agregan. Los importes prorrateados se calculan en función del número de días restantes del contrato. El contrato cubre únicamente el nodo de trabajo v CPUs y los planos de control que especifique durante la creación del contrato. Las actualizaciones de los contratos no afectan a las tarifas cobradas por AWS la infraestructura.

Tras la actualización, los aviones v CPUs y de control añadidos se convierten en una cuota de uso mensual utilizando las mismas fórmulas utilizadas en el contrato original. Se aplican tarifas de uso bajo demanda por hora para el uso de vCPU y plano de control que supere la cuota mensual. Para obtener más información, consulte the section called “Cuota de uso mensual”.

Para actualizar un contrato de 12 meses de ROSA con HCP

1. Vaya a la consola de ROSA.
2. En el panel de navegación izquierdo, seleccione Contratos.
3. Elija Contratos para ROSA con HCP.
4. Seleccione Actualizar.
5. Introduzca el número de v CPUs que desee sumar. Especifique en múltiplos de 4.
6. Ingrese el número de planos de control que desea agregar al contrato.
7. Elija Revisar actualización.
8. Revise los detalles del contrato y elija Adquirir actualización.

> **Note**
>
> Los contratos de 12 meses de ROSA clásico no se pueden actualizar. Se pueden comprar contratos adicionales de ROSA Classic de 12 meses en cualquier momento a través de la ROSA consola.

Obtención de una oferta privada

Puede solicitar una oferta AWS Marketplace privada de ROSA con HCP o ROSA classic para recibir el precio del producto y las condiciones del acuerdo de licencia para el usuario final (EULA) negociadas con Red Hat. Para obtener más información, consulte las ofertas privadas en la Guía del AWS Marketplace comprador.

Para obtener una oferta ROSA privada

> **Note**
>
> Si es un AWS Organizations usuario y ha recibido una oferta privada para sus cuentas de pagador y de miembro, siga el procedimiento que se indica a continuación para suscribirse ROSA directamente en cada cuenta de su organización.
> Si recibe una oferta privada clásica de ROSA que solo se emitió para la cuenta del AWS Organizations pagador, tendrá que compartir la suscripción con las cuentas de los miembros de su organización. Para obtener más información, consulte Compartir suscripciones en una organización en la Guía del AWS Marketplace comprador.

1. Una vez enviada la oferta privada, conéctese a la consola de AWS Marketplace.
2. Abre el correo electrónico con un enlace a una oferta ROSA privada.
3. Siga el enlace para acceder directamente a la oferta privada.

   > **Note**
   >
   > Si sigue este enlace antes de iniciar sesión en la cuenta correcta, aparecerá el error Página no encontrada (404).

4. Revise los términos y condiciones.
5. Elija Aceptar condiciones.

> **Note**
>
> Si no se acepta una oferta AWS Marketplace privada, las tarifas de ROSA servicio AWS Marketplace se seguirán facturando según la tarifa pública por hora.

6. Para comprobar los detalles de la oferta, seleccione Mostrar detalles en el listado de productos.
7. Para empezar a usarlo ROSA, selecciona Continuar con la configuración. Se le redirigirá a la ROSA consola.

Private Marketplace

Private Marketplace permite a los administradores crear catálogos digitales personalizados de productos aprobados desde AWS Marketplace. Los administradores pueden crear conjuntos únicos de software aprobado que estén disponibles en AWS Marketplace las unidades AWS organizativas o Cuentas de AWS en otras unidades de su organización para su compra.

Si tu organización utiliza un mercado privado, un administrador debe añadir los AWS Marketplace anuncios al mercado privado ROSA para que los usuarios puedan habilitar el servicio. Para obtener más información, consulta Cómo empezar a utilizar un mercado privado en la Guía del AWS Marketplace comprador.

Resolución de problemas

En la página siguiente se detallan algunos problemas comunes que se producen al crear o administrar ROSA clústeres.

Temas

Acceda a los ROSA registros de depuración de clústeres

Para comenzar a solucionar los problemas de la aplicación, revise primero los registros de depuración. Los registros de depuración de la ROSA CLI proporcionan detalles sobre los mensajes de error que se producen cuando clúster no se crea una.

Para mostrar la información de clúster depuración, ejecute el siguiente comando ROSA CLI. En el comando, `<cluster_name>` sustitúyalo por el nombre de su clúster.

```
rosa describe cluster -c <cluster_name> --debug
```

ROSA El clúster no supera la comprobación de la cuota de AWS servicio durante clúster la creación

Para usarlo ROSA, es posible que debas aumentar las cuotas de servicio de tu cuenta. Para obtener más información, consulte Puntos de conexión y cuotas de Red Hat OpenShift Service en AWS.

1. Ejecute el siguiente comando para identificar las cuotas de la cuenta.

   ```
   rosa verify quota
   ```

> **Note**
>
> Las cuotas son diferentes en diferentes Regiones de AWS. Asegúrese de verificar cada una de las cuotas de sus regiones.

2. Si necesita aumentar su cuota, acceda a la consola de Service Quotas.
3. En el panel de navegación, selecciona AWS servicios.
4. Seleccione el servicio que necesita un aumento de cuota.
5. Seleccione la cuota que debe aumentarse y seleccione Solicitar aumento de cuota.
6. En Solicitar aumento de cuota, introduzca la cantidad total que desea asignarle a la cuota y seleccione Solicitar.

Solucionar problemas con los tokens de acceso sin conexión caducados por ROSA CLI

Si utilizas la ROSA CLI y tu token de acceso sin conexión a api.openshift.com caduca, aparece un mensaje de error. Esto ocurre cuando sso.redhat.com invalida el token.

1. Ve a la página del token de la API de OpenShift Cluster Manager y selecciona Cargar token.
2. Copie y pegue el siguiente comando de autenticación en el terminal.

```
rosa login --token="<api_token>"
```

No se pudo crear un clúster con un osdCcsAdmin error

> **Note**
>
> Este error solo se produce cuando se utiliza un método distinto de STS para aprovisionar clústeres ROSA . Para evitar este problema, aprovisione los ROSA clústeres mediante. AWS STS Para obtener más información, consulte the section called “Cree un clúster clásico de ROSA - CLI”.

Si clúster no se puede crear, es posible que reciba el siguiente mensaje de error:

```
Failed to create cluster: Unable to create cluster spec: Failed to get access keys for
 user 'osdCcsAdmin': NoSuchEntity: The user with name osdCcsAdmin cannot be found.
```

1. Elimine la pila.

```
rosa init --delete-stack
```

2. Reinicialice su cuenta.

```
rosa init
```

Siguientes pasos

- Consulta la OpenShift documentación.
- Abra un Soporte caso o un caso de Red Hat Support.
- Encuentre respuestas a las preguntas más frecuentes sobre Red Hat OpenShift Service en AWS.
- Para obtener más información sobre el modelo de soporte de ROSA, consultethe section called “Cómo obtener asistencia”.

Obtener ROSA apoyo

Con ROSA, puede recibir el apoyo de Soporte los equipos de soporte de Red Hat. Los casos de asistencia se pueden abrir con cualquiera de las organizaciones y se envían al equipo correcto para resolver el problema.

Abra un Soporte caso

Se requiere un plan de soporte para AWS desarrolladores para abrir casos ROSA técnicos, pero se recomienda un plan AWS Business, Enterprise o Enterprise On-Ramp Support para tener acceso continuo al soporte ROSA técnico y a la orientación de arquitectura. Red Hat usa la Soporte API para abrir casos para los clientes cuando es necesario. AWS Los planes de soporte Business, Enterprise y Enterprise On-Ramp permiten el acceso continuo por teléfono, web y chat a los ingenieros de soporte. Para obtener más información sobre Soporte los planes, consulte Soporte.

Para ver los pasos para habilitar un Soporte plan, consulta ¿Cómo me suscribo a un Soporte plan?

Para obtener información sobre cómo crear un Soporte caso, consulte Creación de casos de soporte y administración de casos.

Abrir un caso de Red Hat Support

ROSA incluye Red Hat Premium Support. Para recibir Red Hat Premium Support, diríjase al Portal de clientes de Red Hat y utilice la herramienta de casos de asistencia para crear un ticket de asistencia. Para más información, consulte Cómo comunicarse con la asistencia de Red Hat.

Historial del documento

En la siguiente tabla se describen los cambios importantes en la documentación de . Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Actualizado ROSAControlPlaneOperatorPolicy	Se actualizó la política AWS gestionada ROSAControl PlaneOperatorPolicy para permitir el etiquetado de los grupos de seguridad gestionados por Red Hat para gestionar adecuadamente el ciclo de vida de los recursos y para añadir Security-group/* a Manage para corregir los errores de reconciliación de VPCE durante las actualizaciones de VPCEndpoint WithCondition los clústeres. Para obtener más información, consulte las actualizaciones de las políticas administradas.ROSAAWS	9 de abril de 2026
Actualizado ROSAKubeControllerPolicy	Se actualizó la política AWS administrada ROSAKube ControllerPolicy para aclarar los permisos de Elastic Load Balancing para registrar y anular el registro de objetivos en los grupos de destino. Para obtener más información, consulte ROSA las actualiza	5 de marzo de 2026

	ciones de las políticas AWS administradas.	
Actualizado ROSANodePoolManagementPolicy	ROSA ha actualizado la política gestionada `ROSANodePoolManagementPolicy` para añadir el acceso a los recursos para las reservas de capacidad a fin de admitir la función de reservas de capacidad. Para obtener más información, consulte ROSA las actualizaciones de las políticas AWS gestionadas.	3 de septiembre de 2025
ROSAInstallerPolítica actualizada	Se actualizó la ROSAInstaller política de AWS gestión para respaldar la nueva función de reservas de capacidad de ROSA y mejorar la gestión de las etiquetas de clúster de Kubernetes. Para obtener más información, consulte las ROSA actualizaciones de las políticas gestionadas AWS.	7 de agosto de 2025
Nueva ROSASharedVPCRoute53 política	ROSA ha publicado una nueva política gestionada que permite `ROSASharedVPCRoute53Policy` al instalador de ROSA configurar los registros de Route 53 en entornos de VPC compartidos. Para obtener más información, consulte ROSA las actualizaciones de las políticas AWS administradas.	7 de agosto de 2025

Nueva ROSAShared VPCEndpoint política	ROSA ha publicado una nueva política gestionada que permite `ROSAShare dVPCEndpointPolicy` al instalador de ROSA configurar puntos finales de VPC y grupos de seguridad en entornos de VPC compartid os. Esta política proporciona un subconjunto de permisos de EC2 diseñados para casos de uso de VPC compartidas. Para obtener más informaci ón, consulte las ROSA actualizaciones de las políticas gestionadas AWS.	7 de agosto de 2025
Actualizado ROSAImage RegistryOperatorPolicy	Se actualizó la política AWS gestionada ROSAImage RegistryOperatorPolicy.	19 de mayo de 2025
Actualizado ROSANodeP oolManagementPolicy	Se actualizó la política AWS gestionada ROSANodeP oolManagementPolicy .	5 de mayo de 2025
Actualizado ROSAImage RegistryOperatorPolicy	Se actualizó la política AWS gestionada ROSAImage RegistryOperatorPolicy.	16 de abril de 2025
Actualizado ROSAWorke rInstancePolicy	Se actualizó la política AWS gestionada ROSAWorke rInstancePolicy.	3 de marzo de 2025
Actualizado ROSANodeP oolManagementPolicy	Se actualizó la política AWS gestionada ROSANodeP oolManagementPolicy.	24 de febrero de 2025

Actualizado ROSAAmazonEBSCSIDriverOperatorPolicy	Se actualizó la política AWS gestionada ROSAAmazon EBSCSIDriverOperatorPolicy.	17 de enero de 2025
ROSA con expansión de HCP Región de AWS	ROSA con aviones de control alojados (HCP) ya está disponible en Oriente Medio (Emiratos Árabes Unidos). Región de AWS	13 de mayo de 2024
ROSA con expansión de HCP Región de AWS	ROSA con planos de control alojados (HCP) ya está disponible en Europa (París). Región de AWS	6 de mayo de 2024
Actualizado ROSANodePoolManagementPolicy	Se actualizó la política AWS ROSANode PoolManagementPolicy gestionada.	2 de mayo de 2024
ROSA con expansión de HCP Región de AWS	ROSA con planes de control alojados (HCP) ya está disponible en Europa (España). Región de AWS	29 de abril de 2024
Política actualizada ROSAInstaller	Se actualizó la ROSAInstaller política AWS gestionada.	24 de abril de 2024
ROSA con la expansión de HCP Región de AWS	ROSA con planos de control alojados (HCP) ya está disponible en Europa (Zúrich). Región de AWS	19 de abril de 2024
ROSA con expansión de HCP Región de AWS	ROSA con aviones de control alojados (HCP) ya está disponible en Asia Pacífico (Osaka). Región de AWS	17 de abril de 2024

ROSAInstallerPolítica y ROSASRESupport política actualizadas	Se actualizaron la ROSAInstaller política y ROSASRESupport la política de políticas AWS gestionadas.	10 de abril de 2024
ROSA con la expansión de HCP Región de AWS	ROSA con aviones de control alojados (HCP) ya está disponible en Asia Pacífico (Hong Kong). Región de AWS	8 de abril de 2024
ROSA con expansión de HCP Región de AWS	ROSA con planos de control alojados (HCP) ya está disponible en Sudamérica (São Paulo). Región de AWS	1 de abril de 2024
ROSA con expansión de HCP Región de AWS	ROSA con aviones de control alojados (HCP) ya está disponible en Oriente Medio (Baréin). Región de AWS	25 de marzo de 2024
ROSA con expansión de HCP Región de AWS	ROSA con aviones de control alojados (HCP) ya está disponible en Asia Pacífico (Seúl). Región de AWS	14 de marzo de 2024
ROSA con expansión de HCP Región de AWS	ROSA con aviones de control alojados (HCP) ya está disponible en África (Ciudad del Cabo). Región de AWS	5 de marzo de 2024
Política actualizada ROSAInstaller	Se actualizó la ROSAInstaller política AWS gestionada.	26 de enero de 2024
ROSASRESupportPolítica actualizada	Se actualizó la ROSASRESupport política AWS gestionada.	22 de enero de 2024

Actualizado ROSAImage RegistryOperatorPolicy	Se actualizó la política AWS gestionada ROSAImage RegistryOperatorPolicy.	12 de diciembre de 2023
Actualizado ROSAKubeC ontrollerPolicy	Se actualizó la política AWS gestionada ROSAKubeC ontrollerPolicy.	16 de octubre de 2023
ROSAManageSuscripción actualizada	Se actualizó la ROSAManage suscripción a la política AWS gestionada.	1 de agosto de 2023
Actualizado ROSAKubeC ontrollerPolicy	Se actualizó la política AWS gestionada ROSAKubeC ontrollerPolicy.	13 de julio de 2023
Se agregaron las páginas de seguridad de ROSA	Se agregaron las páginas de resiliencia en ROSA, seguridad de infraestructura en ROSA y protección de datos en ROSA.	30 de junio de 2023
Se agregó la página de opciones de implementación	Se agregó la página de opciones de implementación.	9 de junio de 2023
Se agregó una nueva política AWS gestionada ROSANode PoolManagementPolicy	Se agregó una nueva política AWS ROSANode PoolManag ementPolicy gestionada.	8 de junio de 2023
Se agregó una nueva política AWS gestionada (ROSAInsta llerPolítica)	Se agregó una nueva ROSAInstaller política de políticas AWS administradas.	6 de junio de 2023
Se agregó una nueva política AWS gestionada (ROSASRESupportPolítica)	Se agregó una nueva ROSASRESupport política de políticas AWS administradas.	1 de junio de 2023

Se agregó información general de responsabilidades para ROSA	Se agregó una página de información general de responsabilidades para ROSA.	26 de mayo de 2023
Actualizado ¿Qué es Red Hat OpenShift Service en AWS?	Se actualizó la Red Hat OpenShift Service en AWS página Qué es.	24 de mayo de 2023
Se agregaron nuevas políticas AWS administradas para los roles de operador de ROSA	Se agregaron nuevas políticas AWS ROSAImage RegistryOperatorPolicy gestionadas y ROSAKMSProvider políticas. ROSAKube ControllerPolicy	27 de abril de 2023
Se agregó una nueva política AWS administrada ROSAControl PlaneOperatorPolicy	Se agregó una nueva política AWS ROSAControl PlaneOperatorPolicy gestionada.	24 de abril de 2023
Se agregaron nuevas políticas AWS administradas para los roles de las cuentas ROSA	Se agregaron nuevas páginas de políticas AWS administradas para la cuenta ROSA y la página de roles de operador.	20 de abril de 2023
Se agregó la página de Service Quotas de ROSA	Se agregó la página de cuotas de servicio de ROSA.	22 de diciembre de 2022
Se agregaron páginas de solución de problemas	Se agregaron páginas de solución de problemas.	1 de noviembre de 2022
Se agregaron páginas de introducción	Se agregaron páginas de introducción.	12 de agosto de 2022
Se agregó una nueva política AWS gestionada: ROSAManage Suscripción	Se agregó una nueva ROSAManage suscripción a una política AWS gestionada.	11 de abril de 2022

Versión inicial	La versión inicial de la Guía Red Hat OpenShift Service en AWS del usuario.	24 de marzo de 2021

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.