aws

Manual do usuário

Serviço Red Hat OpenShift na AWS

Serviço Red Hat OpenShift na AWS: Manual do usuário

Table of Contents

O que Serviço Red Hat OpenShift na AWSé

Serviço Red Hat OpenShift na AWS (ROSA) é um serviço gerenciado que você pode usar para criar, escalar e implantar aplicativos em contêineres com a plataforma OpenShift corporativa Kubernetes da Red Hat. AWS ROSA simplifica a transferência de OpenShift cargas de trabalho locais da Red Hat e oferece uma forte integração com outras. AWS Serviços da AWS

Recursos

ROSA é suportado e operado em conjunto pela Red AWS Hat. Cada ROSA cluster vem com suporte 24 horas do Red Hat Site Reliability Engineer (SRE) para gerenciamento de clusters, respaldado pelo acordo de nível de serviço (SLA) de 99,95% de tempo de atividade da Red Hat. Para obter mais informações sobre o modelo de suporte do serviço, consultethe section called “Obter suporte”.

ROSA também fornece os seguintes recursos:

- Instalação de cluster com suporte SRE da Red Hat, manutenção do cluster e atualizações do cluster.
- AWS service (Serviço da AWS) as integrações incluem AWS computação, banco de dados, análise, aprendizado de máquina, redes e dispositivos móveis.
- Execute e escale o plano de controle do Kubernetes em várias zonas de AWS disponibilidade para garantir alta disponibilidade.
- OpenShift APIs Opere clusters usando ferramentas de produtividade para desenvolvedores, incluindo Service Mesh, CodeReady Workspaces e Serverless.

Acessando ROSA

Você pode definir e configurar suas implantações ROSA de serviços usando as seguintes interfaces.

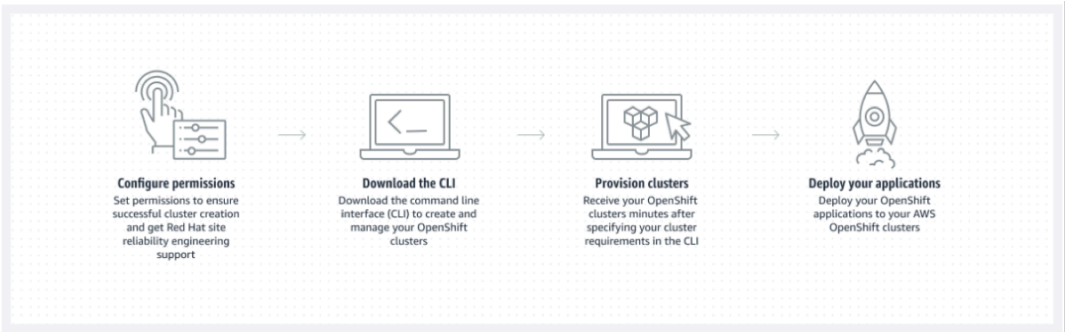
AWS

- ROSA console — fornece uma interface web para permitir a ROSA assinatura e a compra de um contrato ROSA de software.
- AWS Command Line Interface (AWS CLI) — Fornece comandos para um amplo conjunto de Serviços da AWS e é compatível com Windows, macOS e Linux. Para obter mais informações, consulte AWS Command Line Interface.

Red Hat OpenShift

- Red Hat Hybrid Cloud Console — fornece uma interface web para criar, atualizar e gerenciar ROSA clusters, instalar complementos de cluster e criar e implantar aplicativos em um ROSA cluster.
- ROSA CLI (rosa) — Fornece comandos para criar, atualizar e gerenciar ROSA clusters.
- OpenShift CLI (oc) — Fornece comandos para criar aplicativos e gerenciar projetos da OpenShift Container Platform.
- CLI do Knative (kn) - Fornece comandos que podem ser usados para interagir OpenShift com componentes sem servidor, como o Knative Serving e o Eventing.
- PIPELINES CLI (tkn) - Fornece comandos para interagir OpenShift com Pipelines usando o terminal.
- opm CLI - Fornece comandos que ajudam desenvolvedores de operadores e administradores de cluster a criar e OpenShift manter catálogos de operadores a partir do terminal.
- CLI do SDK do operador - fornece comandos que um desenvolvedor do Operator pode usar para criar, testar e implantar OpenShift um operador.

Como começar com ROSA



O seguinte resume o processo de introdução do. ROSA Para obter instruções detalhadas de introdução, consulteComece com ROSA .

AWS Management Console/AWS CLI

1. Configure as permissões necessárias para Serviços da AWS fornecer a funcionalidade do serviço. ROSA Para obter mais informações, consulte the section called “Pré-requisitos”.
2. Instale e configure a AWS CLI ferramenta mais recente. Para obter mais informações, consulte Instalando ou atualizando a versão mais recente do AWS CLI no Guia AWS CLI do Usuário.

3. Ative ROSA no ROSA console.

ROSA Console/CLI de nuvem híbrida Red Hat

1. Baixe a versão mais recente da CLI e da ROSA OpenShift CLI no Red Hat Hybrid Cloud Console. Para obter mais informações, consulte Introdução à ROSA CLI na documentação da Red Hat.
2. Crie ROSA clusters no Red Hat Hybrid Cloud Console ou com a ROSA CLI.
3. Quando seu cluster estiver pronto, configure um provedor de identidade para conceder acesso do usuário ao cluster.
4. Implante e gerencie cargas de trabalho em seu ROSA cluster da mesma forma que faria com qualquer outro OpenShift ambiente.

Preços

O custo total do ROSA consiste em dois componentes: taxas ROSA de serviço e taxas de AWS infraestrutura. Para saber mais sobre precificação, consulte Precificação do Serviço Red Hat OpenShift na AWS.

ROSA taxas de serviço

Por padrão, as taxas ROSA de serviço são acumuladas sob demanda a uma taxa horária por 4 vCPUs usadas pelos nós de trabalho. As taxas de serviço são uniformes em todas as regiões AWS padrão suportadas. Além da taxa de serviço do nó de trabalho, o ROSA com clusters de planos de controle hospedados (HCP) incorre em uma taxa de cluster por hora.

ROSA oferece contratos de taxa de serviço de 1 e 3 anos que você pode comprar para economizar nas taxas de serviço sob demanda para nós de trabalho. Para obter mais informações, consulte the section called “Comprando um ROSA contrato”.

AWS taxas de infraestrutura

AWS as taxas de infraestrutura se aplicam aos nós subjacentes de trabalho, nós de infraestrutura, nós do plano de controle, armazenamento e recursos de rede hospedados na infraestrutura AWS global. AWS as taxas de infraestrutura variam de acordo com Região da AWS.

Visão geral das responsabilidades por ROSA

Esta documentação descreve as responsabilidades da Amazon Web Services (AWS), da Red Hat e dos clientes pelo serviço gerenciado Serviço Red Hat OpenShift na AWS (ROSA). Para obter mais informações sobre ROSA seus componentes, consulte Políticas e definição de serviços na documentação da Red Hat.

O modelo de responsabilidade AWS compartilhada define a AWS responsabilidade de proteger a infraestrutura que executa todos os serviços oferecidos no Nuvem AWS, inclusive ROSA. AWS a infraestrutura inclui o hardware, o software, a rede e as instalações que executam Nuvem AWS os serviços. Essa AWS responsabilidade é comumente chamada de “segurança da nuvem”. Para operar ROSA como um serviço totalmente gerenciado, a Red Hat e o cliente são responsáveis pelos elementos do serviço que o modelo de AWS responsabilidade define como “segurança na nuvem”.

A Red Hat é responsável pelo gerenciamento e pela segurança contínuos da infraestrutura do ROSA cluster, da plataforma de aplicativos subjacente e do sistema operacional. Embora os ROSA clusters sejam hospedados em AWS recursos do cliente Contas da AWS, eles são acessados remotamente pelos componentes do ROSA serviço e pelos engenheiros de confiabilidade do site da Red Hat (SREs) por meio de IAM funções criadas pelo cliente. A Red Hat utiliza esse acesso para gerenciar a implantação e a capacidade de todos os nós do ambiente de gerenciamento e da infraestrutura no cluster, além de manter as versões dos nós do ambiente de gerenciamento, nós de infraestrutura e nós de processamento.

A Red Hat e o cliente compartilham a responsabilidade pelo gerenciamento de ROSA rede, registro de clusters, controle de versões de clusters e gerenciamento de capacidade. Enquanto a Red Hat gerencia o ROSA serviço, o cliente é totalmente responsável por gerenciar e proteger todos os aplicativos, cargas de trabalho e dados implantados. ROSA

Visão geral do

A tabela a seguir fornece uma visão geral das AWS responsabilidades da Red Hat e do cliente pela Serviço Red Hat OpenShift na AWS.

> **Note**
>
> Se a função `cluster-admin` for adicionada a um usuário, consulte as responsabilidades e notas de exclusão no Anexo 4 do Acordo Empresarial da Red Hat (serviços de assinatura online).

Recurso	Gerenciamento de incidentes e operações	Gerenciamento de alterações	Autorização de acesso e identidade	Conformidade regulatória e de segurança	Recuperação de desastres
Dados de cliente	Cliente	Cliente	Cliente	Cliente	Cliente
Aplicações personalizadas	Cliente	Cliente	Cliente	Cliente	Cliente
Serviços do desenvolvedor	Cliente	Cliente	Cliente	Cliente	Cliente
Monitoramento da plataforma	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Registro em log	Red Hat	Red Hat e o cliente	Red Hat e o cliente	Red Hat e o cliente	Red Hat
Rede de aplicações	Red Hat e o cliente	Red Hat e o cliente	Red Hat e o cliente	Red Hat	Red Hat
Rede em cluster	Red Hat	Red Hat e o cliente	Red Hat e o cliente	Red Hat	Red Hat
Gerenciamento de rede virtual	Red Hat e o cliente	Red Hat e o cliente	Red Hat e o cliente	Red Hat e o cliente	Red Hat e o cliente
Gerenciamento de computação virtual (ambiente de gerenciam	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat

Recurso	Gerenciamento de incidentes e operações	Gerenciamento de alterações	Autorização de acesso e identidade	Conformidade regulatória e de segurança	Recuperação de desastres
ento, infraestrutura e nós de processamento)					
Versões do cluster	Red Hat	Red Hat e o cliente	Red Hat	Red Hat	Red Hat
Gerenciamento de capacidade	Red Hat	Red Hat e o cliente	Red Hat	Red Hat	Red Hat
Gerenciamento de armazenamento virtual	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS software (público Serviços da AWS)	AWS	AWS	AWS	AWS	AWS
Hardware/ infraestrutura global AWS	AWS	AWS	AWS	AWS	AWS

Tarefas para responsabilidades compartilhadas por área

AWS, a Red Hat e os clientes compartilham a responsabilidade pelo monitoramento e pela manutenção dos ROSA componentes. Essa documentação define as responsabilidades do ROSA serviço por área e tarefa.

Gerenciamento de incidentes e operações

AWS é responsável por proteger a infraestrutura de hardware que executa todos os serviços oferecidos no Nuvem AWS. A Red Hat é responsável por gerenciar os componentes de serviço necessários para a rede da plataforma padrão. O cliente é responsável pelo gerenciamento de incidentes e operações dos dados da aplicação do cliente e de qualquer rede personalizada que o cliente possa ter configurado.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Rede de aplicações	Red Hat • Monitore o serviço OpenShift do roteador nativo e responda aos alertas.	Cliente • Monitorar a saúde das rotas da aplicação e os pontos de extremidade associados a elas. • Relate interrupções à Red Hat AWS e à Red Hat.
Gerenciamento de rede virtual	Red Hat • Monitore balanceadores de AWS carga, Amazon VPC sub-redes e AWS service (Serviço da AWS) componentes necessári os para a rede padrão da plataforma. Responder a alertas.	Cliente • Monitore a integridade dos endpoints do balanceador de AWS carga. • Monitore o tráfego de rede que é configurado opcionalmente por Amazon VPC meio de conexão com o VPC, Site-to-Site VPN conexão ou Direct Connect para possíveis problemas ou ameaças à segurança.
Gerenciamento de armazenamento virtual	Red Hat • Monitore Amazon EBS os volumes usados para os nós do cluster e Amazon	Cliente • Monitorar a integridade dos dados da aplicação.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
	S3 os buckets usados para o registro de imagens de contêiner incorporado do ROSA serviço. Responder a alertas.	• Se as políticas gerenciadas pelo cliente AWS KMS keys forem usadas, crie e controle o ciclo de vida da chave e as principais políticas para Amazon EBS criptografia.
AWS software (público Serviços da AWS)	AWS • Para obter informações sobre gerenciamento de AWS incidentes e operações, consulte Como AWS mantém a resiliência operacional e a continuidade do serviço no AWS whitepaper.	Cliente • Monitore a integridade dos AWS recursos na conta do cliente. • Use IAM ferramentas para aplicar as permissões apropriadas aos AWS recursos na conta do cliente.
Hardware/infraestrutura global AWS	AWS • Para obter informações sobre gerenciamento de AWS incidentes e operações, consulte Como AWS mantém a resiliência operacional e a continuidade do serviço no AWS whitepaper.	Cliente • Configure, gerencie e monitore aplicações e dados do cliente para garantir que os controles de segurança das aplicações e dados sejam devidamente aplicados.

Gerenciamento de alterações

AWS é responsável por proteger a infraestrutura de hardware que executa todos os serviços oferecidos no Nuvem AWS. A Red Hat é responsável por habilitar alterações na infraestrutura e serviços do cluster que o cliente controlará, além de manter as versões para os nós do ambiente de

gerenciamento, nós de infraestrutura e nós de processamento. O cliente é responsável por iniciar as mudanças na infraestrutura. O cliente também é responsável por instalar e manter serviços opcionais, configurações de rede no cluster e alterações nos dados e aplicações do cliente.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Registro em log	Red Hat • Centralizar a agregação e monitoramento de logs de auditoria da plataforma. • Fornecer e manter um operador de logs para permitir que o cliente implemente uma pilha de logs para o log padrão de aplicações. • Fornecer logs de auditoria mediante solicitação do cliente.	Cliente • Instale o operador de logs de aplicação padrão opcional no cluster. • Instalar, configurar e manter quaisquer soluções opcionais de logs de aplicações, como contêiner es de logs auxiliares (sidecar) ou aplicações de logs de terceiros. • Ajustar o tamanho e a frequência dos logs de aplicação produzidos pelas aplicações do cliente, caso estejam afetando a estabilid ade da pilha de logs ou do cluster. • Solicitar logs de auditoria da plataforma por meio de um chamado de suporte para investigar incidentes específicos.
Rede de aplicações	Red Hat • Configurar balancead ores de carga públicos. Forneça a capacidade de configurar balanceadores	Cliente • Configure permissões de rede de pod não padrão para redes de projeto e pod, entrada e saída de pod

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
	de carga privados e até um balanceador de carga adicional quando necessário. • Configure o serviço de OpenShift roteador nativo. Forneça a capacidade de definir o roteador como privado e adicionar até um fragmento de roteador adicional. • Instale, configure e mantenha componentes OpenShift SDN para o tráfego interno padrão do pod. • Forneça ao cliente a capacidade de gerenciar objetos do `NetworkPolicy` e `EgressNetworkPolicy` (firewall).	usando objetos `NetworkPolicy` . • Use o OpenShift Cluster Manager para solicitar um balanceador de carga privado para rotas de aplicativos padrão. • Use o OpenShift Cluster Manager para configurar até um fragmento de roteador público ou privado adicional e o balanceador de carga correspondente. • Solicite e configure quaisquer balanceadores de carga de serviço adicionais para serviços específicos. • Configure todas as regras de encaminhamento de DNS necessárias.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Rede em cluster	Red Hat • Configure componentes de gerenciamento de cluster, como endpoints de serviço públicos ou privados e a integração necessária com Amazon VPC os componentes. • Configurar os componentes internos de rede necessários para a comunicação interna do cluster entre os nós de processamento, infraestrutura e ambiente de gerenciamento.	Cliente • Forneça intervalos opcionais de endereços IP não padrão para CIDR de máquina, CIDR de serviço e CIDR de pod, se necessário, por meio do OpenShift Cluster Manager quando o cluster for provisionado. • Solicite que o endpoint do serviço de API seja tornado público ou privado na criação do cluster ou após a criação do OpenShift cluster por meio do Cluster Manager.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Gerenciamento de rede virtual	Red Hat • Configure e configure Amazon VPC os componentes necessários para provisionar o cluster, como sub-redes, balanceadores de carga, gateways de internet e gateways NAT. • Forneça ao cliente a capacidade de gerenciar a Site-to-Site VPN conectividade com recursos locais, Amazon VPC conectividade com o VPC e, Direct Connect conforme necessário, por meio OpenShift do Cluster Manager. • Permita que os clientes criem e implantem AWS balanceadores de carga para uso com balanceadores de carga de serviço.	Cliente • Configure e mantenha Amazon VPC componentes opcionais, como conexão Amazon VPC com o VPC, Site-to-Site VPN conexão ou. Direct Connect • Solicite e configure quaisquer balanceadores de carga adicionais para serviços específicos.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Gerenciamento de computação virtual	Red Hat • Configure e configure o plano ROSA de controle e o plano de dados para usar Amazon EC2 instâncias para computação em cluster. • Monitore e gerencie a implantação do plano de Amazon EC2 controle e dos nós de infraestrutura no cluster.	Cliente • Monitore e gerencie os nós de Amazon EC2 trabalho criando um pool de máquinas usando o OpenShift Cluster Manager ou a ROSA CLI. • Gerencie as alterações nas aplicações implantadas pelo cliente e nos dados do aplicação.
Versões do cluster	Red Hat • Habilite processo de agendamento de atualização. • Monitore o progresso da atualização e solucione quaisquer problemas encontrados. • Publique logs de alterações e notas de versão para atualizações menores e de manutenção.	Cliente • Agende atualizações de versões de manutenção imediatamente, para o futuro, ou faça atualizações automáticas. • Reconheça e agende pequenas atualizações de versões. • Certifique-se de que a versão do cluster permaneça em uma versão secundária compatível. • Teste as aplicações do cliente em versões secundárias e de manutenção para garantir a compatibilidade.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Gerenciamento de capacidade	Red Hat • Monitore o uso do ambiente de gerenciamento. Os ambientes de gerenciam ento incluem nós do ambiente de gerenciamento e nós de infraestrutura. • Dimensione e redimensi one os nós do ambiente de gerenciamento para manter a qualidade do serviço.	Cliente • Monitore a utilização do nó de processamento e, se apropriado, ative o recurso de ajuste de escala automático. • Determine a estratégia de escalabilidade do cluster. • Use os controles do OpenShift Cluster Manager fornecidos para adicionar ou remover outros nós de trabalho, conforme necessário. • Responda às notificaç ões da Red Hat sobre os requisitos de recursos do cluster.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Gerenciamento de armazenamento virtual	Red Hat • Configure e configure Amazon EBS para provisionar armazenamento de nós locais e armazenamento de volume persistente para o cluster. • Configure e configure o registro de imagens incorporado para usar o armazenamento em Amazon S3 bucket. • Remova regularmente os recursos de registro de imagens Amazon S3 para otimizar o Amazon S3 uso e o desempenho do cluster.	Cliente • Opcionalmente, configure o driver Amazon EBS CSI ou o driver Amazon EFS CSI para provisionar volumes persistentes no cluster.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente

AWS software (AWS serviços públicos)	AWS
	
	Computação
	
	• Forneça o Amazon EC2 serviço, usado para o plano ROSA de controle, a infraestrutura e os nós de trabalho.
	
	Armazenamento
	
	• Forneça Amazon EBS para permitir que o ROSA serviço provisione armazenamento de nós locais e armazenam ento de volume persistente para o cluster.
	
	Redes
	
	• Forneça os seguintes Nuvem AWS serviços para satisfazer as necessidades de infraestrutura de rede ROSA virtual:
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• Forneça as seguintes AWS service (Serviço da AWS) integrações opcionais para ROSA:
	  • Site-to-Site VPN
		Cliente
		
		• Assine solicitações usando uma ID de chave de acesso e uma chave de acesso secreta associada a uma credencial de segurança IAM principal ou AWS STS temporária.
		• Especifique sub-redes VPC para o cluster usar durante a criação do cluster.
		• Opcionalmente, configure uma VPC gerenciada pelo cliente para uso com clusters. ROSA

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
	• Direct Connect • AWS PrivateLink • AWS Transit Gateway	
Hardware/infraestrutura global AWS	AWS • Para obter informaçõ es sobre controles de gerenciamento para data AWS centers, consulte Nossos controles na página Nuvem AWS Segurança. • Para obter informaçõ es sobre as melhores práticas de gerenciamento de mudanças, consulte Orientações para gerenciam ento de mudanças AWS na Biblioteca de AWS soluções.	Cliente • Implemente as melhores práticas de gerenciam ento de mudanças para aplicações e dados de clientes hospedados no Nuvem AWS.

Autorização de acesso e identidade

A autorização de acesso e identidade inclui responsabilidades pelo gerenciamento do acesso autorizado a clusters, aplicações e recursos de infraestrutura. Isso inclui tarefas como fornecer mecanismos de controle de acesso, autenticação, autorização e gerenciamento do acesso aos recursos.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Registro em log	Red Hat • Siga um processo de acesso interno hierárquico baseado em padrões do	Cliente • Configure o OpenShift RBAC para controlar o acesso aos projetos e, por

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
	setor para logs de auditoria da plataforma. • Forneça recursos nativos OpenShift de RBAC.	extensão, aos registros do aplicativo de um projeto. • Para soluções de registro de aplicações de terceiros ou personalizadas, o cliente é responsável pelo gerenciamento de acesso.
Rede de aplicações	Red Hat • Forneça OpenShift RBAC e `dedicated-admin` recursos nativos.	Cliente • Configure OpenShift `dedicated-admin` um RBAC para controlar o acesso à configuração da rota, conforme necessário. • Gerencie os administr adores da organização Red Hat para que a Red Hat conceda acesso ao OpenShift Cluster Manager. O gerenciador de cluster é usado para configura r as opções do roteador e fornecer a cota do balanceador de carga de serviço.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Rede em cluster	Red Hat • Forneça controles de acesso ao cliente por meio OpenShift do Cluster Manager. Forneça OpenShift RBAC e `dedicated-admin` recursos nativos.	Cliente • Configure OpenShift `dedicated-admin` um RBAC para controlar o acesso à configuração da rota, conforme necessário. • Gerencie a associação da organização Red Hat às contas Red Hat. • Gerencie os administr adores da organização para que a Red Hat conceda acesso ao OpenShift Cluster Manager.
Gerenciamento de rede virtual	Red Hat • Forneça controles de acesso ao cliente por meio OpenShift do Cluster Manager.	Cliente • Gerencie o acesso opcional do usuário aos AWS componentes por meio do OpenShift Cluster Manager.
Gerenciamento de computaçã o virtual	Red Hat • Forneça controles de acesso ao cliente por meio OpenShift do Cluster Manager.	Cliente • Gerencie o acesso opcional do usuário aos AWS componentes por meio do OpenShift Cluster Manager. • Crie IAM funções e políticas anexadas necessárias para permitir o acesso ao ROSA serviço.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Gerenciamento de armazenamento virtual	Red Hat • Forneça controles de acesso ao cliente por meio OpenShift do Cluster Manager.	Cliente • Gerencie o acesso opcional do usuário aos AWS componentes por meio do OpenShift Cluster Manager. • Crie IAM funções e políticas anexadas necessárias para permitir o acesso ao ROSA serviço.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
AWS software (AWS serviços públicos)	AWS Computação • Forneça o Amazon EC2 serviço, usado para o plano ROSA de controle, a infraestrutura e os nós de trabalho. Armazenamento • Provide Amazon EBS, usado ROSA para permitir o provisionamento de armazenamento de nós locais e armazenamento de volume persistente para o cluster. • Forneça Amazon S3, usado para o registro de imagens integrado do serviço. Redes • AWS Identity and Access Management Provide (IAM), usado pelos clientes para controlar o acesso aos ROSA recursos executados nas contas dos clientes.	Cliente • Crie IAM funções e políticas anexadas necessárias para permitir o acesso ao ROSA serviço. • Use IAM ferramentas para aplicar as permissõe s apropriadas aos AWS recursos na conta do cliente. • Para habilitar ROSA em toda a AWS organização, o cliente é responsável por gerenciar AWS Organizat ions os administradores. • Para habilitar ROSA em toda a sua AWS organizaç ão, o cliente é responsáv el por distribuir a ROSA concessão de direitos usando. AWS License Manager

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Hardware/infraestrutura global AWS	AWS • Para obter informações sobre controles de acesso físico para data AWS centers, consulte Nossos controles na página Nuvem AWS Segurança.	Cliente • O cliente não é responsáv el pela infraestrutura AWS global.

Conformidade regulatória e de segurança

A seguir estão as responsabilidades e os controles relacionados à conformidade:

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Registro em log	Red Hat • Envie logs de auditoria de cluster para um Red Hat SIEM para analisar eventos de segurança. Retenha os logs de auditoria por um período definido para apoiar a análise forense.	Cliente • Analise os registros da aplicação em busca de eventos de segurança. • Envie os registros da aplicação para um endpoint externo por meio de contêineres auxiliares de logs ou aplicações de logs de terceiros se for necessári a uma retenção maior do que a oferecida pela pilha de logs padrão.
Gerenciamento de rede virtual	Red Hat • Monitore os componentes da rede virtual em busca	Cliente • Monitore os componentes da rede virtual opcionais configurados em busca

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
	de possíveis problemas e ameaças à segurança. • Use AWS ferramentas públicas para monitoram ento e proteção adicionais.	de possíveis problemas e ameaças à segurança. • Configure todas as regras de firewall necessárias ou as proteções do datacente r do cliente, conforme necessário.
Gerenciamento de computaçã o virtual	Red Hat • Monitore componentes de computação virtual em busca de possíveis problemas e ameaças à segurança. • Use AWS ferramentas públicas para monitoram ento e proteção adicionais.	Cliente • Monitore os componentes da rede virtual opcionais configurados em busca de possíveis problemas e ameaças à segurança. • Configure todas as regras de firewall necessárias ou as proteções do datacente r do cliente, conforme necessário.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Gerenciamento de armazenamento virtual	Red Hat • Monitore componentes de armazenamento virtual em busca de possíveis problemas e ameaças à segurança. • Use AWS ferramentas públicas para monitoram ento e proteção adicionais. • Configure o ROSA serviço para criptografar os dados do plano de controle, da infraestrutura e do volume do nó de trabalho por padrão usando a chave KMS AWS gerenciada que Amazon EBS fornece. • Configure o ROSA serviço para criptografar volumes persistentes do cliente que usam a classe de armazenamento padrão com a chave KMS AWS gerenciada fornecida. Amazon EBS • Ofereça ao cliente a capacidade de usar um sistema gerenciado pelo cliente KMS key para criptografar volumes persistentes. • Configure o registro de imagem de contêiner para	Cliente • Amazon EBS Volumes de provisionamento. • Gerencie Amazon EBS o armazenamento de volume para garantir que haja armazenamento suficiente disponível para montagem como um volume ROSA. • Crie a declaração de volume persistente e gere um volume persistente por meio OpenShift do Cluster Manager.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
	criptografar dados de registro de imagem em repouso usando criptografia do lado do servidor com chaves Amazon S3 gerenciadas (SSE-3). • Ofereça ao cliente a capacidade de criar um registro de imagens público ou privado Amazon S3 para proteger suas imagens de contêiner contra o acesso não autorizado de usuários.	

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
AWS software (AWS serviços públicos)	AWS Computação • Forneça Amazon EC2, usado para plano de ROSA controle, infraestrutura e nós de trabalho. Para obter mais informações, consulte Segurança da infraestrutura Amazon EC2 no Guia Amazon EC2 do usuário. Armazenamento • Forneça Amazon EBS, usado para planos de ROSA controle, infraestrutura e volumes de nós de trabalho, bem como volumes persistentes do Kubernetes. Para obter mais informações, consulte Proteção de dados Amazon EC2 no Guia Amazon EC2 do usuário. • Provide AWS KMS, que é ROSA usado para criptografar volumes do plano de controle, da infraestrutura e do nó de trabalho e volumes persistentes. Para obter mais informações, consulte Amazon EBS criptografia	Cliente • Garanta que as melhores práticas de segurança e o princípio do menor privilégio sejam seguidos para proteger os dados na Amazon EC2 instância. Para obter mais informações, consulte Segurança de infraestrutura em Amazon EC2 e Proteção de dados em Amazon EC2. • Monitore os componentes da rede virtual opcionais configurados em busca de possíveis problemas e ameaças à segurança. • Configure todas as regras de firewall necessárias ou as proteções do datacenter do cliente, conforme necessário. • Crie uma chave KMS opcional gerenciada pelo cliente e criptografe o volume Amazon EBS persistente usando a chave KMS. • Monitore os dados do cliente armazenados virtualmente em busca de possíveis problemas e ameaças de segurança

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
	no Guia Amazon EC2 do usuário. • Forneça Amazon S3, usado para o registro de imagem de contêiner integrado do serviço ROSA. Para obter mais informações, consulte Amazon S3 segurança no Guia Amazon S3 do usuário. Redes • Forneça recursos e serviços de segurança para aumentar a privacidade e controlar o acesso à rede na infraestrutura AWS global, incluindo firewalls de rede integrados Amazon VPC, conexões de rede privadas ou dedicadas e criptografia automática de todo o tráfego nas redes AWS globais e regionais entre instalações AWS protegidas. Para obter mais informações, consulte o Modelo de Responsabilidade AWS Compartilhada e a segurança da infraestrutura no whitepaper Introdução à AWS Segurança.	. Para mais informações, consulte o .Modelo de responsabilidade compartilhada da AWS.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Hardware/infraestrutura global AWS	AWS • Forneça a infraestrutura AWS global ROSA usada para fornecer a funcionalidade do serviço. Para obter mais informações sobre controles de AWS segurança, consulte Segurança da AWS infraestrutura no AWS whitepaper. • Forneça documentação para que o cliente gerencie as necessidades de conformidade e verifique seu estado de segurança AWS usando ferramentas como AWS Artifact o AWS Security Hub.	Cliente • Configure, gerencie e monitore aplicações e dados do cliente para garantir que os controles de segurança das aplicações e dados sejam devidamente aplicados. • Use IAM ferramentas para aplicar as permissões apropriadas aos AWS recursos na conta do cliente.

Recuperação de desastres

A recuperação de desastres inclui backup de dados e configurações, replicação de dados e configuração do ambiente de recuperação de desastres e failover em eventos de desastres.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
Gerenciamento de rede virtual	Red Hat • Restaure ou recrie componentes de rede virtual afetados que sejam necessários para o funcionamento da plataforma.	Cliente • Configure conexões de rede virtual com mais de um túnel sempre que possível para proteção contra interrupções.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
		• Mantenha o DNS de failover e o balanceamento de carga se estiver usando um balanceador de carga global com vários clusters.
Gerenciamento de computaçã o virtual	Red Hat • Monitore o cluster e substitua os nós do plano Amazon EC2 de controle ou da infraestrutura com falha. • Forneça ao cliente a capacidade de substituir manual ou automaticamente os nós de processamento que falharam.	Cliente • Substitua os nós de Amazon EC2 trabalho com falha editando a configura ção do pool de máquinas por meio OpenShift do Cluster Manager ou da ROSA CLI.
Gerenciamento de armazenamento virtual	Red Hat • Para ROSA clusters criados com credenciais de AWS IAM usuário, faça backup de todos os objetos do Kubernetes no cluster por meio de snapshots de volume de hora em hora, diariamente e semanalme nte.	Cliente • Faça backup de aplicaçõe s de clientes e dados de aplicações..

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
AWS software (AWS serviços públicos)	AWS Computação • Forneça Amazon EC2 recursos que ofereçam suporte à resiliência de dados, como Amazon EBS instantâneos e. Amazon EC2 Auto Scaling Para obter mais informaçõ es, consulte Resiliência Amazon EC2 no Guia do Amazon EC2 Usuário. Armazenamento • Forneça a capacidade para que o ROSA serviço e os clientes façam backup do Amazon EBS volume no cluster por meio de instantâneos de Amazon EBS volume. • Para obter informações sobre Amazon S3 recursos que oferecem suporte à resiliência de dados, consulte Resiliência em. Amazon S3 Redes • Para obter informaçõ es sobre Amazon VPC	Cliente • Configure clusters ROSA Multi-AZ para melhorar a tolerância a falhas e a disponibilidade do cluster. • Provisione volumes persistentes usando o driver Amazon EBS CSI para habilitar instantâneos de volume. • Crie instantâneos de volume CSI de volumes Amazon EBS persistentes.

Recurso	Responsabilidades de serviço	Responsabilidades do cliente
	recursos que oferecem suporte à resiliência de dados, consulte Resiliência Amazon Virtual Private Cloud no Guia do Amazon VPC usuário.	
Hardware/infraestrutura global AWS	AWS • Forneça uma infraestrutura AWS global que permita ROSA escalar o plano de controle, a infraestrutura e os nós de trabalho em todas as zonas de disponibilidade. Essa funcionalidade permite ROSA orquestrar o failover automático entre zonas sem interrupção. • Para obter mais informações sobre as melhores práticas de recuperação de desastres, consulte Opções de recuperação de desastres na nuvem no AWS Well-Architected Framework.	Cliente • Configure clusters ROSA Multi-AZ para melhorar a tolerância a falhas e a disponibilidade do cluster.

Responsabilidades do cliente por dados e aplicações

O cliente é responsável pelos aplicativos, cargas de trabalho e dados nos quais ele implementa. Serviço Red Hat OpenShift na AWS No entanto, AWS a Red Hat fornece várias ferramentas para ajudar o cliente a gerenciar dados e aplicativos na plataforma.

Recurso	Como AWS a Red Hat ajuda	Responsabilidades do cliente
Dados de cliente	Red Hat • Mantenha padrões em nível de plataforma para criptografia de dados, conforme definido pelos padrões de segurança e conformidade do setor. • Forneça OpenShift componentes para ajudar a gerenciar dados do aplicativo, como segredos. • Permita a integração com serviços Amazon RDS de dados, como armazenar e gerenciar dados fora do cluster e/ou AWS. AWS • Forneça Amazon RDS para permitir que os clientes armazenem e gerenciem dados fora do cluster.	Cliente • Mantenha a responsabilidade por todos os dados do cliente armazenados na plataforma e pela forma como as aplicações do cliente consomem e expõem esses dados.
Aplicações personalizadas	Red Hat • Provisione clusters com OpenShift componentes instalados para que os clientes possam acessar o OpenShift e o Kubernetes APIs para implantar e gerenciar aplicativos em contêineres.	Cliente • Mantenha a responsabilidade pelas aplicações e dados de clientes e de terceiros e pelo ciclo de vida completo da aplicação. • Se um cliente adicionar serviços da Red Hat, da comunidade, de terceiros

Recurso	Como AWS a Red Hat ajuda	Responsabilidades do cliente
	• Crie clusters com segredos de extração de imagens para que as implantações do cliente possam extrair imagens do registro do catálogo de contêiner da Red Hat. • Forneça acesso ao OpenShift APIs que um cliente pode usar para configurar operadores para adicionar serviços comunitários AWS, de terceiros e da Red Hat ao cluster. • Forneça classes de armazenamento e plug-ins para dar suporte a volumes persistentes para uso com aplicações do cliente. • Forneça um registro de imagens de contêiner para que os clientes possam armazenar com segurança imagens de contêiner de aplicações no cluster para implantar e gerenciar aplicações. AWS • Amazon EBS Forneça suporte a volumes persistentes para uso com aplicativos do cliente.	, próprios ou outros serviços ao cluster usando operadores ou imagens externas, o cliente será responsável por esses serviços e por trabalhar com o provedor apropriado (incluindo a Red Hat) para solucionar problemas. quaisquer problemas. • Use as ferramentas e os recursos fornecidos para configurar e implantar ; manter-se atualizado; configurar solicitações e limites de recursos; dimensionar o cluster para ter recursos suficientes para executar aplicações; configurar permissões; integrar-se a outros serviços; gerenciar qualquer fluxo de imagem ou modelo implantado pelo cliente; servir externamente; salvar, fazer backup e restaurar dados; e, de outra forma, gerenciar suas cargas de trabalho altamente disponíveis e resilientes. • Mantenha a responsabilidade pelo monitoramento dos aplicativos executados Serviço Red Hat OpenShift

Recurso	Como AWS a Red Hat ajuda	Responsabilidades do cliente
	• Forneça suporte Amazon S3 ao provisionamento do Red Hat do registro de imagens de contêineres.	na AWS, incluindo a instalação e a operação de software para coletar métricas, criar alertas e proteger segredos no aplicativo.

ROSA arquitetura

Serviço Red Hat OpenShift na AWS (ROSA) tem as seguintes topologias de cluster:

- Plano de controle hospedado (HCP) - O plano de controle é hospedado na Red Hat Conta da AWS e gerenciado pela Red Hat. Os nós de trabalho são implantados no cliente Conta da AWS.
- Clássico — O plano de controle e os nós de trabalho são implantados no do Conta da AWS cliente.

O ROSA com HCP oferece uma arquitetura de plano de controle mais eficiente que ajuda a reduzir as taxas de AWS infraestrutura incorridas durante a execução ROSA e permite tempos de criação de clusters mais rápidos. Tanto o ROSA com HCP quanto o ROSA classic podem ser ativados no AWS ROSA console. Você tem a opção de selecionar qual arquitetura deseja usar ao provisionar ROSA clusters usando a ROSA CLI.

> **Note**
>
> - ROSA oferece certificações de conformidade FedRAMP High e HIPAA Qualified AWS GovCloud em arquiteturas de plano de controle clássicas e hospedadas. Para obter mais informações, consulte Conformidade na documentação da Red Hat.
> - ROSA oferece endpoints do Federal Information Processing Standard (FIPS) AWS GovCloud em arquiteturas de plano de controle clássicas e hospedadas.

Comparando o ROSA com o HCP e o ROSA classic

A tabela a seguir compara o ROSA com os modelos de arquitetura clássica HCP e ROSA.

	ROSA com HCP	ROSA classic
Hospedagem da infraestrutura do cluster	Os componentes do plano de controle, como etcd, servidor de API e oauth, são hospedados em um local de propriedade da Red Hat. Conta da AWS	Os componentes do plano de controle, como etcd, servidor de API e oauth, são hospedados em um local de propriedade do cliente. Conta da AWS
Amazon VPC	Os nós de trabalho se comunicam com o plano de controle AWS PrivateLink.	Os nós de trabalho e os nós do plano de controle são implantados na VPC do cliente.
AWS Identity and Access Management	Usa políticas AWS gerenciadas.	Usa políticas gerenciadas pelo cliente que são definidas pelo serviço.
Implantação em várias zonas	O plano de controle é implantado em várias zonas de disponibilidade (AZs).	O plano de controle pode ser implantado em uma única AZ ou em várias AZs.
Nodos de infraestrutura	Não usa nós de infraestrutura dedicados. Os componentes da plataforma são implantados nos nós de trabalho.	Usa dois nós dedicados Single-AZ ou três Multi-AZ para hospedar os componentes da plataforma.
OpenShift capacidades	O monitoramento da plataforma, o registro de imagens e o controlador de entrada são implantados nos nós de trabalho.	O monitoramento da plataforma, o registro de imagens e o controlador de entrada são implantados em nós de infraestrutura dedicados.
Atualizações de cluster	O plano de controle e cada pool de máquinas podem ser atualizados separadamente.	O cluster inteiro deve ser atualizado ao mesmo tempo.

	ROSA com HCP	ROSA classic
Amazon EC2 Pegada mínima	São necessárias duas Amazon EC2 instâncias para criar um cluster.	São necessárias sete Amazon EC2 instâncias Single-AZ ou nove Multi-AZ para criar um cluster.
Regiões da AWS	Para obter Região da AWS informações sobre disponibilidade, consulte Serviço Red Hat OpenShift na AWS endpoints e cotas no Guia de referência AWS geral.	Para obter Região da AWS informações sobre disponibilidade, consulte Serviço Red Hat OpenShift na AWS endpoints e cotas no Guia de referência AWS geral.

Comece com ROSA

Serviço Red Hat OpenShift na AWS (ROSA) é um serviço gerenciado que você pode usar para criar, escalar e implantar aplicativos em contêineres com a plataforma OpenShift corporativa Kubernetes da Red Hat. AWS

Você pode usar os guias a seguir para criar seu primeiro ROSA cluster, conceder acesso ao usuário, implantar seu primeiro aplicativo e aprender como revogar o acesso do usuário e excluir seu cluster.

- the section called “Criar um cluster ROSA HCP - CLI”- Crie seu primeiro ROSA com cluster HCP usando AWS STS e a ROSA CLI.
- the section called “Crie um cluster ROSA clássico - AWS PrivateLink ”- Crie seu primeiro cluster ROSA classic usando AWS PrivateLink.
- the section called “Crie um cluster ROSA clássico - CLI”- Crie seu primeiro cluster ROSA clássico usando AWS STS e a ROSA CLI.

Configurado para usar ROSA

Para preparar seu ambiente para criar um ROSA cluster, você precisa concluir as ações a seguir.

Pré-requisitos

Os pré-requisitos a seguir devem ser atendidos para permitir ROSA a criação de clusters.

- Instale e configure o mais recente AWS CLI. Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI.
- Instale e configure a CLI e a ROSA CLI mais recentes da OpenShift Container Platform. Para obter mais informações, consulte Introdução à ROSA CLI.
- Você deve ter as cotas de serviço necessárias definidas para Amazon EC2 Amazon VPC, Amazon EBS, e. Elastic Load Balancing AWS ou a Red Hat pode solicitar aumentos de cota de serviço em seu nome, conforme necessário para a resolução de problemas. Para ver as cotas de serviço necessárias ROSA, consulte Serviço Red Hat OpenShift na AWS endpoints e cotas na AWS Referência geral.
- Para receber AWS suporte ROSA, você deve habilitar os planos de suporte AWS Business, Enterprise On-Ramp ou Enterprise. A Red Hat pode solicitar AWS suporte em seu nome, conforme

necessário, para a resolução de problemas. Para obter mais informações, consulte the section called “Obter suporte”. Para habilitar Suporte, consulte a Suporte página.

- Se você estiver usando AWS Organizations para gerenciar Contas da AWS aquele host do ROSA serviço, a política de controle de serviços (SCP) da organização deve ser configurada para permitir que a Red Hat execute ações políticas listadas no SCP sem restrições. Para obter mais informações, consulte o the section called “AWS Organizations a política de controle de serviços nega as permissões necessárias AWS Marketplace”. Para obter mais informações sobre SCPs, consulte Políticas de controle de serviço (SCPs).
- Se implantar um ROSA cluster with AWS STS em um ativado Região da AWS que está desativado por padrão, você deve atualizar o token de segurança para a versão 2 para todas as regiões do Conta da AWS com o comando a seguir.

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

Para obter mais informações sobre como habilitar regiões, consulte o link: accounts/latest/reference/manage

Ativar ROSA e configurar AWS pré-requisitos

Para criar um ROSA cluster, você deve habilitar o ROSA serviço no AWS ROSA console. O AWS ROSA console verifica se você Conta da AWS tem as AWS Marketplace permissões necessárias, as cotas de serviço e a função vinculada ao serviço Elastic Load Balancing (ELB) chamada. `AWSServiceRoleForElasticLoadBalancing` Se algum desses pré-requisitos estiver ausente, o console fornecerá orientações sobre como configurar sua conta para atender aos pré-requisitos.

1. Navegue até o console do ROSA.
2. Escolha Conceitos básicos.
3. Na página Verificar ROSA pré-requisitos, selecione Eu concordo em compartilhar minhas informações de contato com a Red Hat.
4. Selecione Habilitar ROSA .
5. Depois que a página verificar se suas cotas de serviço atendem aos ROSA pré-requisitos e a função vinculada ao serviço ELB for criada, abra uma nova sessão de terminal para criar a primeira usando a CLI. ROSA cluster ROSA

Crie um ROSA com cluster HCP usando a CLI ROSA

As seções a seguir descrevem como começar a usar o ROSA com planos de controle hospedados (ROSA com HCP) usando AWS STS e a ROSA CLI. Para ver as etapas para criar um cluster ROSA com HCP usando o Terraform, consulte a documentação da Red Hat. Para saber mais sobre o provedor do Terraform para criar ROSA clusters, consulte a documentação do Terraform.

A ROSA CLI usa o `auto` modo ou `manual` modo para criar os IAM recursos e a configuração do OpenID Connect (OIDC) necessários para criar um. ROSA cluster`auto`O modo cria automaticamente as IAM funções e políticas necessárias e o provedor OIDC. `manual`O modo gera os AWS CLI comandos necessários para criar os IAM recursos manualmente. Ao usar o `manual` modo, você pode revisar os AWS CLI comandos gerados antes de executá-los manualmente. Com o modo `manual`, você também pode passar os comandos para outro administrador ou grupo em sua organização para que eles possam criar os recursos.

Os procedimentos neste documento usam o `auto` modo da ROSA CLI para criar os IAM recursos necessários e a configuração do OIDC para ROSA com HCP. Para obter mais opções para começar, consulteComece com ROSA .

Tópicos

Pré-requisitos

Conclua as ações de pré-requisito listadas em. the section called “Configurar”

Crie Amazon VPC arquitetura

O procedimento a seguir cria uma Amazon VPC arquitetura que pode ser usada para hospedar um cluster. Todos os cluster recursos estão hospedados na sub-rede privada. A sub-rede pública roteia o tráfego de saída da sub-rede privada por meio de um gateway NAT para a Internet pública. Este exemplo usa o bloco CIDR `10.0.0.0/16` para o Amazon VPC. No entanto, você pode escolher um bloco CIDR diferente. Para obter mais informações, consulte Dimensionamento da VPC.

> **Important**
>
> Se Amazon VPC os requisitos não forem atendidos, a criação do cluster falhará.

Example

Terraform

1. Instale a CLI do Terraform. Para obter mais informações, consulte as instruções de instalação na documentação do Terraform.
2. Abra uma sessão de terminal e clone o repositório VPC do Terraform.

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

3. Navegue até o diretório criado.

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

4. Inicie o arquivo Terraform.

   ```
   terraform init
   ```

   Depois de concluída, a CLI retorna uma mensagem de que o Terraform foi inicializado com sucesso.

5. Para criar um plano do Terraform com base no modelo existente, execute o comando a seguir. O Região da AWS deve ser especificado. Opcionalmente, você pode optar por especificar um nome de cluster.

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

   Depois que o comando é executado, um `rosa.tfplan` arquivo é adicionado ao `hypershift-tf` diretório. Para opções mais detalhadas, consulte o arquivo README do repositório Terraform VPC.

6. Aplique o arquivo de plano para criar a VPC.

```
terraform apply rosa.tfplan
```

   Depois de concluída, a CLI retornou uma mensagem de sucesso que verifica os recursos adicionados.

   a. (Opcional) Crie variáveis de ambiente para a sub-rede privada, pública e de pool de máquinas provisionada pelo Terraform IDs para usar ao criar seu cluster ROSA com HCP.

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

   b. (Opcional) Verifique se as variáveis de ambiente foram definidas corretamente.

```
echo $SUBNET_IDS
```

Amazon VPC console

1. Abra o console do Amazon VPC.
2. No painel da VPC, escolha Criar VPC.
3. Em Resources to create (Recursos a serem criados), escolha VPC and more (VPC e mais).
4. Mantenha a opção Geração automática de tags de nome selecionada para criar tags de nome para os recursos da VPC, ou desmarque-a para fornecer suas próprias tags de nome para os recursos da VPC.
5. Para o bloco IPv4 CIDR, insira um intervalo de IPv4 endereços para a VPC. Uma VPC deve ter um intervalo de IPv4 endereços.

6. (Opcional) Para oferecer suporte ao IPv6 tráfego, escolha bloco IPv6 CIDR, bloco CIDR fornecido pela Amazon IPv6 .
7. Deixe a locação como`Default`.
8. Em Número de zonas de disponibilidade (AZs), escolha o número que você precisa. Para implantações Multi-AZ, são ROSA necessárias três zonas de disponibilidade. Para escolher o AZs para suas sub-redes, expanda Personalizar. AZs

   > **Note**
   >
   > Alguns tipos de ROSA instância só estão disponíveis em algumas zonas de disponibilidade. Você pode usar o `rosa list instance-types` comando ROSA CLI para listar todos os tipos de ROSA instância disponíveis. Para verificar se um tipo de instância está disponível para uma determinada zona de disponibilidade, use o 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 suas sub-redes, escolha valores para Número de sub-redes públicas e Número de sub-redes privadas. Para escolher os intervalos de endereços IP para suas sub-redes, expanda Personalizar blocos CIDR de sub-redes.

   > **Note**
   >
   > ROSA com HCP requer que os clientes configurem pelo menos uma sub-rede pública e uma privada por Zona de Disponibilidade usada para criar clusters.

10. Para conceder aos recursos da sub-rede privada acesso à Internet pública por meio de IPv4, para gateways NAT, escolha o número AZs no qual criar gateways NAT. Em produção, recomendamos que você implante um gateway NAT em cada AZ com recursos que precisem de acesso à Internet pública.
11. (Opcional) Se você precisar acessar Amazon S3 diretamente da sua VPC, escolha VPC endpoints, S3 Gateway.
12. Deixe as opções de DNS padrão selecionadas. ROSA requer suporte a nomes de host DNS na VPC.

13 Expanda Tags adicionais, escolha Adicionar nova tag e adicione as seguintes chaves de tag. ROSA usa verificações automáticas de pré-voo que verificam se essas tags são usadas.

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

14 Escolha Criar VPC.

AWS CLI

1. Crie uma VPC com um bloco CIDR `10.0.0.0/16`.

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

O comando anterior retorna o ID da VPC. Veja a seguir um exemplo de saída.

```
vpc-1234567890abcdef0
```

2. Armazene o ID da VPC em uma variável de ambiente.

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

3. Crie uma `Name` tag para a VPC usando a variável de `VPC_ID` ambiente.

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

4. Habilite o suporte ao nome de host DNS na VPC.

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

5. Crie uma sub-rede pública e privada na VPC, especificando as zonas de disponibilidade em que os recursos devem ser criados.

> **Important**
>
> ROSA com HCP requer que os clientes configurem pelo menos uma sub-rede pública e uma privada por Zona de Disponibilidade usada para criar clusters. Para implantações Multi-AZ, são necessárias três zonas de disponibilidade. Se estes requisitos não forem atendidos, a criação do cluster falhará.

> **Note**
>
> Alguns tipos de ROSA instância só estão disponíveis em algumas zonas de disponibilidade. Você pode usar o `rosa list instance-types` comando ROSA CLI para listar todos os tipos de ROSA instância disponíveis. Para verificar se um tipo de instância está disponível para uma determinada zona de disponibilidade, use o 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. Armazene a sub-rede pública e privada IDs em variáveis de ambiente.

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

7. Crie as seguintes tags para suas sub-redes VPC. ROSA usa verificações automáticas de pré-voo que verificam se essas tags são usadas.

> **Note**
>
> Você deve marcar pelo menos uma sub-rede privada e, se aplicável, uma sub-rede 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. Crie um gateway de internet e uma tabela de rotas para o tráfego de saída. Crie uma tabela de rotas e um endereço IP elástico para tráfego 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. Armazene IDs as variáveis de ambiente.

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

10. Anexar o Gateway da Internet à VPC.

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

11. Associe a tabela de rotas públicas à sub-rede pública e configure o tráfego para rotear para o gateway da 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. Crie o gateway NAT e associe-o ao endereço IP elástico para habilitar o tráfego para a sub-rede privada.

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

13. Associe a tabela de rotas privadas à sub-rede privada e configure o tráfego para rotear para o gateway 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 implantações Multi-AZ, repita as etapas acima para configurar mais duas zonas de disponibilidade com sub-redes públicas e privadas.

Crie as IAM funções necessárias e a configuração do OpenID Connect

Antes de criar um cluster ROSA com HCP, você deve criar as IAM funções e políticas necessárias e a configuração do OpenID Connect (OIDC). Para obter mais informações sobre IAM funções e políticas do ROSA com HCP, consultethe section called “ AWS políticas gerenciadas”.

Esse procedimento usa o `auto` modo da ROSA CLI para criar automaticamente a configuração OIDC necessária para criar um ROSA com cluster HCP.

1. Crie as funções e políticas de IAM conta necessárias. O `--force-policy-creation` parâmetro atualiza todas as funções e políticas existentes que estejam presentes. Se não houver funções e políticas presentes, o comando cria esses recursos em vez de atualizá-los.

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

   > **Note**
   >
   > Se seu token de acesso off-line tiver expirado, a ROSA CLI exibirá uma mensagem de erro informando que seu token de autorização precisa ser atualizado. Para obter as etapas de solução de problemas, consultethe section called “Solucionar problemas de tokens de acesso off-line expirados na ROSA CLI”.

2. Crie a configuração do OpenID Connect (OIDC) que permite a autenticação do usuário no cluster. Essa configuração está registrada para ser usada com o OpenShift Cluster Manager (OCM).

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

3. Copie o ID de configuração do OIDC fornecido na saída da CLI ROSA . O ID de configuração do OIDC precisa ser fornecido posteriormente para criar o ROSA com o cluster HCP.
4. Para verificar as configurações do OIDC disponíveis para clusters associados à sua organização de usuário, execute o seguinte comando.

   ```
   rosa list oidc-config
   ```

5. Crie as funções de IAM operador necessárias, `<OIDC_CONFIG_ID>` substituindo-as pela ID de configuração do OIDC copiada anteriormente.

Example

> **Important**
>
> Você deve fornecer um prefixo <PREFIX_NAME> ao criar as funções de operador. Não fazer isso gerará um erro.

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

6. Para verificar se as funções do IAM operador foram criadas, execute o seguinte comando:

```
rosa list operator-roles
```

Crie um cluster ROSA com HCP usando a ROSA CLI e AWS STS

Você pode criar um ROSA com HCP cluster usando AWS Security Token Service (AWS STS) e o `auto` modo fornecido na ROSA CLI. Você tem a opção de criar um cluster com uma API e Ingress públicos ou uma API e Ingress privados.

Você pode criar uma cluster com uma única zona de disponibilidade (Single-AZ) ou várias zonas de disponibilidade (Multi-AZ). Em ambos os casos, o valor do CIDR da sua máquina deve coincidir com o valor do CIDR da sua VPC.

O procedimento a seguir usa o `rosa create cluster --hosted-cp` comando para criar um ROSA Single-AZ com cluster HCP. Para criar um Multi-AZ cluster, especifique `multi-az` no comando e na sub-rede privada IDs para cada sub-rede privada na qual você deseja implantar.

1. Crie um cluster do ROSA com HCP com um dos comandos a seguir.
   - Crie um cluster ROSA com HCP com API pública e entrada, especificando o nome do cluster, o prefixo da função do operador, o ID de configuração do OIDC e a sub-rede pública e 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>
     ```

- Crie um cluster ROSA com HCP com API e entrada privadas, especificando o nome do cluster, o prefixo da função do operador, o ID de configuração do OIDC e a sub-rede privada. IDs

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

2. Verifique o status do seu cluster.

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

> **Note**
>
> Se o processo de criação falhar ou o `State` campo não mudar para o status pronto após 10 minutos, consulteSolução de problemas.
> Para entrar em contato com Suporte o suporte da Red Hat para obter assistência, consultethe section called “Obter suporte”.

3. Acompanhe o progresso da cluster criação observando os registros do OpenShift instalador.

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

Configurar um provedor de identidade e conceder cluster acesso

ROSA inclui um OAuth servidor embutido. Depois que o seu cluster for criado, você deverá configurar OAuth para usar um provedor de identidade. Em seguida, você pode adicionar usuários ao provedor de identidade configurado para conceder a eles acesso ao seu cluster. Você pode conceder a esses usuários permissões `cluster-admin` ou `dedicated-admin` conforme necessário.

Você pode configurar diferentes tipos de provedores de identidade para o seu ROSA cluster. Os tipos compatíveis incluem GitHub Enterprise GitHub, Google GitLab, LDAP, OpenID Connect e provedores de identidade. HTPasswd

> **Important**
>
> O provedor de HTPasswd identidade é incluído somente para permitir a criação de um único usuário administrador estático. HTPasswd não é suportado como provedor de identidade de uso geral para. ROSA

O procedimento a seguir configura um provedor de GitHub identidade como exemplo. Para obter instruções sobre como configurar cada um dos tipos de provedores de identidade compatíveis, consulte Configurando provedores de identidade para AWS STS.

1. Navegue até github.com e faça login na sua GitHub conta.
2. Se você não tiver uma GitHub organização para usar para provisionamento de identidade cluster, crie uma. Para obter mais informações, consulte as etapas na GitHub documentação.
3. Usando o modo interativo da ROSA CLI, configure um provedor de identidade para seu cluster.

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

4. Siga as instruções de configuração na saída para restringir o cluster acesso aos membros da sua GitHub organização.

```
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. Abra a URL na saída, `<GITHUB_ORG_NAME>` substituindo-a pelo nome da sua GitHub organização.

6. Na página da GitHub web, escolha Registrar aplicativo para registrar um novo OAuth aplicativo em sua GitHub organização.
7. Use as informações da GitHub OAuth página para preencher os prompts `rosa create idp` interativos restantes executando o comando a seguir. Substitua `<GITHUB_CLIENT_ID>` e `<GITHUB_CLIENT_SECRET>` pelas credenciais do seu GitHub OAuth aplicativo.

```
...
? 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**
>
> Pode levar aproximadamente dois minutos para que a configuração do provedor de identidade se torne ativa. Se você configurou um `cluster-admin` usuário, pode correr `oc get pods -n openshift-authentication --watch` para observar a reimplantação OAuth dos pods com a configuração atualizada.

8. Verifique se o provedor de identidade está configurado corretamente.

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

Conceder acesso ao usuário a um cluster

Você pode conceder a um usuário acesso ao seu cluster adicionando-o ao provedor de identidade configurado.

O procedimento a seguir adiciona um usuário a uma GitHub organização que está configurada para provisionamento de identidade no cluster.

1. Navegue até github.com e faça login na sua GitHub conta.

2. Convide usuários que precisam de cluster acesso à sua GitHub organização. Para obter mais informações, consulte Convidar usuários para participar da sua organização na GitHub documentação.

Configurar permissões do **`cluster-admin`**

1. Conceda as permissões `cluster-admin` executando o seguinte comando. Substitua `<IDP_USER_NAME>` e `<CLUSTER_NAME>` pelo nome do usuário e do cluster.

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

2. Verifique se o usuário está listado como membro do grupo `cluster-admins`.

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

Configurar permissões do **`dedicated-admin`**

1. Conceda as permissões `dedicated-admin` usando o seguinte comando. `<CLUSTER_NAME>`Substitua `<IDP_USER_NAME>` e por seu usuário e cluster nome executando o comando a seguir.

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

2. Verifique se o usuário está listado como membro do grupo `cluster-admins`.

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

Acesse um cluster por meio do Red Hat Hybrid Cloud Console

Faça login no seu cluster por meio do Red Hat Hybrid Cloud Console.

1. Obtenha o URL do console para você cluster usando o comando a seguir. `<CLUSTER_NAME>`Substitua pelo nome do seu cluster.

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

2. Navegue até o URL do console na saída e faça login.

Na caixa de diálogo Fazer login com..., escolha o nome do provedor de identidade e conclua todas as solicitações de autorização apresentadas pelo seu provedor.

Implemente um aplicativo do Catálogo de Desenvolvedores

No console de nuvem híbrida da Red Hat, você pode implantar um aplicativo de teste do Catálogo do desenvolvedor e expô-lo com uma rota.

1. Navegue até o Console de nuvem híbrida da Red Hat e escolha o cluster no qual você deseja implantar o aplicativo.
2. Na página do cluster, escolha Abrir console.
3. Na perspectiva do administrador, escolha Início > Projetos > Criar projeto.
4. Insira um nome para seu projeto e, opcionalmente, adicione um nome de exibição e uma descrição.
5. Selecione Criar para criar o projeto.
6. Mude para a perspectiva do desenvolvedor e escolha +Adicionar. Certifique-se de que o projeto selecionado seja aquele que acabou de ser criado.
7. Na caixa de diálogo Catálogo do desenvolvedor, escolha Todos os serviços.
8. Na página Catálogo do desenvolvedor, escolha Idiomas > no JavaScriptmenu.
9. Escolha Node.js e, em seguida, escolha Criar aplicativo para abrir a página Criar Source-to-Image aplicativo.

> **Note**
>
> Talvez seja necessário escolher Limpar todos os filtros para exibir a opção Node.js.

10. Na seção Git, escolha Testar amostra.
11. No campo Nome, adicione um nome exclusivo.
12. Escolha Criar.

> **Note**
>
> O novo aplicativo leva alguns minutos para ser implantado.

13. Quando a implantação estiver concluída, escolha o URL da rota para o aplicativo.

Uma nova guia no navegador é aberta com uma mensagem semelhante à seguinte.

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

14. (Opcional) Exclua o aplicativo e limpe os recursos:

    a. Na perspectiva do Administrador, escolha Início > Projetos.

    b. Abra o menu de ação do seu projeto e escolha Excluir projeto.

Revogue as permissões **`cluster-admin`** de um usuário

1. Revogue as permissões `cluster-admin` usando o seguinte comando. `<CLUSTER_NAME>`Substitua `<IDP_USER_NAME>` e por seu usuário e cluster nome.

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

2. Verifique se o usuário não está listado como membro do grupo `cluster-admins`.

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

Revogue as permissões do **`dedicated-admin`** de um usuário

1. Revogue as permissões do `dedicated-admin` usando o seguinte comando. `<CLUSTER_NAME>`Substitua `<IDP_USER_NAME>` e por seu usuário e cluster nome.

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

2. Verifique se o usuário não está listado como membro do grupo `dedicated-admins`.

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

Revogar o acesso do usuário a um cluster

Você pode revogar o cluster acesso de um usuário do provedor de identidade removendo-o do provedor de identidade configurado.

Você pode configurar diferentes tipos de provedores de identidade para o seu cluster. O procedimento a seguir revoga o cluster acesso de um membro de uma GitHub organização.

1. Navegue até github.com e faça login na sua GitHub conta.
2. Remova o usuário da sua GitHub organização. Para obter mais informações, consulte Removendo um membro da sua organização na GitHub documentação.

Excluir um cluster e AWS STS recursos

Você pode usar a ROSA CLI para excluir uma cluster que usa AWS Security Token Service ()AWS STS. Você também pode usar a ROSA CLI para excluir as IAM funções e o provedor OIDC criados por. ROSA Para excluir as IAM políticas criadas por ROSA, você pode usar o IAM console.

> **Note**
>
> IAM as funções e políticas criadas por ROSA podem ser usadas por outros ROSA clusters na mesma conta.

1. Exclua o cluster e observe os registros. Substitua <CLUSTER_NAME> pelo nome ou ID do seu cluster.

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

> **Important**
>
> Você deve aguardar cluster a exclusão completa antes de remover as IAM funções, as políticas e o provedor OIDC. As perfis do IAM da conta são necessárias para excluir os recursos criados pelo instalador. As funções do operador IAM são necessárias para limpar os recursos criados pelos OpenShift operadores. Os operadores utilizam o provedor OIDC para autenticação.

2. Exclua o provedor OIDC que os cluster operadores usam para autenticar executando o comando a seguir.

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

3. Exclua as funções de operador específicas do cluster. IAM

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

4. Exclua os perfis do IAM da conta usando o comando a seguir. Substitua `<PREFIX>` pelo prefixo das perfis do IAM da conta a serem excluídas. Se você especificou um prefixo personalizado ao criar as perfis do IAM da conta, especifique o prefixo padrão `ManagedOpenShift`.

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

5. Exclua IAM as políticas criadas por ROSA.
   a. Fazer login no console do IAM.
   b. No menu à esquerda, em Gerenciamento de acesso, escolha Políticas.
   c. Selecione a política que deseja excluir e escolha Ações > Excluir.
   d. Insira o nome da política e escolha Excluir.
   e. Repita essa etapa para excluir cada uma das políticas do IAM para o cluster.

Crie um cluster ROSA clássico usando a ROSA CLI

As seções a seguir descrevem como começar a usar o ROSA classic AWS STS e a ROSA CLI. Para ver as etapas para criar um cluster ROSA clássico usando o Terraform, consulte a documentação da Red Hat. Para saber mais sobre o provedor do Terraform para criar ROSA clusters, consulte a documentação do Terraform.

A ROSA CLI usa o `auto` modo ou `manual` modo para criar os IAM recursos necessários para provisionar um. ROSA cluster`auto`O modo cria imediatamente as IAM funções e políticas necessárias e um provedor OpenID Connect (OIDC). `manual`o modo gera os AWS CLI comandos necessários para criar os IAM recursos. Ao usar o `manual` modo, você pode revisar os AWS CLI comandos gerados antes de executá-los manualmente. Com o modo `manual`, você também pode passar os comandos para outro administrador ou grupo em sua organização para que eles possam criar os recursos.

Para obter mais opções para começar, consulteComece com ROSA .

Tópicos

- Pré-requisitos
- Crie um cluster ROSA clássico usando a ROSA CLI e AWS STS
- Configurar um provedor de identidade e conceder cluster acesso

- Conceder acesso ao usuário a um cluster
- Configurar permissões do cluster-admin
- Configurar permissões do dedicated-admin
- Acesse um cluster por meio do Red Hat Hybrid Cloud Console
- Implemente um aplicativo do Catálogo de Desenvolvedores
- Revogue as permissões cluster-admin de um usuário
- Revogue as permissões do dedicated-admin de um usuário
- Revogar o acesso do usuário a um cluster
- Excluir um cluster e AWS STS recursos

Pré-requisitos

Conclua as ações de pré-requisito listadas em. the section called “Configurar”

Crie um cluster ROSA clássico usando a ROSA CLI e AWS STS

Você pode criar um ROSA clássico cluster usando a ROSA CLI e. AWS STS

1. Crie as funções e políticas de IAM conta necessárias usando `--mode auto` ou`--mode manual`.
   - ```
     rosa create account-roles --classic --mode auto
     ```
   - ```
     rosa create account-roles --classic --mode manual
     ```

     > **Note**
     >
     > Se seu token de acesso off-line tiver expirado, a ROSA CLI exibirá uma mensagem de erro informando que seu token de autorização precisa ser atualizado. Para obter as etapas de solução de problemas, consultethe section called “Solucionar problemas de tokens de acesso off-line expirados na ROSA CLI”.
2. Crie um cluster usando `--mode auto` ou`--mode manual`. `auto`O modo permite que você crie um cluster mais rapidamente. `manual`O modo solicita que você especifique configurações personalizadas para seu cluster.

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

  > **Note**
  >
  > Quando você especifica `--mode auto`, o `rosa create cluster` comando cria automaticamente as IAM funções de operador específicas do cluster e o provedor OIDC. Os operadores utilizam o provedor OIDC para autenticação.

  > **Note**
  >
  > Ao usar os `--mode auto` padrões, a OpenShift versão estável mais recente é instalada.

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

  > **Important**
  >
  > Se você habilitar a criptografia etcd no `manual` modo, incorrerá em uma sobrecarga de desempenho de aproximadamente 20%. A sobrecarga é resultado da introdução dessa segunda camada de criptografia, além da criptografia padrão do Amazon EBS que criptografa os volumes etcd.

  > **Note**
  >
  > Depois de executar o `manual` modo para criar o cluster, você precisa criar manualmente as funções do IAM do operador específico do cluster e o provedor OpenID Connect que os operadores do cluster usam para se autenticar.

3. Verifique o status do seu cluster.

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

> **Note**
>
> Se o processo de provisionamento falhar ou o `State` campo não mudar para o status pronto após 40 minutos, consulte. Solução de problemas Para entrar em contato com Suporte o suporte da Red Hat para obter assistência, consultethe section called “Obter suporte”.

4. Acompanhe o progresso da cluster criação observando os registros do OpenShift instalador.

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

Configurar um provedor de identidade e conceder cluster acesso

ROSA inclui um OAuth servidor embutido. Depois que o seu cluster for criado, você deverá configurar OAuth para usar um provedor de identidade. Em seguida, você pode adicionar usuários ao provedor de identidade configurado para conceder a eles acesso ao seu cluster. Você pode conceder a esses usuários permissões `cluster-admin` ou `dedicated-admin` conforme necessário.

Você pode configurar diferentes tipos de provedores de identidade para o seu ROSA cluster. Os tipos compatíveis incluem GitHub Enterprise GitHub, Google GitLab, LDAP, OpenID Connect e provedores de identidade. HTPasswd

> **Important**
>
> O provedor de HTPasswd identidade é incluído somente para permitir a criação de um único usuário administrador estático. HTPasswd não é suportado como provedor de identidade de uso geral para. ROSA

O procedimento a seguir configura um provedor de GitHub identidade como exemplo. Para obter instruções sobre como configurar cada um dos tipos de provedores de identidade compatíveis, consulte Configurando provedores de identidade para AWS STS.

1. Navegue até github.com e faça login na sua GitHub conta.
2. Se você não tiver uma GitHub organização para usar para provisionamento de identidade cluster, crie uma. Para obter mais informações, consulte as etapas na GitHub documentação.

3. Usando o modo interativo da ROSA CLI, configure um provedor de identidade para seu cluster.

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

4. Siga as instruções de configuração na saída para restringir o cluster acesso aos membros da sua GitHub organização.

```
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. Abra a URL na saída, <GITHUB_ORG_NAME> substituindo-a pelo nome da sua GitHub organização.
6. Na página da GitHub web, escolha Registrar aplicativo para registrar um novo OAuth aplicativo em sua GitHub organização.
7. Use as informações da GitHub OAuth página para preencher os prompts `rosa create idp` interativos restantes executando o comando a seguir. Substitua <GITHUB_CLIENT_ID> e <GITHUB_CLIENT_SECRET> pelas credenciais do seu GitHub OAuth aplicativo.

```
...
? 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**
>
> Pode levar aproximadamente dois minutos para que a configuração do provedor de identidade se torne ativa. Se você configurou um `cluster-admin` usuário, pode correr `oc get pods -n openshift-authentication --watch` para observar a reimplantação OAuth dos pods com a configuração atualizada.

8. Verifique se o provedor de identidade está configurado corretamente.

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

Conceder acesso ao usuário a um cluster

Você pode conceder a um usuário acesso ao seu cluster adicionando-o ao provedor de identidade configurado.

O procedimento a seguir adiciona um usuário a uma GitHub organização que está configurada para provisionamento de identidade no cluster.

1. Navegue até github.com e faça login na sua GitHub conta.
2. Convide usuários que precisam de cluster acesso à sua GitHub organização. Para obter mais informações, consulte Convidar usuários para participar da sua organização na GitHub documentação.

Configurar permissões do **`cluster-admin`**

1. Conceda as permissões `cluster-admin` executando o seguinte comando. Substitua `<IDP_USER_NAME>` e `<CLUSTER_NAME>` pelo nome do usuário e do cluster.

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

2. Verifique se o usuário está listado como membro do grupo `cluster-admins`.

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

Configurar permissões do **`dedicated-admin`**

1. Conceda as permissões `dedicated-admin` usando o seguinte comando. `<CLUSTER_NAME>`Substitua `<IDP_USER_NAME>` e por seu usuário e cluster nome executando o comando a seguir.

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

2. Verifique se o usuário está listado como membro do grupo `cluster-admins`.

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

Acesse um cluster por meio do Red Hat Hybrid Cloud Console

Depois de criar um usuário cluster administrador ou adicionar um usuário ao seu provedor de identidade configurado, você pode fazer login no seu cluster por meio do Red Hat Hybrid Cloud Console.

1. Obtenha o URL do console para você cluster usando o comando a seguir. `<CLUSTER_NAME>`Substitua pelo nome do seu cluster.

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

2. Navegue até o URL do console na saída e faça login.
   - Se você criou um `cluster-admin` usuário, faça login usando as credenciais fornecidas.
   - Se você configurou um provedor de identidade para o seu cluster, escolha o nome do provedor de identidade na caixa de diálogo Fazer login com... e conclua todas as solicitações de autorização apresentadas pelo seu provedor.

Implemente um aplicativo do Catálogo de Desenvolvedores

No console de nuvem híbrida da Red Hat, você pode implantar um aplicativo de teste do Catálogo do desenvolvedor e expô-lo com uma rota.

1. Navegue até o Console de nuvem híbrida da Red Hat e escolha o cluster no qual você deseja implantar o aplicativo.
2. Na página do cluster, escolha Abrir console.
3. Na perspectiva do administrador, escolha Início > Projetos > Criar projeto.
4. Insira um nome para seu projeto e, opcionalmente, adicione um nome de exibição e uma descrição.
5. Selecione Criar para criar o projeto.
6. Mude para a perspectiva do desenvolvedor e escolha +Adicionar. Certifique-se de que o projeto selecionado seja aquele que acabou de ser criado.
7. Na caixa de diálogo Catálogo do desenvolvedor, escolha Todos os serviços.
8. Na página Catálogo do desenvolvedor, escolha Idiomas > no JavaScriptmenu.
9. Escolha Node.js e, em seguida, escolha Criar aplicativo para abrir a página Criar Source-to-Image aplicativo.

> **Note**
>
> Talvez seja necessário escolher Limpar todos os filtros para exibir a opção Node.js.

10. Na seção Git, escolha Testar amostra.
11. No campo Nome, adicione um nome exclusivo.
12. Escolha Criar.

> **Note**
>
> O novo aplicativo leva alguns minutos para ser implantado.

13. Quando a implantação estiver concluída, escolha o URL da rota para o aplicativo.

    Uma nova guia no navegador é aberta com uma mensagem semelhante à seguinte.

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

14. (Opcional) Exclua o aplicativo e limpe os recursos:
    a. Na perspectiva do Administrador, escolha Início > Projetos.
    b. Abra o menu de ação do seu projeto e escolha Excluir projeto.

Revogue as permissões **`cluster-admin`** de um usuário

1. Revogue as permissões `cluster-admin` usando o seguinte comando. `<CLUSTER_NAME>`Substitua `<IDP_USER_NAME>` e por seu usuário e cluster nome.

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

2. Verifique se o usuário não está listado como membro do grupo `cluster-admins`.

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

Revogue as permissões do **`dedicated-admin`** de um usuário

1. Revogue as permissões do `dedicated-admin` usando o seguinte comando. `<CLUSTER_NAME>`Substitua `<IDP_USER_NAME>` e por seu usuário e cluster nome.

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

2. Verifique se o usuário não está listado como membro do grupo `dedicated-admins`.

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

Revogar o acesso do usuário a um cluster

Você pode revogar o cluster acesso de um usuário do provedor de identidade removendo-o do provedor de identidade configurado.

Você pode configurar diferentes tipos de provedores de identidade para o seu cluster. O procedimento a seguir revoga o cluster acesso de um membro de uma GitHub organização.

1. Navegue até github.com e faça login na sua GitHub conta.
2. Remova o usuário da sua GitHub organização. Para obter mais informações, consulte Removendo um membro da sua organização na GitHub documentação.

Excluir um cluster e AWS STS recursos

Você pode usar a ROSA CLI para excluir uma cluster que usa AWS Security Token Service ()AWS STS. Você também pode usar a ROSA CLI para excluir as IAM funções e o provedor OIDC criados por. ROSA Para excluir as IAM políticas criadas por ROSA, você pode usar o IAM console.

> **Important**
>
> IAM as funções e políticas criadas por ROSA podem ser usadas por outros ROSA clusters na mesma conta.

1. Exclua o cluster e observe os registros. Substitua `<CLUSTER_NAME>` pelo nome ou ID do seu cluster.

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

   > **Important**
   >
   > Você deve aguardar cluster a exclusão completa antes de remover as IAM funções, as políticas e o provedor OIDC. As perfis do IAM da conta são necessárias para excluir os recursos criados pelo instalador. As funções do operador IAM são necessárias para limpar os recursos criados pelos OpenShift operadores. Os operadores utilizam o provedor OIDC para autenticação.

2. Exclua o provedor OIDC que os cluster operadores usam para autenticar executando o comando a seguir.

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

3. Exclua as funções de operador específicas do cluster. IAM

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

4. Exclua os perfis do IAM da conta usando o comando a seguir. Substitua `<PREFIX>` pelo prefixo das perfis do IAM da conta a serem excluídas. Se você especificou um prefixo personalizado ao criar as perfis do IAM da conta, especifique o prefixo padrão `ManagedOpenShift`.

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

5. Exclua IAM as políticas criadas por ROSA.
   a. Fazer login no console do IAM.
   b. No menu à esquerda, em Gerenciamento de acesso, escolha Políticas.
   c. Selecione a política que deseja excluir e escolha Ações > Excluir.
   d. Insira o nome da política e escolha Excluir.
   e. Repita essa etapa para excluir cada uma das políticas do IAM para o cluster.

Crie um cluster ROSA clássico que usa AWS PrivateLink

Os clusters clássicos do ROSA podem ser implantados de algumas maneiras diferentes: públicos, privados ou privados com AWS PrivateLink. Para obter mais informações sobre o ROSA classic, consultethe section called “Arquitetura”. Para cluster configurações públicas e privadas, o OpenShift cluster tem acesso à Internet e a privacidade é definida nas cargas de trabalho do aplicativo na camada do aplicativo.

Se você precisar que as cargas de trabalho do aplicativo cluster e as do aplicativo sejam privadas, você pode configurar AWS PrivateLink com o ROSA classic. AWS PrivateLink é uma tecnologia altamente disponível e escalável ROSA usada para criar uma conexão privada entre o ROSA serviço e os recursos do cluster na conta do AWS cliente. Com isso AWS PrivateLink, a equipe de engenharia de confiabilidade de sites (SRE) da Red Hat pode acessar o cluster para fins de suporte e remediação usando uma sub-rede privada conectada ao endpoint do cluster. AWS PrivateLink

Para obter mais informações sobre AWS PrivateLink, consulte O que é AWS PrivateLink?

Tópicos

- Pré-requisitos
- Crie Amazon VPC arquitetura
- Crie um cluster ROSA clássico usando a ROSA CLI e AWS PrivateLink
- Configurar o AWS PrivateLink encaminhamento de DNS
- Configurar um provedor de identidade e conceder cluster acesso
- Conceder acesso ao usuário a um cluster
- Configurar permissões do cluster-admin

- Configurar permissões do dedicated-admin
- Acesse um cluster por meio do Red Hat Hybrid Cloud Console
- Implemente um aplicativo do Catálogo de Desenvolvedores
- Revogue as permissões cluster-admin de um usuário
- Revogue as permissões dedicated-admin de um usuário
- Revogar o acesso do usuário a um cluster
- Excluir um cluster e AWS STS recursos

Pré-requisitos

Conclua as ações de pré-requisito listadas em. the section called “Configurar”

Crie Amazon VPC arquitetura

O procedimento a seguir cria uma Amazon VPC arquitetura que pode ser usada para hospedar um cluster. Todos os cluster recursos estão hospedados na sub-rede privada. A sub-rede pública roteia o tráfego de saída da sub-rede privada por meio de um gateway NAT para a Internet pública. Este exemplo usa o bloco CIDR `10.0.0.0/16` para o Amazon VPC. No entanto, você pode escolher um bloco CIDR diferente. Para obter mais informações, consulte Dimensionamento da VPC.

> **Important**
>
> Se Amazon VPC os requisitos não forem atendidos, a criação do cluster falhará.

Example

Amazon VPC console

1. Abra o console do Amazon VPC.
2. No painel da VPC, escolha Criar VPC.
3. Em Resources to create (Recursos a serem criados), escolha VPC and more (VPC e mais).
4. Mantenha a opção Geração automática de tags de nome selecionada para criar tags de nome para os recursos da VPC, ou desmarque-a para fornecer suas próprias tags de nome para os recursos da VPC.

5. Para o bloco IPv4 CIDR, insira um intervalo de IPv4 endereços para a VPC. Uma VPC deve ter um intervalo de IPv4 endereços.
6. (Opcional) Para oferecer suporte ao IPv6 tráfego, escolha bloco IPv6 CIDR, bloco CIDR fornecido pela Amazon IPv6 .
7. Deixe a locação como`Default`.
8. Em Número de zonas de disponibilidade (AZs), escolha o número necessário. Para implantações Multi-AZ, são ROSA necessárias três zonas de disponibilidade. Para escolher o AZs para suas sub-redes, expanda Personalizar. AZs

   > **Note**
   >
   > Alguns tipos de ROSA instância só estão disponíveis em algumas zonas de disponibilidade. Você pode usar o `rosa list instance-types` comando ROSA CLI para listar todos os tipos de ROSA instância disponíveis. Para verificar se um tipo de instância está disponível para uma determinada zona de disponibilidade, use o 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 suas sub-redes, escolha valores para Número de sub-redes públicas e Número de sub-redes privadas. Para escolher os intervalos de endereços IP para suas sub-redes, expanda Personalizar blocos CIDR de sub-redes.

   > **Note**
   >
   > ROSA exige que os clientes configurem pelo menos uma sub-rede privada por zona de disponibilidade usada para criar clusters.

10. Para conceder aos recursos da sub-rede privada acesso à Internet pública por meio de IPv4, para gateways NAT, escolha o número AZs no qual criar gateways NAT. Em produção, recomendamos que você implante um gateway NAT em cada AZ com recursos que precisem de acesso à Internet pública.
11. (Opcional) Se você precisar acessar Amazon S3 diretamente da sua VPC, escolha VPC endpoints, S3 Gateway.

12 Deixe as opções de DNS padrão selecionadas. ROSA requer suporte a nomes de host DNS na VPC.

13 Escolha Criar VPC.

AWS CLI

1. Crie uma VPC com um bloco CIDR `10.0.0.0/16`.

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

O comando anterior retorna o ID da VPC. Veja a seguir um exemplo de saída.

```
vpc-1234567890abcdef0
```

2. Armazene o ID da VPC em uma variável de ambiente.

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

3. Crie uma `Name` tag para a VPC usando a variável de `VPC_ID` ambiente.

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

4. Habilite o suporte ao nome de host DNS na VPC.

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

5. Crie uma sub-rede pública e privada na VPC, especificando as zonas de disponibilidade em que os recursos devem ser criados.

> **Important**
>
> ROSA exige que os clientes configurem pelo menos uma sub-rede privada por zona de disponibilidade usada para criar clusters. Para implantações Multi-AZ, são necessárias

três zonas de disponibilidade. Se estes requisitos não forem atendidos, a criação do cluster falhará.

> **Note**
>
> Alguns tipos de ROSA instância só estão disponíveis em algumas zonas de disponibilidade. Você pode usar o `rosa list instance-types` comando ROSA CLI para listar todos os tipos de ROSA instância disponíveis. Para verificar se um tipo de instância está disponível para uma determinada zona de disponibilidade, use o 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. Armazene a sub-rede pública e privada IDs em variáveis de ambiente.

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

7. Crie um gateway de internet e uma tabela de rotas para o tráfego de saída. Crie uma tabela de rotas e um endereço IP elástico para tráfego 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. Armazene IDs as variáveis de ambiente.

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

9. Anexar o Gateway da Internet à VPC.

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

10. Associe a tabela de rotas públicas à sub-rede pública e configure o tráfego para rotear para o gateway da 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. Crie o gateway NAT e associe-o ao endereço IP elástico para habilitar o tráfego para a sub-rede privada.

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

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

12 Associe a tabela de rotas privadas à sub-rede privada e configure o tráfego para rotear para o gateway 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 implantações Multi-AZ, repita as etapas acima para configurar mais duas zonas de disponibilidade com sub-redes públicas e privadas.

Crie um cluster ROSA clássico usando a ROSA CLI e AWS PrivateLink

Você pode usar a ROSA CLI e AWS PrivateLink criar uma cluster com uma única zona de disponibilidade (Single-AZ) ou várias zonas de disponibilidade (Multi-AZ). Em ambos os casos, o valor do CIDR da sua máquina deve coincidir com o valor do CIDR da sua VPC.

O procedimento a seguir usa o `rosa create cluster` comando para criar um ROSA clássico cluster. Para criar um Multi-AZ cluster, especifique `--multi-az` no comando e selecione a sub-rede privada IDs que você deseja usar quando solicitado.

> **Note**
>
> Se você usa um firewall, deve configurá-lo para que ROSA possa acessar os sites necessários para funcionar.
> Para obter mais informações, consulte Requisitos para o uso de AWS PrivateLink clusters na documentação da Red Hat.

1. Crie as funções e políticas de IAM conta necessárias usando `--mode auto` ou`--mode manual`.

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

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

  > **Note**
  >
  > Se seu token de acesso off-line tiver expirado, a ROSA CLI exibirá uma mensagem de erro informando que seu token de autorização precisa ser atualizado. Para obter as etapas de solução de problemas, consultethe section called “Solucionar problemas de tokens de acesso off-line expirados na ROSA CLI”.

2. Crie um cluster executando um dos seguintes 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 criar um cluster que usa AWS PrivateLink com AWS Security Token Service (AWS STS) credenciais de curta duração, anexe `--sts --mode auto` ou `--sts --mode manual` ao final do comando. `rosa create cluster`

3. Crie as IAM funções de cluster operador seguindo as instruções interativas.

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

4. Crie o provedor OpenID Connect (OIDC) que os cluster operadores usam para autenticar.

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

5. Verifique o status do seu cluster.

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

> **Note**
>
> Pode levar até 40 minutos para que o cluster `State` campo mostre o `ready` status. Se o provisionamento falhar ou não aparecer `ready` após 40 minutos, consulte. Solução de problemas Para entrar em contato com Suporte o suporte da Red Hat para obter assistência, consultethe section called “Obter suporte”.

6. Acompanhe o progresso da cluster criação observando os registros do OpenShift instalador.

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

Configurar o AWS PrivateLink encaminhamento de DNS

Os clusters que usam AWS PrivateLink criam uma zona hospedada pública e uma zona hospedada privada em Route 53. Os registros na zona hospedada Route 53 privada só podem ser resolvidos na VPC à qual estão atribuídos.

A validação DNS-01 do Let's Encrypt requer uma zona pública para que certificados válidos e publicamente confiáveis possam ser emitidos para o domínio. Os registros de validação são excluídos após a conclusão da validação do Let's Encrypt. A zona ainda é necessária para emitir e renovar esses certificados, que geralmente são necessários a cada 60 dias. Embora essas zonas geralmente pareçam vazias, uma zona pública desempenha um papel crítico no processo de validação.

Para obter mais informações sobre zonas hospedadas AWS privadas, consulte Como trabalhar com zonas privadas. Para obter mais informações sobre zonas hospedadas, consulte Como trabalhar com zonas hospedadas.

Configurar um Route 53 Resolver endpoint de entrada

1. Para permitir registros como `api.<cluster_domain>` e `*.apps.<cluster_domain>` resolver fora da VPC, configure um endpoint de Route 53 Resolver entrada.

> **Note**
>
> Ao configurar um endpoint de entrada, é necessário especificar no mínimo dois endereços IP para redundância. É recomendável especificar endereços IP em pelo menos duas

zonas de disponibilidade. Opcionalmente, você pode especificar endereços IP adicionais nessas ou em outras zonas de disponibilidade.

2. Ao configurar o endpoint de entrada, selecione a VPC e as sub-redes privadas que foram usadas quando você criou o cluster.

Configure o encaminhamento de DNS para o cluster

Depois que o endpoint Route 53 Resolver interno estiver associado e operacional, configure o encaminhamento de DNS para que as consultas de DNS possam ser tratadas pelos servidores designados em sua rede.

1. Configure sua rede corporativa para encaminhar consultas de DNS para esses endereços IP do domínio de nível superior, como `drow-pl-01.htno.p1.openshiftapps.com`.
2. Se você estiver encaminhando consultas ao DNS de uma VPC para outra VPC, siga as instruções em Gerenciando regras de encaminhamento.
3. Se estiver configurando o servidor DNS de sua rede remota, consulte a documentação específica do seu servidor DNS para configurar o encaminhamento seletivo de DNS para o domínio do cluster instalado.

Configurar um provedor de identidade e conceder cluster acesso

ROSA inclui um OAuth servidor embutido. Depois que o seu ROSA cluster for criado, você deverá configurar OAuth para usar um provedor de identidade. Em seguida, você pode adicionar usuários ao provedor de identidade configurado para conceder a eles acesso ao seu cluster. Você pode conceder a esses usuários permissões `cluster-admin` ou `dedicated-admin` conforme necessário.

Você pode configurar diferentes tipos de provedores de identidade para o seu cluster. Os tipos compatíveis incluem GitHub Enterprise GitHub, Google GitLab, LDAP, OpenID Connect e provedores de identidade. HTPasswd

> **Important**
>
> O provedor de HTPasswd identidade é incluído somente para permitir a criação de um único usuário administrador estático. HTPasswd não é suportado como provedor de identidade de uso geral para. ROSA

O procedimento a seguir configura um provedor de GitHub identidade como exemplo. Para obter instruções sobre como configurar cada um dos tipos de provedores de identidade compatíveis, consulte Configurando provedores de identidade para AWS STS.

1. Navegue até github.com e faça login na sua GitHub conta.
2. Se você não tiver uma GitHub organização para usar para provisionamento de identidade ROSA cluster, crie uma. Para obter mais informações, consulte as etapas na GitHub documentação.
3. Usando o modo interativo da ROSA CLI, configure um provedor de identidade para seu cluster executando o comando a seguir.

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

4. Siga as instruções de configuração na saída para restringir o cluster acesso aos membros da sua GitHub organização.

```
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. Abra a URL na saída, <GITHUB_ORG_NAME> substituindo-a pelo nome da sua GitHub organização.
6. Na página da GitHub web, escolha Registrar aplicativo para registrar um novo OAuth aplicativo em sua GitHub organização.
7. Use as informações da GitHub OAuth página para preencher os prompts `rosa create idp` interativos restantes, substituindo <GITHUB_CLIENT_ID> e <GITHUB_CLIENT_SECRET> com as credenciais do seu aplicativo. 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**
>
> Pode levar cerca de dois minutos para que a configuração do provedor de identidade se torne ativa. Se você configurou um `cluster-admin` usuário, pode executar o `oc get pods -n openshift-authentication --watch` comando para observar a reimplantação OAuth dos pods com a configuração atualizada.

8. Verifique se o provedor de identidade foi configurado corretamente.

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

Conceder acesso ao usuário a um cluster

Você pode conceder a um usuário acesso ao seu cluster adicionando-o ao provedor de identidade configurado.

O procedimento a seguir adiciona um usuário a uma GitHub organização que está configurada para provisionamento de identidade no cluster.

1. Navegue até github.com e faça login na sua GitHub conta.
2. Convide usuários que precisam de cluster acesso à sua GitHub organização. Para obter mais informações, consulte Convidar usuários para participar da sua organização na GitHub documentação.

Configurar permissões do **`cluster-admin`**

1. Conceda as permissões `cluster-admin` usando o seguinte comando. Substitua `<IDP_USER_NAME>` e `<CLUSTER_NAME>` pelo nome do usuário e do cluster.

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

2. Verifique se o usuário está listado como membro do grupo `cluster-admins`.

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

Configurar permissões do **`dedicated-admin`**

1. Conceda as permissões `dedicated-admin` com o seguinte comando. `<CLUSTER_NAME>`Substitua `<IDP_USER_NAME>` e por seu usuário e cluster nome.

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

2. Verifique se o usuário está listado como membro do grupo `cluster-admins`.

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

Acesse um cluster por meio do Red Hat Hybrid Cloud Console

Depois de criar um usuário cluster administrador ou adicionar um usuário ao seu provedor de identidade configurado, você pode fazer login no seu cluster por meio do Red Hat Hybrid Cloud Console.

1. Obtenha o URL do console para você cluster usando o comando a seguir. `<CLUSTER_NAME>`Substitua pelo nome do seu cluster.

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

2. Navegue até o URL do console na saída e faça login.
   - Se você criou um `cluster-admin` usuário, faça login usando as credenciais fornecidas.
   - Se você configurou um provedor de identidade para o seu cluster, escolha o nome do provedor de identidade na caixa de diálogo Fazer login com... e conclua todas as solicitações de autorização apresentadas pelo seu provedor.

Implemente um aplicativo do Catálogo de Desenvolvedores

No console de nuvem híbrida da Red Hat, você pode implantar um aplicativo de teste do Catálogo do desenvolvedor e expô-lo com uma rota.

1. Navegue até o Console de nuvem híbrida da Red Hat e escolha o cluster no qual deseja implantar o aplicativo.
2. Na página do cluster, escolha Abrir console.
3. Na perspectiva do administrador, escolha Início > Projetos > Criar projeto.
4. Insira um nome para seu projeto e, opcionalmente, adicione um nome de exibição e uma descrição.
5. Selecione Criar para criar o projeto.
6. Mude para a perspectiva do desenvolvedor e escolha +Adicionar. Certifique-se de que o projeto selecionado seja aquele que acabou de ser criado.
7. Na caixa de diálogo Catálogo do desenvolvedor, escolha Todos os serviços.
8. Na página Catálogo do desenvolvedor, escolha Idiomas > no JavaScriptmenu.
9. Escolha Node.js e, em seguida, escolha Criar aplicativo para abrir a página Criar Source-to-Image aplicativo.

> **Note**
>
> Talvez seja necessário escolher Limpar todos os filtros para exibir a opção Node.js.

10. Na seção Git, escolha Testar amostra.

11. No campo Nome, adicione um nome exclusivo.
12. Escolha Criar.

> **Note**
>
> O novo aplicativo leva alguns minutos para ser implantado.

13. Quando a implantação estiver concluída, escolha o URL da rota para o aplicativo.

    Uma nova guia no navegador é aberta com uma mensagem semelhante à seguinte.

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

14. (Opcional) Exclua o aplicativo e limpe os recursos:
    a. Na perspectiva do Administrador, escolha Início > Projetos.
    b. Abra o menu de ação do seu projeto e escolha Excluir projeto.

Revogue as permissões **`cluster-admin`** de um usuário

1. Revogue as permissões `cluster-admin` usando o seguinte comando. `<CLUSTER_NAME>`Substitua `<IDP_USER_NAME>` e por seu usuário e cluster nome.

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

2. Verifique se o usuário não está listado como membro do grupo `cluster-admins`.

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

Revogue as permissões **`dedicated-admin`** de um usuário

1. Revogue as permissões `dedicated-admin` usando o seguinte comando. `<CLUSTER_NAME>`Substitua `<IDP_USER_NAME>` e por seu usuário e cluster nome.

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

2. Verifique se o usuário não está listado como membro do grupo `dedicated-admins`.

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

Revogar o acesso do usuário a um cluster

Você pode revogar o cluster acesso de um usuário do provedor de identidade removendo-o do provedor de identidade configurado.

Você pode configurar diferentes tipos de provedores de identidade para o seu cluster. O procedimento a seguir revoga o cluster acesso de um membro de uma GitHub organização.

1. Navegue até github.com e faça login na sua GitHub conta.
2. Remova o usuário da sua GitHub organização. Para obter mais informações, consulte Removendo um membro da sua organização na GitHub documentação.

Excluir um cluster e AWS STS recursos

Você pode usar a ROSA CLI para excluir uma cluster que usa AWS Security Token Service ()AWS STS. Você também pode usar a ROSA CLI para excluir as IAM funções e o provedor OIDC criados por. ROSA Para excluir as IAM políticas criadas por ROSA, você pode usar o IAM console.

> **Important**
>
> IAM funções e políticas criadas por ROSA podem ser usadas por outros ROSA clusters na mesma conta.

1. Exclua o cluster e observe os registros. Substitua <CLUSTER_NAME> pelo nome ou ID do seu cluster.

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

> **Important**
>
> Você deve aguardar cluster a exclusão completa antes de remover as IAM funções, as políticas e o provedor OIDC. As perfis do IAM da conta são necessárias para excluir os recursos criados pelo instalador. As funções do operador IAM são necessárias para limpar

os recursos criados pelos OpenShift operadores. Os operadores utilizam o provedor OIDC para autenticação.

2. Exclua o provedor OIDC que os cluster operadores usam para autenticar executando o comando a seguir.

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

3. Exclua as funções de operador específicas do cluster. IAM

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

4. Exclua os perfis do IAM da conta usando o comando a seguir. Substitua `<PREFIX>` pelo prefixo das perfis do IAM da conta a serem excluídas. Se você especificou um prefixo personalizado ao criar as perfis do IAM da conta, especifique o prefixo padrão `ManagedOpenShift`.

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

5. Exclua IAM as políticas criadas por ROSA.
   a. Fazer login no console do IAM.
   b. No menu à esquerda, em Gerenciamento de acesso, escolha Políticas.
   c. Selecione a política que deseja excluir e escolha Ações **>** Excluir.
   d. Insira o nome da política e escolha Excluir.
   e. Repita essa etapa para excluir cada uma das políticas do IAM para o cluster.

Segurança em ROSA

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade aplicáveis ROSA, consulte Serviços da AWS Escopo por Programa de Conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar ROSA. Ele mostra como configurar para atender ROSA aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros Serviços da AWS que o ajudem a monitorar e proteger seus ROSA recursos.

Conteúdo

Proteção de dados em ROSA

A the section called “Responsabilidades” documentação e o modelo de responsabilidade AWS compartilhada definem a proteção de dados em ROSA. AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. A Red Hat é responsável por proteger a infraestrutura do cluster e a plataforma de serviços subjacente. O cliente é responsável por manter

o controle sobre o conteúdo hospedado nesta infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança do Serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços de segurança gerenciados avançados Amazon Macie, como, que ajudam a descobrir e proteger dados confidenciais armazenados em. Amazon S3
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de conta dos seus clientes, em campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com ROSA ou Serviços da AWS usa o console, a API ou AWS SDKs. AWS CLI Todos os dados que você inserir ROSA ou outros serviços podem ser coletados para inclusão nos registros de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar a solicitação a esse servidor.

Tópicos

- Proteção de dados usando criptografia

Proteção de dados usando criptografia

A proteção de dados se refere à proteção de dados em trânsito (à medida que viajam de e para lá ROSA) e em repouso (enquanto são armazenados em discos em data AWS centers).

Serviço Red Hat OpenShift na AWS fornece acesso seguro a Amazon Elastic Block Store (Amazon EBS) volumes de armazenamento anexados a Amazon EC2 instâncias para plano de ROSA controle, infraestrutura e nós de trabalho, bem como volumes persistentes do Kubernetes para armazenamento persistente. ROSA criptografa dados de volume em repouso e em trânsito e usa AWS Key Management Service (AWS KMS) para ajudar a proteger seus dados criptografados. O serviço usa Amazon S3 para armazenamento de registro de imagens de contêiner, que é criptografado em repouso por padrão.

> **Important**
>
> Porque ROSA é um serviço gerenciado, AWS e a Red Hat gerencia a infraestrutura que ROSA usa. Os clientes não devem tentar desligar manualmente as Amazon EC2 instâncias que ROSA usam a partir do AWS console ou da CLI. Essa ação pode levar à perda de dados do cliente.

Criptografia de dados para Amazon EBS volumes de armazenamento garantidos

Serviço Red Hat OpenShift na AWS usa a estrutura de volume persistente (PV) do Kubernetes para permitir que administradores de cluster provisionem um cluster com armazenamento persistente. Os volumes persistentes, bem como o plano de controle, a infraestrutura e os nós de trabalho, são apoiados por Amazon Elastic Block Store (Amazon EBS) volumes de armazenamento anexados às Amazon EC2 instâncias.

Para volumes ROSA persistentes e nós apoiados por Amazon EBS, as operações de criptografia ocorrem nos servidores que hospedam instâncias do EC2, garantindo a segurança dos dados em repouso e dos dados em trânsito entre uma instância e seu armazenamento conectado. Para obter mais informações, consulte Amazon EBS criptografia no Guia Amazon EC2 do usuário.

Criptografia de dados para o driver Amazon EBS CSI e o driver Amazon EFS CSI

ROSA o padrão é usar o driver Amazon EBS CSI para provisionar o armazenamento. Amazon EBS O driver Amazon EBS CSI e o operador do driver Amazon EBS CSI são instalados no cluster por padrão no `openshift-cluster-csi-drivers` namespace. O driver e o operador Amazon EBS

CSI permitem que você provisione dinamicamente volumes persistentes e crie instantâneos de volume.

ROSA também é capaz de provisionar volumes persistentes usando o driver Amazon EFS CSI e o operador do driver Amazon EFS CSI. O Amazon EFS driver e o operador também permitem que você compartilhe dados do sistema de arquivos entre pods ou com outros aplicativos dentro ou fora do Kubernetes.

Os dados do volume são protegidos em trânsito tanto para o driver Amazon EBS CSI quanto para o driver Amazon EFS CSI. Para obter mais informações, consulte Usando a Container Storage Interface (CSI) na documentação da Red Hat.

> **Important**
>
> Ao provisionar dinamicamente volumes ROSA persistentes usando o driver Amazon EFS CSI, Amazon EFS considere o ID do usuário, o ID do grupo (GID) e o grupo secundário do ponto de acesso ao avaliar as IDs permissões do sistema de arquivos. Amazon EFS substitui o usuário e o grupo IDs nos arquivos pelo usuário e grupo IDs no ponto de acesso e ignora o cliente NFS. IDs Como resultado, ignora Amazon EFS `fsGroup` silenciosamente as configurações. ROSA não é capaz de substituir os arquivos GIDs of usando`fsGroup`. Qualquer pod que possa acessar um ponto de Amazon EFS acesso montado pode acessar qualquer arquivo no volume. Para obter mais informações, consulte Trabalhando com pontos de Amazon EFS acesso no Guia Amazon EFS do usuário.

criptografia etcd

ROSA fornece a opção de habilitar a criptografia de `etcd` valores-chave dentro do `etcd` volume durante a criação do cluster, adicionando uma camada adicional de criptografia. Depois de `etcd` criptografado, você incorrerá em aproximadamente 20% de sobrecarga adicional de desempenho. Recomendamos que você ative a `etcd` criptografia somente se precisar dela especificamente para seu caso de uso. Para obter mais informações, consulte criptografia etcd na definição do ROSA serviço.

Gerenciamento de chaves

ROSA usa KMS keys para gerenciar com segurança o plano de controle, a infraestrutura e os volumes de dados do trabalhador e volumes persistentes para aplicativos de clientes. Durante a criação do cluster, você tem a opção de usar a chave AWS gerenciada padrão KMS key fornecida

por Amazon EBS ou especificar sua própria chave gerenciada pelo cliente. Para obter mais informações, consulte the section called “Gerenciamento de chaves”.

Criptografia de dados para o registro de imagens integrado

ROSA fornece um registro de imagens de contêiner integrado para armazenar, recuperar e compartilhar imagens de contêiner por meio do armazenamento em Amazon S3 bucket. O registro é configurado e gerenciado pelo Operador de Registro de OpenShift Imagens. Ele fornece uma out-of-the-box solução para os usuários gerenciarem as imagens que executam suas cargas de trabalho e são executadas sobre a infraestrutura de cluster existente. Para mais informações, consulte o tópico Registro na documentação da Red Hat.

ROSA oferece registros de imagens públicos e privados. Para aplicações empresariais, recomendamos o uso de um registro privado para proteger suas imagens contra o uso por usuários não autorizados. Para proteger os dados do seu registro em repouso, ROSA usa criptografia do lado do servidor por padrão com chaves Amazon S3 gerenciadas (SSE-S3). Isso não requer nenhuma ação da sua parte e é oferecido sem custo adicional. Para obter mais informações, consulte Proteção de dados usando criptografia do lado do servidor com chaves de criptografia Amazon S3 gerenciadas (SSE-S3) no Guia do usuário. Amazon S3

ROSA usa o protocolo Transport Layer Security (TLS) para proteger dados em trânsito de e para o registro de imagens. Para mais informações, consulte o tópico Registro na documentação da Red Hat.

Privacidade do tráfego entre redes

Serviço Red Hat OpenShift na AWS usa Amazon Virtual Private Cloud (Amazon VPC) para criar limites entre os recursos em seu ROSA cluster e controlar o tráfego entre eles, sua rede local e a Internet. Para obter mais informações sobre Amazon VPC segurança, consulte Privacidade do tráfego entre redes Amazon VPC no Guia do Amazon VPC usuário.

Na VPC, você pode configurar seus ROSA clusters para usar um servidor proxy HTTP ou HTTPS para negar acesso direto à Internet. Se você for administrador de cluster, também poderá definir políticas de rede no nível do pod que restrinjam o tráfego entre redes aos pods do seu ROSA cluster. Para obter mais informações, consulte the section called “Segurança da infraestrutura”.

Criptografia de dados usando KMS

ROSA usa AWS KMS para gerenciar com segurança as chaves dos dados criptografados.
Os volumes do plano de controle, da infraestrutura e do nó de trabalho são criptografados por

padrão usando o AWS gerenciado KMS key fornecido por Amazon EBS. Isso KMS key tem o pseudônimo`aws/ebs`. Os volumes persistentes que usam a classe de armazenamento gp3 padrão também são criptografados por padrão usando esse KMS key.

Os ROSA clusters recém-criados são configurados para usar a classe de armazenamento gp3 padrão para criptografar volumes persistentes. Os volumes persistentes criados usando qualquer outra classe de armazenamento só serão criptografados se a classe de armazenamento estiver configurada para ser criptografada. Para obter mais informações sobre classes de armazenamento ROSA pré-criadas, consulte Configurando o armazenamento persistente na documentação da Red Hat.

Durante a criação do cluster, você pode optar por criptografar os volumes persistentes em seu cluster usando a chave padrão Amazon EBS fornecida ou especificar sua própria simetria gerenciada pelo cliente. KMS key Para obter mais informações sobre a criação de chaves, consulte Criação de chaves KMS de criptografia simétrica no Guia do AWS KMS desenvolvedor.

Você também pode criptografar volumes persistentes para contêineres individuais em um cluster definindo um KMS key. Isso é útil quando você tem diretrizes explícitas de conformidade e segurança ao implantar no. AWS Para obter mais informações, consulte Criptografando volumes persistentes de contêineres AWS com a KMS key na documentação da Red Hat.

Os seguintes pontos devem ser considerados ao criptografar os volumes persistentes usando os seus KMS keys.

- Quando você usa a criptografia KMS com a sua própria KMS key, a chave deve existir da Região da AWS mesma forma que o seu cluster.
- Há um custo associado à criação e ao uso do seu próprio KMS keys. Para obter mais informações, consulte Preços do AWS Key Management Service.

Gerenciamento de identidade e acesso para ROSA

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAM os administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar ROSA os recursos. IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz ROSA.

Usuário do serviço - Se você usar o ROSA serviço para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais ROSA recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se você não conseguir acessar um recurso no ROSA, consultethe section called “Solução de problemas”.

Administrador de serviços - Se você é responsável pelos ROSA recursos da sua empresa, provavelmente tem acesso total ROSA a. É seu trabalho determinar quais ROSA recursos e recursos seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos do IAM.

IAM administrador - Se você for IAM administrador, talvez queira saber detalhes sobre as políticas usadas para gerenciar o acesso ROSA a. Para ver exemplos de políticas ROSA baseadas em identidade que você pode usar em IAM, consulte. the section called “ ROSA exemplos de políticas baseadas em identidade”

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como usuário Conta da AWS raiz Usuário do IAM, ou assumindo uma IAM função.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. Centro de Identidade do AWS IAM (Centro de Identidade do IAM) usuários, a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook

são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do usuário AWS de login.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia IAM do usuário.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte o Guia do usuário da autenticação multifator no AWS IAM Identity Center (sucessor do AWS Single Sign-On) e Como usar a autenticação multifator (MFA) AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login único que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente o usuário raiz possa executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade.

Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o Centro de Identidade do AWS IAM. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no Guia do AWS usuário do IAM Identity Center (sucessor do AWS Single Sign-On).

Usuários do IAM e grupos

An Usuário do IAMé uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar Usuários do IAM credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo Usuários do IAM, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um IAM grupo é uma identidade que especifica uma coleção de Usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar uma Usuário do IAM (em vez de uma função) no Guia do usuário do IAM.

IAM funções

Uma IAM função é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um Usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma

URL personalizada. Para obter mais informações sobre métodos de uso de funções, consulte Como usar IAM funções no Guia do usuário do IAM.

IAM funções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado - Para atribuir permissões a uma identidade federada, você cria uma função e define permissões para a função. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões com uma função no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário AWS do IAM Identity Center (sucessor do AWS Single Sign-On).
- Usuário do IAM Permissões temporárias - Um Usuário do IAM pode assumir uma IAM função para assumir temporariamente diferentes permissões para uma tarefa específica.
- Acesso entre contas - Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Como as IAM funções diferem das políticas baseadas em recursos no Guia do usuário do IAM.
- Acesso entre serviços - Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos Amazon EC2 ou armazene objetos em Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) - Quando você usa uma função Usuário do IAM OR para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

  - Função de serviço - Uma função de serviço é uma IAM função que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamente IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
  - Função vinculada ao serviço - Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua IAM conta e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução Amazon EC2 - Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma Amazon EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na Amazon EC2 instância. Para atribuir uma AWS função a uma Amazon EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na Amazon EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em Amazon EC2 instâncias no Guia do usuário do IAM.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O

administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAM as políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como uma Usuário do IAM função ou grupo. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais atributos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3 . Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte ACLs. Para saber mais ACLs, consulte a visão geral da Lista de Controle de Acesso (ACL) no Guia do usuário do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões - Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (Usuário do IAM ou função). Você pode definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade da entidade e seus limites de permissões. As políticas baseadas em recursos que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) - SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada usuário Conta da AWS root. Para obter mais informações sobre Organizations e SCPs, consulte Políticas de controle de serviços (SCPs) no Guia AWS Organizations do Usuário.
- Políticas de sessão — as políticas de sessão são políticas avançadas enviadas como um parâmetro ao criar de forma programática uma sessão temporária para uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e as políticas da sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

ROSA exemplos de políticas baseadas em identidade

Por padrão, Usuários do IAM as funções não têm permissão para criar ou modificar AWS recursos. Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. Um IAM administrador deve criar IAM políticas que concedam aos usuários e funções permissão para realizar operações de API específicas nos recursos especificados de que precisam. O administrador deve então anexar essas políticas aos grupos Usuários do IAM ou grupos que exigem essas permissões.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de política JSON, consulte Criação de políticas na guia JSON no Guia do usuário do IAM.

Usando o ROSA console

Para se inscrever a ROSA partir do console, seu diretor do IAM deve ter as AWS Marketplace permissões necessárias. As permissões permitem que o diretor assine e cancele a inscrição na lista de ROSA produtos AWS Marketplace e visualize as AWS Marketplace assinaturas. Para adicionar as permissões necessárias, acesse o ROSA console e anexe a política AWS gerenciada `ROSAManageSubscription` ao seu diretor do IAM. Para saber mais sobre o `ROSAManageSubscription`, consulte the section called “AWS política gerenciada: ROSAManage Assinatura”.

Autorizando o ROSA com o HCP a gerenciar recursos AWS

O ROSA com planos de controle hospedados (HCP) usa políticas AWS gerenciadas com permissões necessárias para operação e suporte do serviço. Você usa a ROSA CLI ou o IAM console para anexar essas políticas às funções de serviço em seu. Conta da AWS

Para obter mais informações, consulte the section called “ AWS políticas gerenciadas”.

Autorizando o ROSA classic a gerenciar recursos AWS

O ROSA classic usa políticas de IAM gerenciadas pelo cliente com permissões predefinidas pelo serviço. Você usa a ROSA CLI para criar essas políticas e anexá-las às funções de serviço em seu. Conta da AWS ROSA exige que essas políticas sejam configuradas conforme definido pelo serviço para garantir a operação contínua e o suporte ao serviço.

> **Note**
>
> Você não deve alterar as políticas clássicas do ROSA sem antes consultar a Red Hat. Isso pode anular o contrato de nível de serviço de 99,95% de tempo de atividade do cluster da Red Hat. O ROSA com planos de controle hospedados usa políticas AWS gerenciadas com um conjunto mais limitado de permissões. Para obter mais informações, consulte the section called “ AWS políticas gerenciadas”.

Existem dois tipos de políticas gerenciadas pelo cliente para ROSA: políticas de conta e políticas de operadora. As políticas de conta são anexadas às IAM funções que o serviço usa para estabelecer uma relação de confiança com a Red Hat para suporte de engenharia de confiabilidade do site (SRE), criação de clusters e funcionalidade de computação. As políticas do operador são anexadas às IAM funções que OpenShift os operadores usam para operações de cluster relacionadas à entrada, armazenamento, registro de imagens e gerenciamento de nós. As políticas de conta são criadas uma vez por cluster Conta da AWS, enquanto as políticas do operador são criadas uma vez por cluster.

Para obter mais informações, consulte the section called “Políticas de conta clássicas do ROSA” e the section called “Políticas clássicas de operadoras do ROSA”.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita visualizar Usuários do IAM as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o. 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 conta clássicas do ROSA

Esta seção fornece detalhes sobre as políticas de conta que são necessárias para o ROSA classic. Essas permissões são necessárias para que o ROSA classic gerencie os AWS recursos nos quais os clusters são executados e habilite o suporte do Red Hat Site Reliability Engineer para clusters. Você pode atribuir um prefixo personalizado aos nomes das políticas, mas, caso contrário, essas políticas devem ser nomeadas conforme definido nesta página (por exemplo,`ManagedOpenShift-Installer-Role-Policy`).

As políticas da conta são específicas para uma versão OpenShift menor e são compatíveis com versões anteriores. Antes de criar ou atualizar um cluster, você deve verificar se a versão da política e a versão do cluster são as mesmas executando`rosa list account-roles`. Se a versão da política for menor que a versão do cluster, execute `rosa upgrade account-roles` para atualizar as funções e as políticas anexadas. Você pode usar as mesmas políticas e funções de conta para vários clusters da mesma versão secundária.

[Prefixo] -Política da função do instalador

É possível anexar `[Prefix]-Installer-Role-Policy` às entidades do IAM. Antes de criar um cluster ROSA clássico, você deve primeiro anexar essa política a uma função do IAM chamada`[Prefix]-Installer-Role`. Essa política concede as permissões necessárias que permitem ao ROSA instalador gerenciar os AWS recursos necessários para a criação do cluster.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

```
{
    "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"
                }
            }
```

```
        }
    ]
}
```

[Prefixo] - ControlPlane -Role-Policy

É possível anexar `[Prefix]-ControlPlane-Role-Policy` às entidades do IAM. Antes de criar um cluster ROSA clássico, você deve primeiro anexar essa política a uma função do IAM chamada`[Prefix]-ControlPlane-Role`. Essa política concede as permissões necessárias ao ROSA classic para gerenciar Amazon EC2 Elastic Load Balancing recursos que hospedam o plano de ROSA controle, bem como para leitura KMS keys.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

```
{
    "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": "*"
        }
    ]
}
```

[Prefixo] -Política do papel do trabalhador

É possível anexar `[Prefix]-Worker-Role-Policy` às entidades do IAM. Antes de criar um cluster ROSA clássico, você deve primeiro anexar essa política a uma função do IAM chamada`[Prefix]-Worker-Role`. Essa política concede as permissões necessárias ao ROSA classic para descrever as instâncias do EC2 em execução como nós de trabalho.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

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

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

[Prefixo] - Política da função de suporte

É possível anexar `[Prefix]-Support-Role-Policy` às entidades do IAM. Antes de criar um cluster ROSA clássico, você deve primeiro anexar essa política a uma função do IAM chamada`[Prefix]-Support-Role`. Essa política concede as permissões necessárias à engenharia de confiabilidade do site da Red Hat para observar, diagnosticar e oferecer suporte aos AWS recursos que os clusters clássicos do ROSA usam, incluindo a capacidade de alterar o estado do nó do cluster.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

```
{
    "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*"
            ]
        }
    ]
}
```

Políticas clássicas de operadoras do ROSA

Esta seção fornece detalhes sobre as políticas do operador que são necessárias para o ROSA classic. Antes de criar um cluster ROSA clássico, você deve primeiro anexar essas políticas às funções relevantes do operador. É necessário um conjunto exclusivo de funções de operador para cada cluster.

Essas permissões são necessárias para permitir que os OpenShift operadores gerenciem os nós clássicos do cluster ROSA. Você pode atribuir um prefixo personalizado aos nomes das políticas para simplificar o gerenciamento de políticas (por exemplo,`ManagedOpenShift-openshift-ingress-operator-cloud-credentials`).

[Prefixo] - -credenciais openshift-ingress-operator-cloud

É possível anexar `[Prefix]-openshift-ingress-operator-cloud-credentials` às entidades do IAM. Essa política concede as permissões necessárias ao operador de entrada para provisionar e gerenciar balanceadores de carga e configurações de DNS para acesso externo ao cluster. A política também permite que o operador de entrada leia e filtre os valores das tags de Route 53 recursos para descobrir zonas hospedadas. Para obter mais informações sobre o operador, consulte Operador de OpenShift entrada na OpenShift GitHub documentação.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

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

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

É possível anexar `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` às entidades do IAM. Essa política concede as permissões necessárias ao operador do driver Amazon EBS CSI para instalar e manter o driver Amazon EBS CSI em um cluster ROSA classic. Para obter mais informações sobre o operador, consulte aws-ebs-csi-driver-operator na OpenShift GitHub documentação.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

```
{
    "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": "*"
        }
    ]
}
```

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

É possível anexar `[Prefix]-openshift-machine-api-aws-cloud-credentials` às entidades do IAM. Essa política concede as permissões necessárias ao Operador de Configuração da Máquina para descrever, executar e encerrar Amazon EC2 instâncias gerenciadas como nós de trabalho. Essa política também concede permissões para permitir a criptografia de disco do volume raiz do nó de trabalho usando AWS KMS keys. Para obter mais informações sobre o operador, consulte machine-config-operatora OpenShift GitHub documentação.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

```
{
    "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
                }
            }
```

```
        }
    ]
}
```

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

É possível anexar `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` às entidades do IAM. Essa política concede as permissões necessárias ao Cloud Credential Operator para recuperar Usuário do IAM detalhes, incluindo chave IDs de acesso, documentos de política em linha anexados, data de criação do usuário, caminho, ID do usuário e Amazon Resource Name (ARN). Para obter mais informações sobre o operador, consulte cloud-credential-operatora OpenShift GitHub documentação.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

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

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

É possível anexar `[Prefix]-openshift-image-registry-installer-cloud-credentials` às entidades do IAM. Essa política concede as permissões necessárias ao Operador de Registro de Imagens para provisionar e gerenciar recursos para o registro de imagens em cluster e serviços dependentes do ROSA classic, inclusive Amazon S3. Isso é necessário para que o operador possa instalar e manter o registro interno de um cluster ROSA classic. Para obter mais informações sobre o operador, consulte Operador de registro de imagens na OpenShift GitHub documentação.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

```
{
    "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": "*"
        }
    ]
}
```

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

É possível anexar `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` às entidades do IAM. Essa política concede as permissões necessárias ao Cloud Network Config Controller Operator para provisionar e gerenciar recursos de rede para uso pela sobreposição clássica de rede de cluster ROSA. O operador usa essas permissões para gerenciar endereços IP privados para Amazon EC2 instâncias como parte do cluster ROSA classic. Para obter mais

informações sobre o operador, consulte C loud-network-config-controller na OpenShift GitHub documentação.

Política de permissões

As permissões definidas neste documento de política especificam quais ações são permitidas ou negadas.

```
{
    "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 gerenciadas para ROSA

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades

principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes. Para obter mais informações, consulte políticas AWS gerenciadas no Guia IAM do usuário.

AWS política gerenciada: ROSAManage Assinatura

Você pode anexar a `ROSAManageSubscription` política às suas IAM entidades. Antes de habilitar ROSA no AWS ROSA console, você deve primeiro anexar essa política a uma função do IAM.

Essa política concede as AWS Marketplace permissões necessárias para você gerenciar a ROSA assinatura.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `aws-marketplace:Subscribe`- Concede permissão para assinar o AWS Marketplace produto para ROSA.
- `aws-marketplace:Unsubscribe`- Permite que os diretores removam assinaturas de produtos. AWS Marketplace
- `aws-marketplace:ViewSubscriptions`- Permite que os diretores visualizem as assinaturas de. AWS Marketplace Isso é necessário para que o IAM diretor possa ver as AWS Marketplace assinaturas disponíveis.

Para ver o documento completo da política JSON, consulte ROSAManageAssinatura no Guia de referência de políticas AWS gerenciadas.

ROSA com políticas de conta HCP

Esta seção fornece detalhes sobre as políticas de conta que são necessárias para o ROSA com planos de controle hospedados (HCP). Essas políticas AWS gerenciadas adicionam permissões usadas pelo ROSA com funções do HCP IAM. As permissões são necessárias para o suporte técnico da engenharia de confiabilidade de sites (SRE) da Red Hat, instalação de clusters, ambiente de gerenciamento e funcionalidade computacional.

> **Note**
>
> AWS as políticas gerenciadas devem ser usadas pelo ROSA com planos de controle hospedados (HCP). Os clusters clássicos do ROSA usam políticas de IAM gerenciadas pelo cliente. Para obter mais informações sobre as políticas clássicas do ROSA, consulte the section called “Políticas de conta clássicas do ROSA” the section called “Políticas clássicas de operadoras do ROSA” e.

AWS política gerenciada: ROSAWorker InstancePolicy

Você pode se conectar `ROSAWorkerInstancePolicy` às suas IAM entidades. Antes de criar um cluster, você deve ter uma função do IAM com essa política anexada. Um serviço ROSA faz chamadas para outras pessoas Serviços da AWS em seu nome. Eles fazem isso para gerenciar os recursos que você usa com cada cluster.

Detalhes das permissões

Essa política inclui as seguintes permissões que permitem que os nós de trabalho do ROSA concluam as seguintes tarefas:

- `ec2`— Avalie Região da AWS e Amazon EC2 instaure os detalhes como parte do gerenciamento do ciclo de vida do nó de trabalho do cluster ROSA.
- `ecr`- Avalie e obtenha imagens dos repositórios ECR gerenciados pela ROSA que são necessários para a instalação do cluster e o gerenciamento do ciclo de vida dos nós de trabalho.

Para ver o documento completo da política JSON, consulte o Guia ROSAWorkerInstancePolicyde referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSASRESupport Política

É possível anexar `ROSASRESupportPolicy` às entidades do IAM.

Antes de criar um cluster ROSA com planos de controle hospedados, você deve primeiro anexar essa política a uma função do IAM. Essa política concede as permissões necessárias aos engenheiros de confiabilidade de sites da Red Hat (SREs) para observar, diagnosticar e oferecer suporte diretamente aos AWS recursos associados aos ROSA clusters, incluindo a capacidade de alterar o estado do nó do ROSA cluster.

Detalhes das permissões

Essa política inclui as seguintes permissões que permitem que SREs a Red Hat conclua as seguintes tarefas:

- `cloudtrail`— Leia AWS CloudTrail eventos e trilhas relevantes para o cluster.
- `cloudwatch`— Leia Amazon CloudWatch métricas relevantes para o cluster.
- `ec2`— leia, descreva e analise Amazon EC2 os componentes relacionados à integridade do cluster, como grupos de segurança, conexões de endpoint VPC e status do volume. Inicie, interrompa, reinicie e encerre instâncias. Amazon EC2
- `elasticloadbalancing`— Leia, descreva e analise Elastic Load Balancing os parâmetros relacionados à integridade do cluster.
- `iam`— Avalie as IAM funções relacionadas à integridade do cluster.
- `route53` - Revise as configurações de DNS relacionadas à integridade do cluster.
- `sts`— `DecodeAuthorizationMessage` — Leia IAM mensagens para fins de depuração.

Para ver o documento completo da política JSON, consulte ROSASRESupportPolítica no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSAInstaller Política

Você pode se conectar `ROSAInstallerPolicy` às suas IAM entidades.

Antes de criar um cluster ROSA com planos de controle hospedados, você deve primeiro anexar essa política a uma função do IAM chamada`[Prefix]-ROSA-Worker-Role`. Essa política permite que as entidades adicionem qualquer função que siga o `[Prefix]-ROSA-Worker-Role` padrão a um perfil de instância. Essa política concede as permissões necessárias ao instalador para gerenciar AWS recursos que oferecem suporte à instalação ROSA do cluster.

Detalhes das permissões

Esta política inclui as seguintes permissões que permitem ao instalador realizar as seguintes tarefas:

- `ec2`— Execute Amazon EC2 instâncias usando AMIs sistemas hospedados Contas da AWS de propriedade e gerenciados pela Red Hat. Descreva Amazon EC2 instâncias, volumes e recursos de rede associados aos Amazon EC2 nós. Essa permissão é necessária para que o plano de controle do Kubernetes possa unir instâncias a um cluster e o cluster possa avaliar sua presença

nele. Amazon VPC Inspecione as reservas de capacidade do Amazon EC2 para oferecer suporte ao novo recurso de reservas de capacidade no ROSA. Marque e exclua tags em sub-redes usando a correspondência de chaves de tag. `"kubernetes.io/cluster/*"` Isso é necessário para garantir que o balanceador de carga usado para a entrada do cluster seja criado somente nas sub-redes aplicáveis e para gerenciar as tags de identificação do cluster do Kubernetes.

- `elasticloadbalancing` - Adicione balanceadores de carga aos nós de destino em um cluster. Remova balanceadores de carga aos nós de destino em um cluster. Essa permissão é necessária para que o plano de controle do Kubernetes possa provisionar dinamicamente os balanceadores de carga solicitados pelos serviços e serviços de aplicativos do Kubernetes. OpenShift
- `kms`— Leia uma AWS KMS chave, crie e gerencie doações e devolva uma chave de dados simétrica exclusiva para uso AWS KMS externo. Amazon EC2 Isso é necessário para o uso de dados `etcd` criptografados quando a `etcd` criptografia é habilitada na criação do cluster.
- `iam` - Valide as políticas e funções do IAM. Provisione e gerencie dinamicamente perfis de Amazon EC2 instância relevantes para o cluster. Adicione tags a um perfil de instância do IAM usando a permissão `iam:TagInstanceProfile`. Forneça mensagens de erro do instalador quando a instalação do cluster falhar devido à falta de um provedor OIDC de cluster especificado pelo cliente.
- `route53`— gerencie Route 53 os recursos necessários para criar clusters.
- `servicequotas` - Avalie as Service Quotas necessárias para criar um cluster.
- `sts`— Crie AWS STS credenciais temporárias para ROSA componentes. Suponha as credenciais para criação do cluster.
- `secretsmanager` - Leia um valor secreto para permitir com segurança a configuração OIDC gerenciada pelo cliente como parte do provisionamento do cluster.

Para ver o documento completo da política JSON, consulte ROSAInstallerPolítica no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSAShared VPCRoute53 Política

Você pode se conectar `ROSASharedVPCRoute53Policy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM para permitir que um cluster ROSA faça chamadas para outros Serviços da AWS em ambientes VPC compartilhados.

Essa política permite que o instalador do ROSA configure os registros do Route 53. Essa política deve ser usada em uma VPC compartilhada e fornece um subconjunto de permissões do Route 53 personalizadas para casos de uso de VPC compartilhada.

Detalhes das permissões

Essa política inclui as seguintes permissões que permitem que o instalador do ROSA conclua as seguintes tarefas:

- `route53`— Leia as informações da zona DNS e os registros DNS existentes para entender a configuração atual do DNS. Crie, modifique e exclua registros DNS, mas somente para padrões de domínio específicos relacionados ao ROSA`.hypershift.local`, incluindo,, `.openshiftapps.com.devshift.org`, e. `.openshiftusgov.com` `.devshiftusgov.com` Adicione, modifique ou remova tags nos recursos do Route 53 para gerenciamento e organização de recursos.
- `tag`— Descubra e liste AWS recursos com base em suas tags, o que é útil para identificar recursos gerenciados pelo ROSA.

Para ver mais detalhes sobre a política, incluindo a versão mais recente do documento de política JSON, consulte ROSASharedVPCRoute53Política no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSAShared VPCEndpoint Política

Você pode se conectar `ROSASharedVPCEndpointPolicy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM para permitir que um cluster ROSA faça chamadas para outros Serviços da AWS em ambientes VPC compartilhados.

Essa política permite que o instalador do ROSA configure endpoints de VPC e grupos de segurança em ambientes de VPC compartilhados.

Detalhes das permissões

Essa política inclui as seguintes permissões que permitem que o instalador do ROSA conclua as seguintes tarefas:

- `ec2`— Permissões somente de leitura para descrever recursos relacionados à VPC, incluindo endpoints da VPC e grupos de segurança VPCs, para entender o ambiente de rede. Crie, exclua e modifique grupos de segurança com restrições baseadas em tags, permitindo que o ROSA crie e gerencie grupos de segurança para redes de cluster e, ao mesmo tempo, restrinja as operações somente aos recursos marcados com o ROSA. Crie, modifique e exclua VPC endpoints com restrições baseadas em tags, permitindo que a ROSA crie e gerencie VPC endpoints para conectividade privada com ambientes VPC compartilhados. Serviços da AWS Aplique tags a

endpoints de VPC e grupos de segurança recém-criados durante a criação para identificação e gerenciamento adequados de recursos.

Para ver mais detalhes sobre a política, incluindo a versão mais recente do documento de política JSON, consulte ROSASharedVPCEndpointPolítica no Guia de referência de políticas AWS gerenciadas.

ROSA com políticas de operadores de HCP

Esta seção fornece detalhes sobre as políticas do operador que são necessárias para o ROSA com planos de controle hospedados (HCP). Você pode anexar essas políticas AWS gerenciadas às funções de operador necessárias para usar o ROSA com o HCP. As permissões são necessárias para permitir que OpenShift os operadores gerenciem o ROSA com os nós do cluster HCP.

> **Note**
>
> AWS as políticas gerenciadas devem ser usadas pelo ROSA com planos de controle hospedados (HCP). Os clusters clássicos do ROSA usam políticas de IAM gerenciadas pelo cliente. Para obter mais informações sobre as políticas clássicas do ROSA, consulte the section called “Políticas de conta clássicas do ROSA” the section called “Políticas clássicas de operadoras do ROSA” e.

AWS política gerenciada: ROSAAmazon EBSCSIDriver OperatorPolicy

Você pode se conectar `ROSAAmazonEBSCSIDriverOperatorPolicy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM do operador para permitir que um cluster ROSA com planos de controle hospedados faça chamadas para outro Serviços da AWS. É necessário um conjunto exclusivo de funções de operador para cada cluster.

Essa política concede as permissões necessárias ao operador do driver Amazon EBS CSI para instalar e manter o driver Amazon EBS CSI em um ROSA cluster. Para obter mais informações sobre o operador, consulte o aws-ebs-csi-driver operador na OpenShift GitHub documentação.

Detalhes das permissões

Essa política inclui as seguintes permissões que permitem ao operador do Amazon EBS motorista concluir as seguintes tarefas:

- `ec2`— crie, modifique, anexe, desanexe e exclua Amazon EBS volumes anexados às Amazon EC2 instâncias. Crie e exclua instantâneos de Amazon EBS volume e liste Amazon EC2 instâncias, volumes e instantâneos.

Para ver o documento completo da política JSON, consulte o Guia ROSAAmazonEBSCSIDriverOperatorPolicyde referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSAIngress OperatorPolicy

Você pode se conectar `ROSAIngressOperatorPolicy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM do operador para permitir que um cluster ROSA com planos de controle hospedados faça chamadas para outro Serviços da AWS. É necessário um conjunto exclusivo de funções de operador para cada cluster.

Essa política concede as permissões necessárias ao operador de entrada para provisionar e gerenciar balanceadores de carga e configurações de DNS para clusters. ROSA A política permite acesso de leitura aos valores das tags. Em seguida, o operador filtra os valores da tag em busca de Route 53 recursos para descobrir zonas hospedadas. Para obter mais informações sobre o operador, consulte Operador de OpenShift entrada na OpenShift GitHub documentação.

Detalhes das permissões

Esta política inclui as seguintes permissões que permitem que o operador de Ingress realize as seguintes tarefas:

- `elasticloadbalancing` - Descreva o estado dos balanceadores de carga provisionados.
- `route53`— Listar zonas Route 53 hospedadas e editar registros que gerenciam o DNS controlado pelo cluster ROSA.
- `tag` - Gerencie recursos marcados usando a permissão `tag:GetResources`.

Para ver o documento completo da política JSON, consulte o Guia ROSAIngressOperatorPolicyde referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSAImage RegistryOperatorPolicy

Você pode se conectar `ROSAImageRegistryOperatorPolicy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM do operador para permitir que um cluster ROSA com planos de controle hospedados faça chamadas para outro Serviços da AWS. É necessário um conjunto exclusivo de funções de operador para cada cluster.

Essa política concede as permissões necessárias ao operador de registro de imagens para provisionar e gerenciar recursos para o registro de imagens ROSA no cluster e serviços dependentes, incluindo o S3. Isso é necessário para que o operador possa instalar e manter o registro interno de um ROSA cluster. Para obter mais informações sobre o operador, consulte Operador de registro de imagens na OpenShift GitHub documentação.

Detalhes das permissões

Esta política inclui as seguintes permissões que permitem ao Operador de Registro de Imagens concluir as seguintes ações:

- `s3`— gerencie e avalie Amazon S3 buckets como armazenamento persistente para conteúdo de imagem de contêiner e metadados de cluster.

Para ver o documento completo da política JSON, consulte o Guia ROSAImageRegistryOperatorPolicyde referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSACloud NetworkConfigOperatorPolicy

Você pode se conectar `ROSACloudNetworkConfigOperatorPolicy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM do operador para permitir que um cluster ROSA com planos de controle hospedados faça chamadas para outro Serviços da AWS. É necessário um conjunto exclusivo de funções de operador para cada cluster.

Essa política concede as permissões necessárias ao Cloud Network Config Controller Operator para provisionar e gerenciar recursos de rede para a sobreposição de rede do ROSA cluster. O operador usa essas permissões para gerenciar endereços IP privados para Amazon EC2 instâncias como parte do ROSA cluster. Para obter mais informações sobre o operador, consulte C loud-network-config-controller na OpenShift GitHub documentação.

Detalhes das permissões

Esta política inclui as seguintes permissões que permitem que o operador de ambiente de gerenciamento realize as seguintes tarefas:

- `ec2`— Leia, atribua e descreva configurações para conectar Amazon EC2 instâncias, Amazon VPC sub-redes e interfaces de rede elástica em um cluster. ROSA

Para ver o documento completo da política JSON, consulte o Guia ROSACloudNetworkConfigOperatorPolicyde referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSAKube ControllerPolicy

Você pode se conectar `ROSAKubeControllerPolicy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM do operador para permitir que um cluster ROSA com planos de controle hospedados faça chamadas para outro Serviços da AWS. É necessário um conjunto exclusivo de funções de operador para cada cluster.

Essa política concede as permissões necessárias ao controlador kube para gerenciar Amazon EC2 e AWS KMS os recursos para um cluster ROSA com planos de controle hospedados. Elastic Load Balancing Para obter mais informações sobre esse controlador, consulte Arquitetura do controlador na OpenShift documentação.

Detalhes das permissões

Esta política inclui as seguintes permissões que permitem que o controlador do kube (Kubernetes) execute as seguintes tarefas:

- `ec2`— Crie, exclua e adicione tags aos grupos de segurança da Amazon EC2 instância. Adicione regras de entrada ao grupo de segurança. Descreva zonas de disponibilidade, Amazon EC2 instâncias, tabelas de rotas VPCs, grupos de segurança e sub-redes.
- `elasticloadbalancing`— Crie e gerencie balanceadores de carga e suas políticas. Crie e gerencie ouvintes do balanceador de carga. Registre e cancele o registro de alvos com grupos-alvo e gerencie grupos-alvo. Registre e cancele o registro de Amazon EC2 instâncias com um balanceador de carga e adicione tags aos balanceadores de carga.
- `kms`— Recupere informações detalhadas sobre uma AWS KMS chave. Isso é necessário para o uso de dados `etcd` criptografados quando a `etcd` criptografia é habilitada na criação do cluster.

Para ver o documento completo da política JSON, consulte o Guia ROSAKubeControllerPolicyde referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSANode PoolManagementPolicy

Você pode se conectar `ROSANodePoolManagementPolicy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM do operador para permitir que um cluster ROSA com planos de controle hospedados faça chamadas para outros AWS serviços. É necessário um conjunto exclusivo de funções de operador para cada cluster.

Essa política concede as permissões necessárias ao NodePool controlador para descrever, executar e encerrar Amazon EC2 instâncias gerenciadas como nós de trabalho. Essa política também

concede permissões para permitir a criptografia de disco do volume raiz do nó de trabalho usando AWS KMS chaves, para marcar a interface de rede elástica que está conectada ao nó de trabalho e para acessar as reservas de capacidade do Amazon EC2. Para obter mais informações sobre esse controlador, consulte Arquitetura do controlador na OpenShift documentação.

Detalhes das permissões

Essa política inclui as seguintes permissões que permitem que o NodePool controlador conclua as seguintes tarefas:

- `ec2`— Execute Amazon EC2 instâncias usando AMIs sistemas hospedados Contas da AWS de propriedade e gerenciados pela Red Hat. Gerencie os ciclos de vida do EC2 no cluster. ROSA Crie e integre dinamicamente nós de trabalho com Elastic Load Balancing Amazon VPC, Route 53, Amazon EBS, e. Amazon EC2 Acesse e descreva as reservas de capacidade para apoiar o recurso de reserva de capacidade no ROSA.
- `iam`— Use Elastic Load Balancing por meio da função vinculada ao serviço chamada. `AWSServiceRoleForElasticLoadBalancing` Atribua funções aos perfis de Amazon EC2 instância.
- `kms`— Leia uma AWS KMS chave, crie e gerencie doações e devolva uma chave de dados simétrica exclusiva para uso AWS KMS externo. Amazon EC2 Isso é necessário para permitir a criptografia de disco do volume raiz do nó de processamento.

Para ver o documento completo da política JSON, consulte o Guia ROSANodePoolManagementPolicyde referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSAKMSProvider Política

Você pode se conectar `ROSAKMSProviderPolicy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM do operador para permitir que um cluster ROSA com planos de controle hospedados faça chamadas para outro Serviços da AWS. É necessário um conjunto exclusivo de funções de operador para cada cluster.

Essa política concede as permissões necessárias ao provedor de AWS criptografia integrado para gerenciar AWS KMS chaves que suportam criptografia `etcd` de dados. Essa política permite Amazon EC2 usar chaves KMS fornecidas pelo provedor de AWS criptografia para criptografar e `etcd` descriptografar dados. Para obter mais informações sobre esse provedor, consulte Provedor de AWS criptografia na documentação do Kubernetes GitHub .

Detalhes das permissões

Essa política inclui as seguintes permissões que permitem que o provedor de AWS criptografia conclua as seguintes tarefas:

- `kms`— Criptografe, descriptografe e recupere qualquer chave. AWS KMS Isso é necessário para o uso de dados `etcd` criptografados quando a `etcd` criptografia é habilitada na criação do cluster.

Para ver o documento completo da política JSON, consulte ROSAKMSProviderPolítica no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: ROSAControl PlaneOperatorPolicy

Você pode se conectar `ROSAControlPlaneOperatorPolicy` às suas IAM entidades. Você deve anexar essa política a uma função do IAM do operador para permitir que um cluster ROSA com planos de controle hospedados faça chamadas para outro Serviços da AWS. É necessário um conjunto exclusivo de funções de operador para cada cluster.

Essa política concede as permissões necessárias ao Operador do Plano de Controle para gerenciar Amazon EC2 e Route 53 recursos para o ROSA com clusters de planos de controle hospedados. Para obter mais informações sobre esse operador, consulte Arquitetura do controlador na OpenShift documentação.

Detalhes das permissões

Esta política inclui as seguintes permissões que permitem que o operador de ambiente de gerenciamento realize as seguintes tarefas:

- `ec2`— Crie e gerencie Amazon VPC endpoints.
- `route53`— Listar e alterar conjuntos de Route 53 registros e listar zonas hospedadas.
- Tags adicionadas a RedHatManagedSecurityGroups: Permite que o operador do plano de controle marque grupos de segurança gerenciados pela Red Hat após a criação. Isso é necessário para o gerenciamento adequado do ciclo de vida dos recursos e a limpeza dos grupos de segurança associados ao ROSA com clusters de HCP.
- Grupo de segurança adicionado/* para gerenciar VPCEndpointWithCondition: corrige falhas de reconciliação do VPCE durante as atualizações do cluster. O operador precisa de permissão para modificar os VPC endpoints que fazem referência a grupos de segurança.

Para ver o documento completo da política JSON, consulte o Guia ROSAControlPlaneOperatorPolicyde referência de políticas AWS gerenciadas.

ROSA atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas ROSA desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico do documento.

Alteração	Descrição	Data
ROSAControlPlaneOperatorPolicy — Política atualizada	O ROSA atualizou a política para permitir a marcação de grupos de segurança gerenciados pela Red Hat para o gerenciamento adequado do ciclo de vida dos recursos e para adicionar security-group/* para gerenciar a correção de falhas de reconciliação do VPCE durante as atualizações do cluster. VPCEndpoint WithCondition Para saber mais, consulte the section called “AWS política gerenciada: ROSAControl PlaneOperatorPolicy”.	9 de abril de 2026
ROSAKubeControllerPolicy — Política atualizada	O ROSA atualizou a política para esclarecer as permissões do Elastic Load Balancing para registrar e cancelar o registro de alvos com grupos-alvo. Para saber mais, consulte the section called “AWS política gerenciada: ROSAKube ControllerPolicy”.	5 de março de 2026

Alteração	Descrição	Data
ROSANodePoolManagementPolicy — Política atualizada	ROSA atualizou a política para adicionar acesso a recursos para reservas de capacidade do Amazon EC2. Essa alteração permite que o NodePool controlador acesse e descreva as reservas de capacidade para melhorar o gerenciamento de recursos. Para saber mais, consulte the section called “AWS política gerenciada: ROSANodePoolManagementPolicy”.	3 de setembro de 2025
ROSASharedVPCEndpointPolítica — Nova política adicionada	ROSA adicionou uma nova política para permitir que o ROSA instalador configure endpoints de VPC e grupos de segurança em ambientes de VPC compartilhados. Essa política fornece um subconjunto de permissões do EC2 personalizadas para casos de uso de VPC compartilhados. Para saber mais, consulte the section called “AWS política gerenciada: ROSASharedVPCEndpoint Política”.	7 de agosto de 2025

Alteração	Descrição	Data
ROSASharedVPCRoute 53Política — Nova política adicionada	O ROSA adicionou uma nova política para permitir que o ROSA instalador configure registros do Route 53 em ambientes VPC compartil hados. Essa política fornece um subconjunto de permissõe s do Route 53 personalizadas para casos de uso de VPC compartilhados. Para saber mais, consulte the section called “AWS política gerenciad a: ROSAShared VPCRoute53 Política”.	7 de agosto de 2025
ROSAInstallerPolítica — Política atualizada	O ROSA atualizou a política para permitir que o ROSA instalador inspecione as reservas de capacidade do Amazon EC2 para dar suporte ao novo recurso de reservas de capacidade no ROSA. Essa atualização também permite que o instalador exclua tags em sub-redes usando a correspondência de chaves de tag `"kubernet es.io/cluster/*"` para melhorar o gerenciamento de tags do cluster Kubernetes. Para saber mais, consulte the section called “AWS política gerenciada: ROSAInstaller Política”.	7 de agosto de 2025

Alteração	Descrição	Data
ROSAImageRegistryOperatorPolicy — Política atualizada	O ROSA atualizou a política para que as permissões fossem reduzidas ao nível de recurso do bucket do S3. Essa alteração satisfaz os requisitos de armazenamento do ROSA para áreas AWS comerciais e GovCloud regionais. Para saber mais, consulte the section called “AWS política gerenciada: ROSAImage RegistryOperatorPolicy”.	19 de maio de 2025
ROSANodePoolManagementPolicy — Política atualizada	O ROSA atualizou a política para permitir a marcação da interface de rede elástica que está conectada ao nó de trabalho. Para saber mais, consulte the section called “AWS política gerenciada: ROSANode PoolManagementPolicy”.	5 de maio de 2025

Alteração	Descrição	Data
ROSAImageRegistryOperatorPolicy — Política atualizada	O ROSA atualizou a política para permitir que o Red Hat OpenShift Image Registry Operator provisione e gerencie buckets e objetos do Amazon S3 em AWS GovCloud regiões para uso pelo registro de imagens no cluster do ROSA. Essa alteração satisfaz os requisitos de armazenamento do ROSA para AWS GovCloud regiões. Para saber mais, consulte the section called “AWS política gerenciada: ROSAImageRegistryOperatorPolicy”.	16 de abril de 2025
ROSAWorkerInstancePolicy — Política atualizada	O ROSA atualizou a política para permitir que os nós de trabalho avaliem e obtenham imagens dos repositórios ECR gerenciados pela ROSA que são necessários para a instalação do cluster e o gerenciamento do ciclo de vida do nó de trabalho. Para saber mais, consulte the section called “AWS política gerenciada: ROSAWorkerInstancePolicy”.	3 de março de 2025

Alteração	Descrição	Data
ROSANodePoolManagementPolicy — Política atualizada	O ROSA atualizou a política para permitir que interfaces de rede elásticas sejam marcadas de forma semelhante às instâncias do EC2 somente durante RunInstances chamadas ec2: quando a solicitação inclui a tag. `red-hat-managed: true` Essas permissões são necessárias para oferecer suporte ao ROSA com clusters HCP 4.17. Para saber mais, consulte the section called “AWS política gerenciada: ROSANodePoolManagementPolicy”.	24 de fevereiro de 2025
ROSAAmazonEBSCSIDriverOperatorPolicy — Política atualizada	O ROSA atualizou a política para oferecer suporte à nova API de autorização de Amazon EBS snapshot. Para saber mais, consulte the section called “AWS política gerenciada: ROSAAmazon EBSCSIDriver OperatorPolicy”.	17 de janeiro de 2025

Alteração	Descrição	Data
ROSANodePoolManagementPolicy — Política atualizada	O ROSA atualizou a política para permitir que o gerenciador do pool de ROSA nós descreva os conjuntos de opções DHCP para definir os nomes DNS privados adequados. Para saber mais, consulte the section called “AWS política gerenciada: ROSANodePoolManagementPolicy”.	2 de maio de 2024
ROSAInstallerPolítica — Política atualizada	O ROSA atualizou a política para permitir que o ROSA instalador adicione tags às sub-redes usando chaves de tag correspondentes. `"kubernetes.io/cluster/*"` Para saber mais, consulte the section called “AWS política gerenciada: ROSAInstaller Política”.	24 de abril de 2024
ROSASRESupportPolítica — Política atualizada	O ROSA atualizou a política para permitir que a função SRE recupere informações sobre perfis de instância que foram marcados por ROSA como. `red-hat-managed` Para saber mais, consulte the section called “AWS política gerenciada: ROSASRESupport Política”.	10 de abril de 2024

Alteração	Descrição	Data
ROSAInstallerPolítica — Política atualizada	O ROSA atualizou a política para permitir que o ROSA instalador valide se as políticas AWS gerenciadas ROSA estão anexadas às IAM funções usadas por ROSA. Essa atualização também permite que o instalador identifique se as políticas gerenciadas pelo cliente foram anexadas às ROSA funções. Para saber mais, consulte the section called “AWS política gerenciada: ROSAInstaller Política”.	10 de abril de 2024
ROSAInstallerPolítica — Política atualizada	O ROSA atualizou a política para permitir que o serviço forneça mensagens de alerta ao instalador quando a instalação do cluster falhar devido à falta de um provedor OIDC de cluster especificado pelo cliente. Essa atualização também permite que o serviço recupere os servidores de nomes DNS existentes para que as operações de provision amento do cluster sejam idempotentes. Para saber mais, consulte the section called “AWS política gerenciada: ROSAInstaller Política”.	26 de janeiro de 2024

Alteração	Descrição	Data
ROSASRESupportPolítica — Política atualizada	ROSA atualizou a política para permitir que o serviço realize operações de leitura em grupos de segurança usando a DescribeSecurityGroups API. Para saber mais, consulte the section called “AWS política gerenciada: ROSASRESupport Política”.	22 de janeiro de 2024
ROSAImageRegistryOperatorPolicy — Política atualizada	ROSA atualizou a política para permitir que o operador de registro de imagens realize ações em Amazon S3 buckets em regiões com nomes de 14 caracteres. Para saber mais, consulte the section called “AWS política gerenciada: ROSAImage RegistryOperatorPolicy”.	12 de dezembro de 2023
ROSAKubeControllerPolicy — Política atualizada	ROSA atualizou a política para permitir kube-controller-manager a descrição de zonas de disponibilidade, Amazon EC2 instâncias, tabelas de rotas VPCs, grupos de segurança e sub-redes. Para saber mais, consulte the section called “AWS política gerenciada: ROSAKube ControllerPolicy”.	16 de outubro de 2023

Alteração	Descrição	Data
ROSAManageAssinatura — Política atualizada	ROSA atualizou a política para adicionar o ROSA com planos de controle hospedados ProductId. Para saber mais, consulte the section called “AWS política gerenciada: ROSAManage Assinatura”.	1º de agosto de 2023
ROSAKubeControllerPolicy — Política atualizada	ROSA atualizou a política para permitir a kube-controller-manager criação de balanceadores de carga de rede como balanceadores de carga de serviço Kubernetes. Os balanceadores de carga de rede oferecem maior capacidade de lidar com workloads voláteis e oferecem suporte a endereços IP estáticos para o balanceador de carga. Para saber mais, consulte the section called “AWS política gerenciada: ROSAKube ControllerPolicy”.	13 de julho de 2023

Alteração	Descrição	Data
ROSANodePoolManagementPolicy — Nova política adicionada	ROSA adicionou uma nova política para permitir que o NodePool controlador descreva, execute e encerre Amazon EC2 instâncias gerenciadas como nós de trabalho. Essa política também permite a criptografia de disco do volume raiz do nó de trabalho usando AWS KMS chaves. Para saber mais, consulte the section called “AWS política gerenciada: ROSANode PoolManagementPolicy”.	8 de junho de 2023
ROSAInstallerPolítica — Nova política adicionada	ROSA adicionou uma nova política para permitir que o instalador gerencie AWS recursos que oferecem suporte à instalação do cluster. Para saber mais, consulte the section called “AWS política gerenciada: ROSAInstaller Política”.	6 de junho de 2023

Alteração	Descrição	Data
ROSASRESupportPolítica — Nova política adicionada	ROSA adicionou uma nova política para permitir que SREs a Red Hat observe, diagnostique e ofereça suporte diretamente aos AWS recursos associados aos ROSA clusters, incluindo a capacidade de alterar o estado do nó do ROSA cluster. Para saber mais, consulte the section called “AWS política gerenciada: ROSASRESupport Política”.	1º de junho de 2023
ROSAKMSProviderPolítica — Nova política adicionada	ROSA adicionou uma nova política para permitir que o provedor de AWS criptografia integrado gerencie AWS KMS chaves para oferecer suporte à criptografia de dados etcd. Para saber mais, consulte the section called “AWS política gerenciada: ROSAKMSProvider Política”.	27 de abril de 2023

Alteração	Descrição	Data
ROSAKubeControllerPolicy — Nova política adicionada	ROSA adicionou uma nova política para permitir que o controlador kube Amazon EC2 gerencie e AWS KMS recursos para clusters de planos ROSA de controle hospedados. Elastic Load Balancing Para saber mais, consulte the section called “AWS política gerenciada: ROSAKube ControllerPolicy”.	27 de abril de 2023
ROSAImageRegistryOperatorPolicy — Nova política adicionada	ROSA adicionou uma nova política para permitir que o operador de registro de imagens provisione e gerencie recursos para o registro de imagens ROSA no cluster e serviços dependentes, incluindo o S3. Para saber mais, consulte the section called “AWS política gerenciada: ROSAImage RegistryOperatorPolicy”.	27 de abril de 2023

Alteração	Descrição	Data
ROSAControlPlaneOperatorPolicy — Nova política adicionada	ROSA adicionou uma nova política para permitir que o operador do plano de controle Amazon EC2 gerencie Route 53 os recursos ROSA com clusters de planos de controle hospedados. Para saber mais, consulte the section called “AWS política gerenciada: ROSAControlPlaneOperatorPolicy”.	24 de abril de 2023
ROSACloudNetworkConfigOperatorPolicy — Nova política adicionada	ROSA adicionou uma nova política para permitir que o Cloud Network Config Controller Operator provisione e gerencie recursos de rede para a sobreposição de rede do ROSA cluster. Para saber mais, consulte the section called “AWS política gerenciada: ROSACloud NetworkConfigOperatorPolicy”.	20 de abril de 2023
ROSAIngressOperatorPolicy — Nova política adicionada	ROSA adicionou uma nova política para permitir que o operador de entrada provisione e gerencie balanceadores de carga e configurações de DNS para clusters. ROSA Para saber mais, consulte the section called “AWS política gerenciada: ROSAIngressOperatorPolicy”.	20 de abril de 2023

Alteração	Descrição	Data
ROSAAmazonEBSCSIDriverOperatorPolicy — Nova política adicionada	ROSA adicionou uma nova política para permitir que o operador do driver Amazon EBS CSI instale e mantenha o driver Amazon EBS CSI em um ROSA cluster. Para saber mais, consulte the section called “AWS política gerenciada: ROSAAmazon EBSCSIDriver OperatorPolicy”.	20 de abril de 2023
ROSAWorkerInstancePolicy — Nova política adicionada	ROSA adicionou uma nova política para permitir que o serviço gerencie os recursos do cluster. Para saber mais, consulte the section called “AWS política gerenciada: ROSAWorker InstancePolicy”.	20 de abril de 2023
ROSAManageAssinatura — Nova política adicionada	ROSA adicionou uma nova política para conceder as AWS Marketplace permissões necessárias para gerenciar a ROSA assinatura. Para saber mais, consulte the section called “AWS política gerenciada: ROSAManage Assinatura”.	11 de abril de 2022
Serviço Red Hat OpenShift na AWS começou a rastrear as alterações	Serviço Red Hat OpenShift na AWS começou a rastrear as mudanças em suas políticas AWS gerenciadas.	2 de março de 2022

Solução de problemas ROSA de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com ROSA e. IAM

AWS Organizations a política de controle de serviços nega as permissões necessárias AWS Marketplace

Se sua política AWS Organizations de controle de serviço (SCP) não permitir as permissões de AWS Marketplace assinatura necessárias ao tentar habilitá-las ROSA, ocorrerá o seguinte erro no console.

```
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.
```

Se você receber esse erro, entre em contato com o administrador para obter assistência. Seu administrador é a pessoa que gerencia as contas da sua organização. Peça a essa pessoa que faça o seguinte:

1. Configure o SCP para permitir`aws-marketplace:Subscribe`,`aws-marketplace:Unsubscribe`, e `aws-marketplace:ViewSubscriptions` permissões. Para obter mais informações, consulte Atualizando um SCP no Guia do AWS Organizations Usuário.
2. Ative ROSA na conta de gerenciamento da organização.
3. Compartilhe a ROSA assinatura com contas de membros que exigem acesso dentro da organização. Para obter mais informações, consulte Compartilhamento de assinaturas em uma organização no Guia do AWS Marketplace comprador.

O usuário ou a função não tem as AWS Marketplace permissões necessárias

Se seu IAM diretor não tiver as permissões de AWS Marketplace assinatura necessárias quando você tentar habilitar ROSA, ocorrerá o seguinte erro no console.

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

Para resolver esse problema, siga estas etapas:

1. Acesse o IAM console e anexe a política AWS gerenciada `ROSAManageSubscription` à sua identidade do IAM. Para obter mais informações, consulte ROSAManageAssinatura no Guia de referência de políticas AWS gerenciadas.
2. Siga o procedimento em the section called “Ativar ROSA e configurar AWS pré-requisitos”.

Se você não tiver permissão para visualizar ou atualizar seu conjunto de permissões IAM ou receber uma mensagem de erro, entre em contato com o administrador para obter ajuda. Peça a essa pessoa que `ROSAManageSubscription` anexe sua IAM identidade e siga o procedimento emthe section called “Ativar ROSA e configurar AWS pré-requisitos”. Quando um administrador executa essa ação, ela é ROSA ativada atualizando o conjunto de permissões para todas as IAM identidades sob o. Conta da AWS

AWS Marketplace Permissões necessárias bloqueadas por um administrador

Se o administrador da sua conta bloqueou as permissões de AWS Marketplace assinatura necessárias, o seguinte erro do console ocorrerá quando você tentar habilitá-las 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.
```

Se você receber esse erro, entre em contato com o administrador para obter assistência. Peça a essa pessoa que faça o seguinte:

1. Acesse o ROSA console e anexe a política AWS gerenciada `ROSAManageSubscription` à sua identidade do IAM. Para obter mais informações, consulte ROSAManageAssinatura no Guia de referência de políticas AWS gerenciadas.
2. Siga o procedimento the section called “Ativar ROSA e configurar AWS pré-requisitos” para habilitar ROSA. Esse procedimento é ativado ROSA atualizando o conjunto de permissões para todas as IAM identidades sob o. Conta da AWS

Erro ao criar o balanceador de carga: AccessDenied

Se você não criou um balanceador de carga, a função `AWSServiceRoleForElasticLoadBalacing` vinculada ao serviço pode não existir na sua conta. O erro a seguir ocorre se você tentar criar uma ROSA cluster sem a `AWSServiceRoleForElasticLoadBalacing` função em sua conta.

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

Para resolver esse problema, siga estas etapas:

1. Verifique se sua conta tem a função `AWSServiceRoleForElasticLoadBalancing`.

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

2. Se você não tiver essa função, siga as instruções para criar a função encontradas em Criar a função vinculada ao serviço no Guia do Elastic Load Balancing usuário.

Resiliência em ROSA

AWS resiliência da infraestrutura global

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, que são conectadas por meio de redes de baixa latência, alta taxa de transferência e altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

ROSA oferece aos clientes a opção de executar o plano de controle e o plano de dados do Kubernetes em uma única zona de AWS disponibilidade ou em várias zonas de disponibilidade. Embora os clusters Single-AZ possam ser úteis para experimentação, os clientes são incentivados a executar workloads em mais de uma zona de disponibilidade. Isso garante que os aplicativos possam suportar até mesmo uma falha completa na Zona de Disponibilidade, um evento muito raro por si só.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

ROSA resiliência de clusters

O plano ROSA de controle consiste em pelo menos três nós do plano de OpenShift controle. Cada nó do ambiente de gerenciamento é composto por uma instância de servidor de API, uma `etcd`

instância e controladores. No caso de uma falha no nó do ambiente de gerenciamento, todas as solicitações de API são automaticamente roteadas para os outros nós disponíveis para garantir a disponibilidade do cluster.

O plano de ROSA dados consiste em pelo menos dois nós de OpenShift infraestrutura e dois nós de OpenShift trabalho. Os nós de infraestrutura executam pods que oferecem suporte aos componentes da infraestrutura do OpenShift cluster, como o roteador padrão, o OpenShift registro incorporado e os componentes para métricas e monitoramento do cluster. OpenShift os nós de trabalho executam pods de aplicativos para o usuário final.

Os engenheiros de confiabilidade de sites da Red Hat (SREs) gerenciam totalmente o plano de controle e os nós da infraestrutura. A Red Hat monitora SREs proativamente o ROSA cluster e é responsável por substituir quaisquer nós do plano de controle e nós de infraestrutura com falha. Para obter mais informações, consulte the section called “Responsabilidades”.

> **Important**
>
> Por ser ROSA um serviço gerenciado, a Red Hat é responsável por gerenciar a AWS infraestrutura subjacente que ROSA usa. Os clientes não devem tentar desligar manualmente as Amazon EC2 instâncias que ROSA usam do AWS console ou AWS CLI. Essa ação pode levar à perda de dados do cliente.

Se um nó de processamento falhar no plano de dados, o ambiente de gerenciamento realoca os pods não programados para o(s) nó(s) de processamento em funcionamento até que o nó com falha seja recuperado ou substituído. Os nós de processamento com falha podem ser substituídos manual ou automaticamente, permitindo o dimensionamento automático de máquinas em um cluster. Para obter mais informações, consulte o Dimensionamento automático do cluster na documentação da Red Hat.

Resiliência de aplicativos implantada pelo cliente

Embora ROSA forneça muitas proteções para garantir a alta disponibilidade do serviço, os clientes são responsáveis por criar seus aplicativos implantados com alta disponibilidade para proteger as cargas de trabalho contra o tempo de inatividade. Para obter mais informações, consulte Sobre disponibilidade para ROSA na documentação da Red Hat.

Segurança da infraestrutura em ROSA

Como serviço gerenciado, Serviço Red Hat OpenShift na AWS é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar — AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar ROSA pela AWS rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Isolamento de rede de cluster

Os engenheiros de confiabilidade de sites da Red Hat (SREs) são responsáveis pelo gerenciamento contínuo e pela segurança da rede do cluster e da plataforma de aplicativos subjacente. Para obter mais informações sobre as responsabilidades da Red Hat ROSA, consultethe section called “Responsabilidades”.

Quando você cria um novo cluster, ROSA oferece a opção de criar um endpoint público do servidor da API Kubernetes e rotas de aplicativos ou um endpoint e rotas de aplicativos da API Kubernetes privados. Essa conexão é usada para se comunicar com seu cluster (usando ferramentas OpenShift de gerenciamento como a CLI e a CLI OpenShift do ROSA). Uma conexão privada permite que toda a comunicação entre seus nós e o servidor de API permaneça dentro da sua VPC. Se você habilitar o acesso privado ao servidor da API e às rotas do aplicativo, deverá usar uma VPC existente e conectar AWS PrivateLink a VPC ao serviço de back-end. OpenShift

O acesso ao servidor da API Kubernetes é protegido usando uma combinação de AWS Identity and Access Management (IAM) e controle de acesso baseado em função (RBAC) nativo do

Kubernetes. Para obter mais informações sobre o RBAC (Controle de Acesso Baseado em Função) no Kubernetes, consulte Usando a autorização RBAC na documentação do Kubernetes.

ROSA permite criar rotas de aplicativos seguras usando vários tipos de terminação TLS para fornecer certificados ao cliente. Para obter mais informações, consulte Rotas seguras na documentação da Red Hat.

Se você criar um ROSA cluster em uma VPC existente, você especifica as sub-redes VPC e as zonas de disponibilidade para seu cluster usar. Você também define os intervalos de CIDR para uso da rede de cluster e combina esses intervalos de CIDR com as sub-redes VPC. Para obter mais informações, consulte as Definições de intervalo CIDR na documentação da Red Hat.

Para clusters que usam o endpoint público da API, é ROSA necessário que sua VPC esteja configurada com uma sub-rede pública e privada para cada zona de disponibilidade na qual você deseja que o cluster seja implantado. Para clusters que usam o endpoint privado da API, somente sub-redes privadas são necessárias.

Se você estiver usando uma VPC existente, poderá configurar seus ROSA clusters para usar um servidor proxy HTTP ou HTTPS durante ou após a criação do cluster para criptografar o tráfego da web do cluster, adicionando outra camada de segurança aos seus dados. Quando você habilita um proxy, os componentes principais do cluster são impedidos de acessar diretamente a Internet. O proxy não nega o acesso à Internet para workloads do usuário. Para obter mais informações, consulte a Configuração de um proxy em todo o cluster na documentação da Red Hat.

Isolamento de rede do pod

Se você for administrador de cluster, poderá definir políticas de rede no nível do pod que restrinjam o tráfego aos pods no seu ROSA cluster.

ROSA cotas de serviço

Serviço Red Hat OpenShift na AWS (ROSA) usa cotas de serviço para Amazon EC2, Amazon Virtual Private Cloud Amazon Elastic Block Store, e para Elastic Load Balancing provisionar clusters. Para obter mais informações, consulte Serviço Red Hat OpenShift na AWS endpoints e cotas no Guia de referência AWS geral.

AWS serviços integrados com ROSA

ROSA trabalha com outros Serviços da AWS para fornecer soluções adicionais para seus desafios de negócios. Este tópico identifica serviços usados ROSA para adicionar funcionalidades ou serviços ROSA usados para executar tarefas.

Tópicos

Como ROSA funciona com AWS Marketplace

AWS Marketplace é um catálogo digital com curadoria que você pode usar para encontrar, comprar, implantar e gerenciar software, dados e serviços de terceiros necessários para criar soluções e administrar seus negócios. AWS Marketplace simplifica o licenciamento e a aquisição de software com opções flexíveis de preços e vários métodos de implantação.

ROSA usos AWS Marketplace para medição e cobrança de serviços. O ROSA classic é medido e faturado por meio de um produto baseado em AWS Marketplace Amazon Machine Image (AMI), enquanto o ROSA com planos de controle hospedados (HCP) é medido e faturado por meio de um produto baseado em AWS Marketplace software como serviço (SaaS).

Esta página explica como ROSA funciona com AWS Marketplace pagamentos, faturamento, assinaturas e compras contratuais.

Terminologia

Esta página usa os seguintes termos ao discutir a integração do ROSA com AWS Marketplace.

Imagem de máquina da Amazon (AMI)

> Uma imagem de um servidor, incluindo um sistema operacional e software adicional, que é executado em AWS.

Assinatura de AMI

> Em AWS Marketplace, produtos de software baseados em AMI, como o ROSA classic, usam um modelo de preço por hora com assinatura anual. O preço por hora é o modelo de preço padrão, mas você tem a opção de comprar antecipadamente o valor de um ano de uso para um tipo de Amazon EC2 instância.

Assinatura de SaaS

Em produtos software-as-a-service (SaaS) AWS Marketplace, como o ROSA com HCP, adotam um modelo de assinatura baseado no uso. O vendedor de software rastreia seu uso e você só paga pelo que usar.

Oferta pública

As ofertas públicas permitem que você compre AWS Marketplace software e serviços diretamente do AWS Management Console.

Oferta privada

As ofertas privadas são um programa de compras que permite que vendedores e compradores negociem preços personalizados e termos do contrato de licenciamento do usuário final (EULA) para compras em. AWS Marketplace

Taxas de serviço do ROSA

Taxas ROSA cobradas pelo gerenciamento OpenShift de software e cluster pelos engenheiros de confiabilidade de sites da Red Hat (SREs). ROSA as taxas de serviço são calculadas AWS Marketplace e aparecem na sua AWS fatura.

Taxas de infraestrutura do AWS

Taxas padrão AWS cobradas pelos ROSA clusters Serviços da AWS subjacentes Amazon EC2, incluindo Amazon EBS Amazon S3,, Elastic Load Balancing e. As taxas são calculadas por meio do AWS service (Serviço da AWS) uso e aparecem na sua AWS fatura.

ROSA pagamentos e faturamento

ROSA se integra AWS Marketplace para permitir a medição e o faturamento das taxas de ROSA serviço. ROSA as taxas de serviço cobrem o acesso ao OpenShift software e ao gerenciamento de clusters pelos engenheiros de confiabilidade de sites da Red Hat (SREs). ROSA as taxas de serviço são uniformes em todas as regiões AWS padrão suportadas. As taxas de serviço do ROSA com HCP são acumuladas sob demanda, por padrão, a uma taxa horária fixa com base no número de clusters em execução e no node de trabalho v em CPUs execução nesses clusters. As taxas de serviço do ROSA Classic são acumuladas sob demanda com base no número de trabalhadores (node v. CPUs O ROSA classic não cobra taxas de serviço pelo plano de controle ou pelos nós de infraestrutura necessários.

ROSA os clientes também pagam taxas de AWS infraestrutura padrão para os ROSA clusters Serviços da AWS subjacentes Amazon EC2 Amazon EBS, incluindo Amazon S3,, Elastic Load Balancing e. AWS as taxas de infraestrutura são um item de cobrança separado das taxas ROSA de serviço que são calculadas. AWS Marketplace AWS por padrão, as taxas de infraestrutura variam Região da AWS e são baseadas no uso por hora. Para reduzir ainda mais os custos de AWS infraestrutura, você pode comprar planos de Amazon EC2 economia ou instâncias reservadas. Para obter mais informações, consulte Compute Savings Plans and Reserved Instances no Guia Amazon EC2 do usuário.

ROSA não cobra taxas até você criar um ROSA cluster ou comprar um ROSA contrato. Para obter mais informações, consulte Preços do Serviço Red Hat OpenShift na AWS.

Você pode ver as taxas de ROSA serviço e taxas de AWS infraestrutura e gerenciar pagamentos no AWS Billing console. Você também pode visualizar seus custos e monitorar o uso usando a AWS Cost Explorer Service interface gratuitamente. Para obter mais informações, consulte Visualizando sua fatura no Guia do Gerenciamento de Faturamento e Custos da AWS usuário e Analisando seus custos AWS Cost Explorer Service no Guia do usuário de gerenciamento de AWS custos.

Inscrever-se em listagens ROSA do Marketplace por meio do console

Quando você ativa ROSA no ROSA console, você Conta da AWS se inscreve nas listagens ROSA classic e ROSA com HCP ativadas. AWS Marketplace Não há taxa para habilitar ROSA assinaturas.

Para AWS Organizations usuários, ROSA permite que você compartilhe assinaturas ROSA classic com outras contas em sua organização. Para obter mais informações, consulte Compartilhamento de assinaturas em uma organização no Guia do AWS Marketplace comprador.

Comprando um ROSA contrato

ROSA usa AWS Marketplace para fornecer contratos opcionais para ROSA com HCP e ROSA classic. Os contratos proporcionam economia nas taxas de serviço do ROSA Worker Node. ROSA os contratos não afetam as taxas cobradas pela AWS infraestrutura.

Contratos de 12 meses

Você pode comprar contratos de oferta pública de 12 meses para ROSA classic e ROSA com HCP no ROSA console.

> **Note**
>
> O ROSA classic deve estar ativado em sua conta antes que você possa comprar contratos de 12 meses no console.

> **Note**
>
> Os contratos de 12 meses não podem ser transferidos para uma oferta privada.

Aquisição de um contrato ROSA classic de 12 meses

Ao comprar um contrato ROSA classic de 12 meses, você faz um pagamento adiantado por um período anual e não paga nenhuma taxa de serviço por hora pelos próximos 12 meses para as instâncias cobertas. O custo do contrato é baseado no tipo de Amazon EC2 instância e no número de instâncias que você seleciona. O contrato não cobre as taxas de AWS infraestrutura ROSA cobradas pelo subjacente Serviços da AWS que são usadas. Para obter mais informações, consulte Serviço Red Hat OpenShift na AWS Preço.

O contrato abrange apenas os tipos de instância especificados durante a criação do contrato (m5.xlarge, por exemplo). Você pode comprar contratos adicionais de 12 meses para economizar em mais de um tipo de Amazon EC2 instância. O uso fora do seu contrato de 12 meses incorre em taxas de ROSA serviço sob demanda.

> **Note**
>
> Os contratos ROSA classic de 12 meses não são renovados automaticamente.

Aquisição de um contrato ROSA classic de 12 meses

> **Note**
>
> Se você estiver usando o ROSA console em uma região que ainda não oferece suporte ao ROSA com HCP, esse fluxo de trabalho ainda não está disponível. Para obter uma lista de regiões que oferecem suporte ao ROSA com HCP, consultethe section called “Comparando o ROSA com o HCP e o ROSA classic”.

Para comprar contratos ROSA classic em regiões sem ROSA com suporte de HCP, acesse o console do ROSA e escolha Comprar um contrato de software e ver os contratos existentes.

1. Acesse o console do ROSA.
2. No painel de navegação à esquerda, escolha Contratos.
3. Escolha Contratos para o ROSA classic.
4. Escolha Contrato de compra.
5. Selecione o tipo de EC2 instância e o número de instâncias que você precisa.
6. Escolha Revisar contrato.
7. Revise os detalhes do contrato e escolha Contrato de compra.

Note

ROSA Os contratos de 12 meses não podem ser rebaixados ou cancelados após a criação usando o console. Se você precisar fazer o downgrade ou cancelar o contrato durante a duração ativa do contrato, acesse o Centro do Suporte e abra um caso de suporte.

Aquisição de um contrato ROSA com HCP de 12 meses

Quando você ativa o ROSA com HCP no console, um contrato ROSA com HCP gratuito de 12 meses é criado inicialmente em sua conta para facilitar o faturamento sob demanda. Se você optar por comprar um contrato ROSA com HCP para economizar nas taxas de serviço do nó de trabalho, o contrato inicial será modificado para cobrir os custos de uso do nó de trabalho v CPUs e dos planos de controle que você especificar.

Ao comprar um contrato ROSA com HCP de 12 meses, você faz um pagamento antecipado por um período anual e não paga nenhuma taxa de uso por hora nos próximos 12 meses para o nó de trabalho v CPUs e os planos de controle cobertos. O custo do contrato é baseado no número de nó de trabalho v CPUs e planos de controle que você seleciona. O contrato abrange somente o nó de trabalho v CPUs e os planos de controle que você especifica durante a criação do contrato. O contrato não cobre as taxas de AWS infraestrutura ROSA cobradas pelo subjacente Serviços da AWS que são usadas. Para obter mais informações, consulte Serviço Red Hat OpenShift na AWS Preço.

Uso da cota mensal

Na compra, seus planos V CPUs e de controle pré-pagos são convertidos em uma cota de uso mensal. As taxas de uso por hora sob demanda se aplicam ao uso da vCPU e do ambientes de gerenciamento que excede a cota mensal. O ROSA com HCP usa as seguintes fórmulas para calcular a cota mensal associada ao contrato:

- Nó de trabalho vCPUs: número de v CPUs x 24 horas x 365 dias/12 meses
- Ambientes de gerenciamento: número de ambientes de gerenciamento x 24 horas x 365 dias/12 meses

Por exemplo, uma compra de 4.000 nós de trabalho v CPUs e 8 planos de controle seria convertida em uma cota mensal de 2.920.000 horas de vCPU de nós de trabalho e 5.840 horas de plano de controle consumíveis por mês.

Para adquirir um contrato ROSA com HCP de 12 meses

> **Note**
>
> Se você estiver usando o Serviço Red Hat OpenShift na AWS console em uma região que ainda não oferece suporte ao ROSA com planos de controle hospedados, esse fluxo de trabalho ainda não está disponível. Para obter uma lista de regiões que oferecem suporte ao ROSA com HCP, consultethe section called “Comparando o ROSA com o HCP e o ROSA classic”.

1. Acesse o console do ROSA.
2. No painel de navegação à esquerda, escolha Contratos.
3. Escolha Contratos para ROSA com HCP.
4. Escolha Contrato de compra.
5. Insira o número de v CPUs para comprar. Especifique em múltiplos de 4.
6. Insira o número de ambientes de gerenciamento a serem comprados.
7. Escolha Revisar contrato.
8. Revise os detalhes do contrato e escolha Contrato de compra.

> **Note**
>
> ROSA Os contratos de 12 meses não podem ser rebaixados ou cancelados após a criação usando o console. Se você precisar fazer o downgrade ou cancelar o contrato durante a duração ativa do contrato, acesse o Centro do Suporte e abra um caso de suporte.

Atualização de um contrato ROSA com HCP de 12 meses

Você pode atualizar seu contrato ativo de 12 meses do ROSA com o HCP a qualquer momento com um nó de trabalho v CPUs e planos de controle adicionais. Ao atualizar seu contrato ROSA com HCP de 12 meses, você faz um pagamento antecipado proporcional pelos recursos adicionais. Os valores rateados são calculados com base no número de dias restantes do contrato. O contrato abrange somente o nó de trabalho v CPUs e os planos de controle que você especifica durante a criação do contrato. As atualizações do contrato não afetam as taxas cobradas pela AWS infraestrutura.

Após a atualização, os planos v CPUs e de controle adicionados são convertidos em uma cota de uso mensal usando as mesmas fórmulas da compra original do contrato. As taxas de uso por hora sob demanda se aplicam ao uso da vCPU e do ambiente de gerenciamento que excede a cota mensal. Para obter mais informações, consulte the section called “Uso da cota mensal”.

Para atualizar um contrato ROSA com HCP de 12 meses

1. Acesse o console do ROSA.
2. No painel de navegação à esquerda, escolha Contratos.
3. Escolha Contratos para ROSA com HCP.
4. Escolha Atualizar.
5. Insira o número de v CPUs a ser adicionado. Especifique em múltiplos de 4.
6. Insira o número de ambientes de gerenciamento a serem adicionados ao contrato.
7. Escolha Revisar a atualização.
8. Revise os detalhes do contrato e escolha Atualizar compra.

> **Note**
>
> Os contratos ROSA classic de 12 meses não podem ser atualizados. Contratos ROSA classic adicionais de 12 meses podem ser adquiridos a qualquer momento usando o ROSA console.

Obtendo uma oferta privada

Você pode solicitar uma oferta AWS Marketplace privada do ROSA com o HCP ou o ROSA classic para receber os preços do produto e os termos do contrato de licenciamento do usuário final (EULA) negociados com a Red Hat. Para obter mais informações, consulte Ofertas privadas no Guia do AWS Marketplace comprador.

Para obter uma oferta ROSA privada

> **Note**
>
> Se você é um AWS Organizations usuário e recebeu uma oferta privada emitida para suas contas de pagador e membro, siga o procedimento abaixo para se inscrever ROSA diretamente em cada conta da sua organização.
> Se você receber uma oferta privada clássica do ROSA que foi emitida apenas para a conta do AWS Organizations pagador, você precisará compartilhar a assinatura com as contas dos membros em sua organização. Para obter mais informações, consulte Compartilhamento de assinaturas em uma organização no Guia do AWS Marketplace comprador.

1. Depois que uma oferta privada for emitida, faça login no console do AWS Marketplace.
2. Abra o e-mail com um link de oferta ROSA particular.
3. Siga o link para acessar diretamente a oferta privada.

   > **Note**
   >
   > Seguir esse link antes de fazer login na conta correta resultará em um erro de Página não encontrada (404).

4. Revise todos os Termos e Condições.
5. Ecolha Aceitar termos.

> **Note**
>
> Se uma oferta AWS Marketplace privada não for aceita, as taxas de ROSA serviço AWS Marketplace continuarão sendo cobradas de acordo com a tarifa pública por hora.

6. Para verificar os detalhes da oferta, selecione Mostrar detalhes na lista de produtos.
7. Para começar a usar ROSA, escolha Continuar com a configuração. Você será redirecionado para o ROSA console.

Loja privada

O Private Marketplace permite que os administradores criem catálogos digitais personalizados de produtos aprovados a partir de. AWS Marketplace Os administradores podem criar conjuntos exclusivos de software aprovado, disponíveis para compra AWS Marketplace por unidades AWS organizacionais ou diferentes Contas da AWS dentro de sua organização.

Se sua organização usa um mercado privado, um administrador deve adicionar as AWS Marketplace listagens ROSA ao mercado privado antes que os usuários possam habilitar o serviço. Para obter mais informações, consulte Introdução ao mercado privado no Guia do AWS Marketplace comprador.

Solução de problemas

A página a seguir detalha alguns problemas comuns encontrados ao criar ou gerenciar ROSA clusters.

Tópicos

Acesse os ROSA registros de depuração do cluster

Para começar a solucionar problemas com sua aplicação, primeiro revise os logs de depuração. Os registros de depuração da ROSA CLI fornecem detalhes sobre as mensagens de erro que são produzidas quando uma cluster falha na criação de um.

Para exibir as informações de cluster depuração, execute o seguinte comando da ROSA CLI. No comando, `<cluster_name>` substitua pelo nome do seu cluster.

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

ROSA o cluster falha na verificação da cota de AWS serviço durante a criação cluster

Para usar ROSA, talvez seja necessário aumentar as cotas de serviço da sua conta. Para saber mais, consulte Endpoints e cotas do Serviço Red Hat OpenShift na AWS.

1. Execute o comando a seguir para identificar as cotas da sua conta.

```
rosa verify quota
```

> **Note**
>
> As cotas são diferentes em diferentes Regiões da AWS. Verifique cada uma das cotas de suas regiões.

2. Se você precisar aumentar sua cota, navegue até o console do Service Quotas.
3. No painel de navegação, escolha AWS serviços.
4. Escolha o serviço que precisa de um aumento de cota.
5. Selecione a cota que precisa ser aumentada e escolha Solicitar aumento de cota.
6. Para Solicitar aumento da cota, insira o valor total que você deseja que a cota seja e escolha Solicitar.

Solucionar problemas de tokens de acesso off-line expirados na ROSA CLI

Se você usar a ROSA CLI e seu token de acesso off-line api.openshift.com expirar, uma mensagem de erro será exibida. Isso acontece quando sso.redhat.com invalida o token.

1. Navegue até a página OpenShift Cluster Manager API Token e escolha Carregar token.
2. Copie e cole o seguinte comando de autenticação no terminal.

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

Falha ao criar um cluster com um osdCcsAdmin erro

> **Note**
>
> Esse erro ocorre somente quando você usa o método não STS de provisionamento de clusters ROSA . Para evitar esse problema, provisione seus ROSA clusters usando AWS STS. Para obter mais informações, consulte the section called “Crie um cluster ROSA clássico - CLI”.

Se sua criação cluster falhar, você poderá receber a seguinte mensagem de erro:

```
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. Exclua a pilha.

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

2. Reinicialize sua conta.

```
rosa init
```

Próximas etapas

- Visite a OpenShift documentação.
- Abra um Suporte case ou case do Red Hat Support.
- Encontre respostas para perguntas frequentes sobre Serviço Red Hat OpenShift na AWS.
- Para obter mais informações sobre o modelo de suporte do ROSA, consultethe section called “Obter suporte”.

Obtendo ROSA suporte

Com isso ROSA, você pode receber suporte das equipes Suporte de suporte da Red Hat. Os casos de suporte podem ser abertos com qualquer organização e encaminhados para a equipe correta para resolver seu problema.

Abra uma Suporte caixa

É necessário um plano de suporte ao AWS desenvolvedor para abrir casos ROSA técnicos, mas um plano AWS Business, Enterprise ou Enterprise On-Ramp Support é recomendado para acesso contínuo ao suporte ROSA técnico e à orientação arquitetônica. A Red Hat usa a Suporte API para abrir casos para clientes quando necessário. AWS Os planos de suporte Business, Enterprise e Enterprise On-Ramp permitem acesso contínuo por telefone, web e chat aos engenheiros de suporte. Para obter mais informações sobre Suporte planos, consulte Suporte.

Para ver as etapas para habilitar um Suporte plano, consulte Como faço para me inscrever em um Suporte plano?

Para obter informações sobre como criar um Suporte caso, consulte Criação de casos de suporte e gerenciamento de casos.

Abra um caso do Red Hat Support

ROSA inclui o Red Hat Premium Support. Para receber o Red Hat Premium Support, navegue até o Portal do cliente da Red Hat e use a ferramenta de caso de suporte para criar um ticket de suporte. Para obter mais informações, consulte Como interagir com o suporte da Red Hat.

Histórico do documento

A tabela a seguir descreve as alterações importantes feitas na documentação do . Para receber notificações sobre atualizações dessa documentação, é possível inscrever-se em um feed RSS.

Alteração	Descrição	Data
Atualizado ROSAControlPlaneOperatorPolicy	Atualizou a política AWS gerenciada ROSAControlPlaneOperatorPolicy para permitir a marcação de grupos de segurança gerenciados pela Red Hat para o gerenciamento adequado do ciclo de vida dos recursos e para adicionar o grupo de segurança/* para gerenciar a correção de falhas de reconciliação do VPCE durante as atualizações do cluster. VPCEndpoint WithCondition Para obter mais informações, consulte ROSA atualizações nas políticas AWS gerenciadas.	9 de abril de 2026
Atualizado ROSAKubeControllerPolicy	A política AWS gerenciada foi atualizada ROSAKubeControllerPolicy para esclarecer as permissões do Elastic Load Balancing para registrar e cancelar o registro de alvos com grupos-alvo. Para obter mais informações, consulte ROSA atualizações	5 de março de 2026

	nas políticas AWS gerenciadas.	
Atualizado ROSANodePoolManagementPolicy	ROSA atualizou a política gerenciada `ROSANodePoolManagementPolicy` para adicionar acesso a recursos para reservas de capacidade para oferecer suporte ao recurso de reservas de capacidade. Para obter informações, consulte ROSA atualizações nas políticas AWS gerenciadas.	3 de setembro de 2025
ROSAInstallerPolítica atualizada	Atualizou a ROSAInstaller política AWS gerenciada para oferecer suporte ao novo recurso de reservas de capacidade no ROSA e melhorar o gerenciamento de tags do cluster Kubernetes. Para obter informações, consulte ROSA atualizações nas políticas AWS gerenciadas.	7 de agosto de 2025

Nova ROSAShared VPCRoute53 política	ROSA lançou uma nova política gerenciada `ROSASharedVPCRoute53Policy` para permitir que o instalador do ROSA configure registros do Route 53 em ambientes VPC compartilhados. Para obter informações, consulte ROSA atualizações nas políticas AWS gerenciadas.	7 de agosto de 2025
Nova ROSAShared VPCEndpoint política	ROSA lançou uma nova política gerenciada `ROSASharedVPCEndpointPolicy` para permitir que o instalador do ROSA configure endpoints de VPC e grupos de segurança em ambientes de VPC compartilhados. Essa política fornece um subconjunto de permissões do EC2 personalizadas para casos de uso de VPC compartilhados. Para obter informações, consulte ROSA atualizações nas políticas AWS gerenciadas.	7 de agosto de 2025
Atualizado ROSAImage RegistryOperatorPolicy	Atualizou a política AWS gerenciada ROSAImage RegistryOperatorPolicy.	19 de maio de 2025
Atualizado ROSANodePoolManagementPolicy	Atualizou a política AWS gerenciada ROSANodePoolManagementPolicy .	5 de maio de 2025

Atualizado ROSAImage RegistryOperatorPolicy	Atualizou a política AWS gerenciada ROSAImage RegistryOperatorPolicy.	16 de abril de 2025
Atualizado ROSAWorke rInstancePolicy	Atualizou a política AWS gerenciada ROSAWorke rInstancePolicy.	3 de março de 2025
Atualizado ROSANodeP oolManagementPolicy	Atualizou a política AWS gerenciada ROSANodeP oolManagementPolicy.	24 de fevereiro de 2025
Atualizado ROSAAmazo nEBSCSIDriverOperatorPolicy	Atualizou a política AWS gerenciada ROSAAmazon EBSCSIDriverOperatorPolicy.	17 de janeiro de 2025
ROSA com expansão de HCP Região da AWS	O ROSA com aviões de controle hospedados (HCP) agora está disponível no Oriente Médio (EAU). Região da AWS	13 de maio de 2024
ROSA com expansão de HCP Região da AWS	O ROSA com aviões de controle hospedados (HCP) está agora disponível na Europa (Paris) Região da AWS.	6 de maio de 2024
Atualizado ROSANodeP oolManagementPolicy	Atualizou a política AWS gerenciada ROSANodeP oolManagementPolicy.	2 de maio de 2024
ROSA com expansão de HCP Região da AWS	O ROSA com planos de controle hospedados (HCP) está agora disponível na Europa (Espanha). Região da AWS	29 de abril de 2024

ROSAInstallerPolítica atualizada	Atualizou a política AWS gerenciada ROSAInstaller da política.	24 de abril de 2024
ROSA com expansão de HCP Região da AWS	O ROSA com aviões de controle hospedados (HCP) está agora disponível na Europa (Zurique). Região da AWS	19 de abril de 2024
ROSA com expansão de HCP Região da AWS	O ROSA com aviões de controle hospedados (HCP) agora está disponível na Ásia-Pacífico (Osaka). Região da AWS	17 de abril de 2024
ROSAInstallerPolítica e ROSASRESupport política atualizadas	Atualizou a ROSAInstaller Política e ROSASRESupport a Política de políticas AWS gerenciadas.	10 de abril de 2024
ROSA com expansão de HCP Região da AWS	O ROSA com aviões de controle hospedados (HCP) agora está disponível na Ásia-Pacífico (Hong Kong) Região da AWS.	8 de abril de 2024
ROSA com expansão de HCP Região da AWS	O ROSA com aviões de controle hospedados (HCP) agora está disponível na América do Sul (São Paulo) Região da AWS.	1º de abril de 2024
ROSA com expansão de HCP Região da AWS	O ROSA com aviões de controle hospedados (HCP) agora está disponível no Oriente Médio (Bahrein Região da AWS).	25 de março de 2024

ROSA com expansão de HCP Região da AWS	O ROSA com aviões de controle hospedados (HCP) agora está disponível na Ásia-Pacífico (Seul). Região da AWS	14 de março de 2024
ROSA com expansão de HCP Região da AWS	O ROSA com aviões de controle hospedados (HCP) agora está disponível na África (Cidade do Cabo) Região da AWS.	5 de março de 2024
ROSAInstallerPolítica atualizada	Atualizou a política AWS gerenciada ROSAInstaller da política.	26 de janeiro de 2024
ROSASRESupportPolítica atualizada	Atualizou a política AWS gerenciada ROSASRESupport da política.	22 de janeiro de 2024
Atualizado ROSAImage RegistryOperatorPolicy	Atualizou a política AWS gerenciada ROSAImage RegistryOperatorPolicy.	12 de dezembro de 2023
Atualizado ROSAKubeC ontrollerPolicy	Atualizou a política AWS gerenciada ROSAKubeC ontrollerPolicy.	16 de outubro de 2023
ROSAManageAssinatura atualizada	Atualizou a ROSAManage assinatura da política AWS gerenciada.	1º de agosto de 2023
Atualizado ROSAKubeC ontrollerPolicy	Atualizou a política AWS gerenciada ROSAKubeC ontrollerPolicy.	13 de julho de 2023

Páginas de segurança ROSA adicionadas	Resiliência em ROSA, segurança de infraestrutura em ROSA e proteção de dados em páginas ROSA foram adicionadas.	30 de junho de 2023
Página de opções de implantação adicionada	A página de opções de implantação foi adicionada.	9 de junho de 2023
Nova política AWS gerenciada adicionada ROSANodePoolManagementPolicy	Uma nova política AWS gerenciada ROSANodePoolManagementPolicy foi adicionada.	8 de junho de 2023
Nova ROSAInstaller política AWS gerenciada adicionada	Foi adicionada uma nova ROSAInstaller política AWS gerenciada.	6 de junho de 2023
Nova ROSASRESupport política AWS gerenciada adicionada	Foi adicionada uma nova ROSASRESupport política AWS gerenciada.	1º de junho de 2023
Visão geral adicionada das responsabilidades do ROSA adicionada	Página da visão geral das responsabilidades do ROSA adicionada.	26 de maio de 2023
Atualizado O que é Serviço Red Hat OpenShift na AWS?	Atualizou a Serviço Red Hat OpenShift na AWS página O que é.	24 de maio de 2023
Novas políticas AWS gerenciadas adicionadas para funções de operador do ROSA	Novas políticas AWS ROSAImage RegistryOperatorPolicy gerenciadas ROSAKube ControllerPolicy e ROSAKMSProvider políticas foram adicionadas.	27 de abril de 2023

Nova política AWS gerenciada adicionada ROSAControlPlaneOperatorPolicy	Uma nova política AWS gerenciada ROSAControlPlaneOperatorPolicy foi adicionada.	24 de abril de 2023
Foram adicionadas novas políticas AWS gerenciadas para funções da conta ROSA	Novas páginas de políticas AWS gerenciadas para a conta ROSA e a página de funções do operador foram adicionadas.	20 de abril de 2023
Página de Service Quotas ROSA adicionada	A página de cotas do serviço ROSA foi adicionada.	22 de dezembro de 2022
Páginas de resolução de problemas adicionadas	Páginas de solução de problemas foram adicionadas.	1º de novembro de 2022
Páginas sobre conceitos básicos adicionadas	Páginas de introdução foram adicionadas.	12 de agosto de 2022
Nova ROSAManage assinatura de política AWS gerenciada adicionada	A nova ROSAManage assinatura de política AWS gerenciada foi adicionada.	11 de abril de 2022
Lançamento inicial	A versão inicial do Guia Serviço Red Hat OpenShift na AWS do Usuário.	24 de março de 2021

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.