Benutzer-Leitfaden

Red Hat OpenShift Service in AWS

Red Hat OpenShift Service in AWS: Benutzer-Leitfaden

Table of Contents

Was ist Red Hat OpenShift Service in AWS?

Red Hat OpenShift Service in AWS (ROSA) ist ein verwalteter Service, mit dem Sie containerisierte Anwendungen mit der Red Hat OpenShift Enterprise Kubernetes-Plattform erstellen, skalieren und bereitstellen können. AWS ROSA optimiert die Migration von lokalen OpenShift RedHat-Workloads zu anderen Workloads und bietet eine enge Integration mit AWS anderen. AWS-Services

Features

ROSA wird gemeinsam von und Red Hat unterstützt AWS und betrieben. Jeder ROSA Cluster bietet rund um die Uhr Support durch den RedHat Site Reliability Engineer (SRE) für das Clustermanagement, unterstützt durch das Service Level Agreement (SLA) von RedHat mit einer Verfügbarkeit von 99,95%. Weitere Informationen zum Support-Modell des Services finden Sie unter. the section called “Supportanfragen”

ROSA bietet außerdem die folgenden Funktionen:

- Von Red Hat SRE unterstützte Cluster-Installation, Cluster-Wartung und Cluster-Upgrades.
- AWS-Service Zu den Integrationen gehören AWS Datenverarbeitung, Datenbank, Analytik, maschinelles Lernen, Netzwerke und Mobilgeräte.
- Führen Sie die Kubernetes-Steuerebene über mehrere AWS Availability Zones aus und skalieren Sie sie, um eine hohe Verfügbarkeit zu gewährleisten.
- Betreiben Sie Cluster mithilfe von Produktivitätstools für Entwickler, darunter Service Mesh, CodeReady Workspaces OpenShift APIs und Serverless.

Zugreifen ROSA

Sie können Ihre ROSA Servicebereitstellungen mithilfe der folgenden Schnittstellen definieren und konfigurieren.

AWS

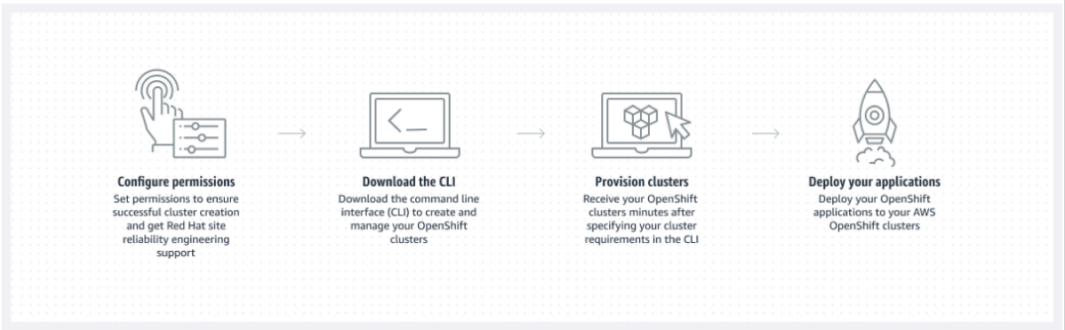
- ROSA Konsole — Stellt eine Weboberfläche zur Verfügung, über die Sie das ROSA Abonnement aktivieren und einen ROSA Softwarevertrag erwerben können.

- AWS Command Line Interface (AWS CLI) — Stellt Befehle für eine Vielzahl von Befehlen bereit AWS-Services und wird unter Windows, MacOS und Linux unterstützt. Weitere Informationen finden Sie unter AWS Command Line Interface.

Red Hat OpenShift

- Red Hat Hybrid Cloud Console — Bietet eine Weboberfläche zum Erstellen, Aktualisieren und Verwalten von ROSA Clustern, Installieren von Cluster-Add-Ons sowie zum Erstellen und Bereitstellen von Anwendungen in einem ROSA Cluster.
- ROSA CLI (rosa) — Stellt Befehle zum Erstellen, Aktualisieren und Verwalten von ROSA Clustern bereit.
- OpenShift CLI (oc) — Stellt Befehle zur Erstellung von Anwendungen und zur Verwaltung von OpenShift Container Platform-Projekten bereit.
- Knative CLI (kn) — Stellt Befehle bereit, die für die Interaktion mit OpenShift serverlosen Komponenten wie Knative Serving und Eventing verwendet werden können.
- Pipelines CLI (tkn) — Stellt Befehle zur Interaktion mit OpenShift Pipelines über das Terminal bereit.
- opm CLI — Stellt Befehle bereit, die Operator-Entwicklern und Clusteradministratoren helfen, OpenShift Operator-Kataloge vom Terminal aus zu erstellen und zu verwalten.
- Operator SDK CLI — Stellt Befehle bereit, mit denen ein Operator-Entwickler einen OpenShift Operator erstellen, testen und bereitstellen kann.

Wie fange ich an mit ROSA



Im Folgenden werden die ersten Schritte für ROSA zusammengefasst. Eine ausführliche Anleitung für die ersten Schritte finden Sie unterFangen Sie an mit ROSA .

AWS-Managementkonsole/AWS CLI

1. Konfigurieren Sie Berechtigungen für AWS-Services das, ROSA worauf die Bereitstellung der Servicefunktionen angewiesen ist. Weitere Informationen finden Sie unter the section called “Voraussetzungen”.
2. Installieren und konfigurieren Sie das neueste AWS CLI Tool. Weitere Informationen finden Sie im AWS CLI Benutzerhandbuch unter Installation oder Aktualisierung AWS CLI der neuesten Version von.
3. ROSA In der ROSA Konsole aktivieren.

RedHat Hybrid Cloud-Konsole/CLI ROSA

1. Laden Sie die neueste Version der ROSA CLI und OpenShift CLI von der Red Hat Hybrid Cloud Console herunter. Weitere Informationen finden Sie unter Erste Schritte mit der ROSA CLI in der Red Hat-Dokumentation.
2. Erstellen Sie ROSA Cluster in der Red Hat Hybrid Cloud Console oder mit der ROSA CLI.
3. Wenn Ihr Cluster bereit ist, konfigurieren Sie einen Identitätsanbieter, um Benutzern Zugriff auf den Cluster zu gewähren.
4. Stellen Sie Workloads auf Ihrem ROSA Cluster genauso bereit und verwalten Sie sie wie in jeder anderen OpenShift Umgebung.

Preisgestaltung

Die Gesamtkosten von setzen ROSA sich aus zwei Komponenten zusammen: ROSA Servicegebühren und AWS Infrastrukturgebühren. Weitere Informationen über die Preise finden Sie unter Red Hat OpenShift Service in AWS – Preise.

ROSA Servicegebühren

Standardmäßig fallen ROSA Servicegebühren bei Bedarf zu einem Stundensatz pro 4 vCPUs an, die von Worker-Knoten genutzt werden. Die Servicegebühren sind in allen unterstützten AWS Standardregionen einheitlich. Zusätzlich zur Worker-Node-Servicegebühr fällt für ROSA mit Clustern mit Hosted Control Planes (HCP) eine stündliche Clustergebühr an.

ROSA bietet ein- und dreijährige Servicegebührenverträge an, die Sie abschließen können, um bei den On-Demand-Servicegebühren für Worker Nodes zu sparen. Weitere Informationen finden Sie unter the section called “Einen ROSA Vertrag abschließen”.

AWS Infrastrukturgebühren

AWS Infrastrukturgebühren fallen für die zugrunde liegenden Worker-Knoten, Infrastrukturknoten, Kontrollebenenknoten, Speicher- und Netzwerkressourcen an, die auf der AWS globalen Infrastruktur gehostet werden. AWS Die Infrastrukturgebühren variieren je nach AWS-Region.

Überblick über die Zuständigkeiten für ROSA

In dieser Dokumentation werden die Verantwortlichkeiten von Amazon Web Services (AWS), Red Hat und Kunden für den Red Hat OpenShift Service in AWS (ROSA) Managed Service beschrieben. Weitere Informationen zu ROSA und seinen Komponenten finden Sie unter Richtlinien und Service-Definition in der Red Hat-Dokumentation.

Das Modell der AWS gemeinsamen Verantwortung definiert die AWS Verantwortung für den Schutz der Infrastruktur, auf der alle im Rahmen der angebotenen Dienste ausgeführt werden AWS Cloud, einschließlich ROSA. AWS Die Infrastruktur umfasst die Hardware, Software, Netzwerke und Einrichtungen, die AWS Cloud Dienste ausführen. Diese AWS Verantwortung wird allgemein als „Sicherheit der Cloud“ bezeichnet. Um ROSA als vollständig verwalteter Service zu agieren, sind Red Hat und der Kunde für die Elemente des Services verantwortlich, die das AWS Verantwortungsmodell als „Sicherheit in der Cloud“ definiert.

Red Hat ist für die laufende Verwaltung und Sicherheit der ROSA Cluster-Infrastruktur, der zugrunde liegenden Anwendungsplattform und des Betriebssystems verantwortlich. ROSA Cluster werden zwar auf AWS Ressourcen beim Kunden gehostet AWS-Konten, der Zugriff auf sie erfolgt jedoch per Fernzugriff durch ROSA Servicekomponenten und Red Hat Site Reliability Engineers (SREs) über IAM Rollen, die der Kunde selbst erstellt. Red Hat verwendet diesen Zugriff, um die Bereitstellung und Kapazität aller Steuerungsebenen und Infrastrukturknoten im Cluster zu verwalten und die Versionen für die Knoten der Kontrollebene, Infrastrukturknoten und Worker-Knoten zu verwalten.

Red Hat und der Kunde teilen sich die Verantwortung für ROSA Netzwerkmanagement, Cluster-Logging, Cluster-Versionierung und Kapazitätsmanagement. Während Red Hat den ROSA Service verwaltet, trägt der Kunde die volle Verantwortung für die Verwaltung und Sicherung aller Anwendungen, Workloads und Daten, auf denen er bereitgestellt wird. ROSA

-Übersicht

Die folgende Tabelle bietet einen Überblick über die Zuständigkeiten von AWS Red Hat und Kunden für Red Hat OpenShift Service in AWS.

> **Note**
>
> Wenn die `cluster-admin` Rolle einem Benutzer hinzugefügt wird, finden Sie weitere Informationen zu den Zuständigkeiten und Ausschlusshinweisen im Red Hat Enterprise Agreement, Anhang 4 (Online-Abonnementdienste).

Ressource	Vorfalls- und Betriebsmanagement	Verwaltung von Änderungen	Zugriff und Identitätsautorisierung	Sicherheit und Einhaltung gesetzlicher Vorschriften	Wiederherstellung nach einem Notfall
Kundendaten	Customer	Customer	Customer	Customer	Customer
Kundenanwendungen	Customer	Customer	Customer	Customer	Customer
Dienste für Entwickler	Customer	Customer	Customer	Customer	Customer
Überwachung der Plattform	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Protokollierung	Red Hat	Red Hat und der Kunde	Red Hat und der Kunde	Red Hat und der Kunde	Red Hat
Netzwerke für Anwendungen	Red Hat und der Kunde	Red Hat und der Kunde	Red Hat und der Kunde	Red Hat	Red Hat
Cluster-Netzwerke	Red Hat	Red Hat und der Kunde	Red Hat und der Kunde	Red Hat	Red Hat
Verwaltung virtueller Netzwerke	Red Hat und der Kunde	Red Hat und der Kunde	Red Hat und der Kunde	Red Hat und der Kunde	Red Hat und der Kunde
Virtuelles Rechenman	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat

Ressource	Vorfalls- und Betriebsmanagement	Verwaltung von Änderungen	Zugriff und Identität sautorisierung	Sicherheit und Einhaltung gesetzlicher Vorschriften	Wiederherstellung nach einem Notfall
agement (Steuerungsebene, Infrastruktur und Worker-Knoten)					
Cluster-Version	Red Hat	Red Hat und Kunde	Red Hat	Red Hat	Red Hat
Kapazitätsmanagement	Red Hat	Red Hat und der Kunde	Red Hat	Red Hat	Red Hat
Virtuelles Speichermanagement	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS Software (öffentlich AWS-Services)	AWS	AWS	AWS	AWS	AWS
Hardware/ globale Infrastruktur AWS	AWS	AWS	AWS	AWS	AWS

Aufgaben für gemeinsame Zuständigkeiten nach Bereichen

AWS, Red Hat und Kunden teilen sich die Verantwortung für die Überwachung und Wartung der ROSA Komponenten. Diese Dokumentation definiert die ROSA Servicezuständigkeiten nach Bereichen und Aufgaben.

Vorfalls- und Betriebsmanagement

AWS ist verantwortlich für den Schutz der Hardwareinfrastruktur, auf der alle in der angebotenen Dienste ausgeführt werden AWS Cloud. Red Hat ist verantwortlich für die Verwaltung der Servicekomponenten, die für das standardmäßige Plattformnetzwerk erforderlich sind. Der Kunde ist für das Incident- und Operationsmanagement der Anwendungsdaten des Kunden und aller kundenspezifischen Netzwerke verantwortlich, die der Kunde möglicherweise konfiguriert hat.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Netzwerke von Anwendungen	Red Hat • Überwachen Sie den systemeigenen OpenShift Router-Dienst und reagieren Sie auf Warnmeldungen.	Kunde • Überwachen Sie den Zustand der Anwendung srouten und der dahinter stehenden Endpunkte. • Melden Sie Ausfälle an AWS und RedHat.
Verwaltung virtueller Netzwerke	Red Hat • Überwachen Sie AWS Load Balancer, Amazon VPC Subnetze und AWS-Service Komponenten, die für Standard-Plattform netzwerke erforderlich sind. Reagieren Sie auf Warnmeldungen.	Kunde • Überwachen Sie den Zustand der AWS Load Balancer-Endpunkte. • Überwachen Sie den Netzwerkverkehr, der optional über eine Amazon VPC zu-VPC-Verbindung, eine Site-to-Site VPN Verbindung oder auf potenzielle Probleme oder

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
		Direct Connect Sicherheitsbedrohungen konfiguriert wird.
Verwaltung virtueller Speicher	Red Hat • Überwachen Sie Amazon EBS Volumes, die für Cluster-Knoten verwendet werden, und Amazon S3 Buckets, die für die integrierte Container-Image-Registry des ROSA Services verwendet werden. Reagieren Sie auf Warnmeldungen.	Kunde • Überwachen Sie den Zustand der Anwendungsdaten. • Wenn vom Kunden verwaltete AWS KMS keys Systeme verwendet werden, erstellen und kontrollieren Sie den Schlüssellebenszyklus und die wichtigsten Richtlinien für die Amazon EBS Verschlüsselung.
AWS Software (öffentlich AWS-Services)	AWS • Informationen zum AWS Vorfall- und Betriebsmanagement finden Sie im AWS Whitepaper unter So AWS wird die betriebliche Resilienz und Betriebskontinuität gewährleistet.	Kunde • Überwachen Sie den Zustand der AWS Ressourcen im Kundenkonto. • Verwenden Sie IAM Tools, um den AWS Ressourcen im Kundenkonto die entsprechenden Berechtigungen zuzuweisen.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Hardware/globale Infrastruktur AWS	AWS • Informationen zum AWS Vorfall- und Betriebsmanagement finden Sie im Whitepaper unter So wird die AWS betriebliche Resilienz und Servicekontinuität gewährleistet. AWS	Kunde • Konfigurieren, verwalten und überwachen Sie Kundenanwendungen und -daten, um sicherzustellen, dass die Anwendungs- und Datensicherheitskontrollen ordnungsgemäß durchgesetzt werden.

Änderungsmanagement

AWS ist verantwortlich für den Schutz der Hardwareinfrastruktur, auf der alle in der AWS Cloud angebotenen Dienste ausgeführt werden. Red Hat ist dafür verantwortlich, Änderungen an der Cluster-Infrastruktur und den Diensten zu ermöglichen, die vom Kunden kontrolliert werden, sowie für die Wartung der Versionen der Knoten auf der Kontrollebene, der Infrastrukturknoten und der Worker-Knoten. Der Kunde ist dafür verantwortlich, Änderungen an der Infrastruktur einzuleiten. Der Kunde ist auch für die Installation und Wartung optionaler Dienste, Netzwerkkonfigurationen auf dem Cluster und Änderungen an Kundendaten und Anwendungen verantwortlich.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Protokollierung	Red Hat • Aggregieren und überwachen Sie die Audit-Logs der Plattform zentral. • Bereitstellung und Wartung eines Logging-Operators, der es dem Kunden ermöglicht, einen Logging-Stack für die Standarda	Kunde • Installieren Sie den optionalen Standard-Operator für die Anwendungsprotokollierung auf dem Cluster. • Installieren, konfigurieren und verwalten Sie alle optionalen Lösungen für die

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
	nwendungsprotokollierung bereitzustellen. • Stellen Sie auf Kundenwun sch Prüfprotokolle zur Verfügung.	Anwendungsprotokollierung, wie z. B. Logging-Sidecar-Container oder Protokoll ierungsanwendungen von Drittanbietern. • Passen Sie Größe und Häufigkeit der Anwendung sprotokolle an, die von Kundenanwendungen erstellt werden, falls sie die Stabilität des Logging-Stacks oder des Clusters beeinträchtigen. • Fordern Sie in einem Support-Fall Plattform-Auditprotokolle an, um spezifische Vorfälle zu untersuchen.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Netzwerke von Anwendungen	Red Hat • Richten Sie öffentliche Load Balancer ein. Bieten Sie die Möglichkeit, private Load Balancer und bei Bedarf bis zu einem zusätzlichen Load Balancer einzurichten. • Richten Sie den systemeig enen OpenShift Router-Dienst ein. Bieten Sie die Möglichkeit, den Router als privat festzulegen und bis zu einem zusätzlichen Router-Shard hinzuzufügen. • Installieren, konfigurieren und verwalten Sie OpenShift SDN-Komponenten für den standardmäßigen internen Pod-Verkehr. • Bieten Sie dem Kunden die Möglichkeit, Objekte zu verwalten `NetworkPolicy` und `EgressNetworkPolicy` (Firewall-) zu verwalten.	Kunde • Konfigurieren Sie nicht standardmäßige Pod-Netzwerkberechtigungen für Projekt- und Pod-Netzwerke, Pod-Ingress und Pod-Egress mithilfe von Objekten. `NetworkPolicy` • Verwenden Sie OpenShift Cluster Manager, um einen privaten Load Balancer für Standardanwendungsrouten anzufordern. • Verwenden Sie OpenShift Cluster Manager, um bis zu einen zusätzlichen öffentlichen oder privaten Router-Shard und den entsprechenden Load Balancer zu konfigurieren. • Fordern Sie zusätzliche Service Load Balancer für bestimmte Dienste an und konfigurieren Sie sie. • Konfigurieren Sie alle erforderlichen DNS-Weiterleitungsregeln.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Cluster-Netzwerke	Red Hat • Richten Sie Cluster-Management-Komponenten wie öffentliche oder private Service-Endpunkte und die erforderliche Integration mit Amazon VPC Komponenten ein. • Richten Sie interne Netzwerkkomponenten ein, die für die interne Clusterkommunikation zwischen Worker-, Infrastruktur- und Steuerebenenknoten erforderlich sind.	Kunde • Geben Sie bei der Bereitstellung des Clusters bei Bedarf optionale, nicht standardmäßige IP-Adressbereiche für Maschinen-CIDR, Service-CIDR und Pod-CIDR über den OpenShift Cluster Manager an. • Fordern Sie an, dass der API-Dienstendpunkt bei der Clustererstellung oder nach der Clustererstellung über den Cluster Manager öffentlich oder privat gemacht wird. OpenShift

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Verwaltung virtueller Netzwerke	Red Hat • Richten Sie die Amazon VPC Komponenten ein, die für die Bereitstellung des Clusters erforderlich sind, wie Subnetze, Load Balancer, Internet-Gateways und NAT-Gateways. • Bieten Sie dem Kunden die Möglichkeit, Site-to-Site VPN Konnektivität mit lokalen Ressourcen, Verbindungen zu Amazon VPC VPC-Verbindungen und nach Direct Connect Bedarf über OpenShift Cluster Manager zu verwalten. • Ermöglichen Sie es Kunden, AWS Load Balancer für die Verwendung mit Service Load Balancers zu erstellen und bereitzustellen.	Kunde • Richten Sie optionale Amazon VPC Komponenten ein und verwalten Sie sie, z. Amazon VPC B. zu VPC-Verbindung, Site-to-Site VPN Verbindung oder. Direct Connect • Fordern Sie zusätzliche Load Balancer für bestimmte Dienste an und konfigurieren Sie sie.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Verwaltung virtueller Rechenleistung	Red Hat • Richten Sie die ROSA Steuerungsebene und die Datenebene ein und konfigurieren Sie sie, um Amazon EC2 Instanzen für Cluster-Computing zu verwenden. • Überwachen und verwalten Sie die Bereitstellung der Amazon EC2 Kontrollebene und der Infrastrukturknoten auf dem Cluster.	Kunde • Überwachen und verwalten Sie Amazon EC2 Worker-Knoten, indem Sie mit dem OpenShift Cluster Manager oder der ROSA CLI einen Maschinenpool erstellen. • Verwalten Sie Änderungen an vom Kunden bereitges tellten Anwendungen und Anwendungsdaten.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Cluster-Version	Red Hat • Aktivieren Sie den Upgrade-Planungsprozess. • Überwachen Sie den Upgrade-Fortschritt und beheben Sie alle aufgetretenen Probleme. • Veröffentlichen Sie Änderungsprotokolle und Versionshinweise für kleinere Upgrades und Wartungsupgrades.	Kunde • Planen Sie Wartungsversions-Upgrades entweder sofort, für die future oder lassen Sie automatische Upgrades durchführen. • Bestätigen Sie kleinere Versions-Upgrades und planen Sie sie. • Stellen Sie sicher, dass für die Cluster-Version weiterhin eine unterstützte Nebenversion verwendet wird. • Testen Sie Kundenanwendungen auf Neben- und Wartungsversionen, um die Kompatibilität sicherzustellen.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Kapazitätsmanagement	Red Hat • Überwachen Sie die Verwendung der Steuerung sebene. Zu den Steuerung sebenen gehören Knoten der Steuerungsebene und Infrastrukturknoten. • Skalieren und skalieren Sie die Knoten der Kontrolle bene, um die Servicequalität aufrechtzuerhalten.	Kunde • Überwachen Sie die Auslastung der Workerkno ten und aktivieren Sie gegebenenfalls die Auto Scaling-Funktion. • Ermitteln Sie die Skalierun gsstrategie des Clusters. • Verwenden Sie die bereitgestellten OpenShift Cluster Manager-S teuerelemente, um nach Bedarf weitere Worker-Kn oten hinzuzufügen oder zu entfernen. • Reagieren Sie auf Benachrichtigungen von Red Hat zu den Anforderungen an Cluster-R essourcen.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Verwaltung virtueller Speicher	Red Hat • Einrichtung und Konfiguration für Amazon EBS die Bereitstellung von lokalem Knotenspeicher und persistentem Volumenspeicher für den Cluster. • Richten Sie die integrierte Image-Registry für die Verwendung von Amazon S3 Bucket-Speicher ein und konfigurieren Sie sie. • Reduzieren Sie regelmäßig die Ressourcen der Image-Registry Amazon S3 , um die Amazon S3 Nutzung und die Cluster-Leistung zu optimieren.	Kunde • Optional können Sie den Amazon EBS CSI-Treiber oder den Amazon EFS CSI-Treiber so konfigurieren, dass persistente Volumes auf dem Cluster bereitgestellt werden.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden

AWS Software (öffentliche AWS Dienste)	AWS
	
	Datenverarbeitung
	
	• Stellen Sie den Amazon EC2 Dienst bereit, der für die ROSA Steuerung sebene, die Infrastruktur und die Worker-Knoten verwendet wird.
	
	Speicherung
	
	• Stellen Sie Amazon EBS bereit, dass der ROSA Dienst lokalen Knotenspe icher und persistenten Volumenspeicher für den Cluster bereitstellen kann.
	
	Netzwerkfunktionen
	
	• Stellen Sie die folgenden AWS Cloud Dienste bereit, um die Anforderungen der ROSA virtuellen Netzwerki nfrastruktur zu erfüllen:
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• Stellen Sie die folgenden optionalen AWS-Service
		Kunde
		
		• Signieren Sie Anfragen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel, der einem IAM Hauptbenutzer zugeordnet ist, oder AWS STS temporären Sicherhei tsanmeldedaten.
		• Geben Sie VPC-Subnetze an, die der Cluster bei der Clustererstellung verwenden soll.
		• Konfigurieren Sie optional eine vom Kunden verwaltete VPC für die Verwendung mit ROSA Clustern.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
	Integrationen bereit für ROSA: • Site-to-Site VPN • Direct Connect • AWS PrivateLink • AWS Transit Gateway	
Hardware/globale Infrastruktur AWS	AWS • Informationen zu Verwaltungskontrollen für AWS Rechenzentren finden Sie auf der Seite Sicherheit unter Unsere Kontrollen. AWS Cloud • Informationen zu bewährten Methoden für das Change-Management finden Sie unter Guidelines for Change Management AWS in der AWS Lösungsbibliothek.	Kunde • Implementieren Sie bewährte Methoden für das Change-Management für Kundenanwendungen und Daten, die auf dem gehostet AWS Cloud werden.

Zugriffs- und Identitätsautorisierung

Die Zugriffs- und Identitätsautorisierung umfasst Aufgaben für die Verwaltung des autorisierten Zugriffs auf Cluster, Anwendungen und Infrastrukturressourcen. Dazu gehören Aufgaben wie die Bereitstellung von Zugriffskontrollmechanismen, Authentifizierung, Autorisierung und Verwaltung des Zugriffs auf Ressourcen.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Protokollierung	Red Hat	Kunde

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
	• Halten Sie sich an ein auf Industriestandards basierendes mehrstufiges Verfahren für den internen Zugriff auf Plattform-Audit-Logs. • Stellen Sie native RBAC-Funktionen OpenShift bereit.	• Konfigurieren Sie OpenShift RBAC, um den Zugriff auf Projekte und damit auf die Anwendungsprotokolle eines Projekts zu kontrollieren. • Bei Protokollierungslösungen von Drittanbietern oder kundenspezifischen Anwendungen ist der Kunde für die Zugriffsverwaltung verantwortlich.
Netzwerke von Anwendungen	Red Hat • Stellen Sie native OpenShift RBAC und `dedicated-admin` Funktionen bereit.	Kunde • Konfiguration OpenShift `dedicated-admin` und RBAC zur Steuerung des Zugriffs auf die Routenkonfiguration nach Bedarf. • Verwalten Sie Red Hat-Organisationsadministratoren, damit Red Hat Zugriff auf OpenShift Cluster Manager gewährt. Der Clustermanager wird verwendet, um Router-Optionen zu konfigurieren und Service-Load-Balancer-Quoten bereitzustellen.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Cluster-Netzwerke	Red Hat • Bieten Sie Kunden Zugriffskontrollen über OpenShift Cluster Manager. Stellen Sie native OpenShift RBAC und `dedicated-admin` Funktionen bereit.	Kunde • Konfiguration OpenShift `dedicated-admin` und RBAC zur Steuerung des Zugriffs auf die Routenkonfiguration nach Bedarf. • Verwaltung der RedHat-Unternehmenszugehörigkeit zu Red Hat Accounts. • Verwaltet Organisationsadministratoren, damit Red Hat Zugriff auf OpenShift Cluster Manager gewährt.
Verwaltung virtueller Netzwerke	Red Hat • Bieten Sie Kunden Zugriffskontrollen über OpenShift Cluster Manager.	Kunde • Verwalten Sie den optionalen Benutzerzugriff auf AWS Komponenten über OpenShift Cluster Manager.
Verwaltung virtueller Rechenleistung	Red Hat • Bieten Sie Kunden Zugriffskontrollen über OpenShift Cluster Manager.	Kunde • Verwalten Sie den optionalen Benutzerzugriff auf AWS Komponenten über OpenShift Cluster Manager. • Erstellen Sie IAM Rollen und zugehörige Richtlinien, die für den Zugriff auf ROSA Dienste erforderlich sind.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Verwaltung virtueller Speicher	Red Hat • Bieten Sie Kunden Zugriffskontrollen über OpenShift Cluster Manager.	Kunde • Verwalten Sie den optionalen Benutzerzugriff auf AWS Komponenten über OpenShift Cluster Manager. • Erstellen Sie IAM Rollen und zugehörige Richtlinien, die für den Zugriff auf ROSA Dienste erforderlich sind.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
AWS Software (öffentliche AWS Dienste)	AWS Datenverarbeitung • Stellen Sie den Amazon EC2 Dienst bereit, der für die ROSA Steuerung sebene, die Infrastruktur und die Worker-Knoten verwendet wird. Speicherung • Provide Amazon EBS, wird verwendet, um ROSA die Bereitstellung von lokalem Knotenspeicher und persistentem Volumensp eicher für den Cluster zu ermöglichen. • Provide Amazon S3, wird für die integrierte Image-Registrierung des Dienstes verwendet. Netzwerkfunktionen • Provide AWS Identity and Access Management (IAM), wird von Kunden verwendet , um den Zugriff auf ROSA Ressourcen zu kontrolli eren, die auf Kundenkonten ausgeführt werden.	Kunde • Erstellen Sie IAM Rollen und zugehörige Richtlinien, die für den Zugriff auf ROSA Dienste erforderlich sind. • Verwenden Sie IAM Tools, um die entsprechenden Berechtigungen auf AWS Ressourcen im Kundenkon to anzuwenden. • Um die Aktivierung ROSA unternehmensweit zu AWS gewährleisten, ist der Kunde für die Verwaltung der AWS Organizations Administr atoren verantwortlich. • Für die ROSA AWS unternehmensweite Aktivierung ist der Kunde für die Verteilung der gewährten ROSA Rechte verantwortlich. AWS License Manager

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Hardware/globale Infrastruktur AWS	AWS • Informationen zu physische n Zugangskontrollen für AWS Rechenzentren finden Sie auf der AWS Cloud Seite Sicherheit unter Unsere Kontrollen.	Kunde • Der Kunde ist nicht für die AWS globale Infrastruktur verantwortlich.

Sicherheit und Einhaltung gesetzlicher Vorschriften

Im Folgenden sind die Verantwortlichkeiten und Kontrollen im Zusammenhang mit der Einhaltung der Vorschriften aufgeführt:

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Protokollierung	Red Hat • Senden Sie Cluster-A udit-Logs an ein Red Hat SIEM, um sie auf Sicherhei tsereignisse hin zu analysier en. Bewahren Sie Audit-Logs für einen definierten Zeitraum auf, um forensisc he Analysen zu unterstüt zen.	Kunde • Analysieren Sie Anwendung sprotokolle auf Sicherhei tsereignisse. • Senden Sie Anwendung sprotokolle über Logging-Sidecar-Container oder Protokollierungsan wendungen von Drittanbi etern an einen externen Endpunkt, wenn eine längere Aufbewahrung erforderlich ist, als sie der Standard-Logging-Stack bietet.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Verwaltung virtueller Netzwerke	Red Hat • Überwachen Sie virtuelle Netzwerkkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Verwenden Sie öffentliche AWS Tools für zusätzliche Überwachung und zusätzlic hen Schutz.	Kunde • Überwachen Sie optional konfigurierte virtuelle Netzwerkkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Konfigurieren Sie nach Bedarf alle erforderl ichen Firewallregeln oder Schutzmaßnahmen für Kundenrechenzentren.
Verwaltung virtueller Rechenleistung	Red Hat • Überwachen Sie virtuelle Rechenkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Verwenden Sie öffentliche AWS Tools für zusätzliche Überwachung und zusätzlic hen Schutz.	Kunde • Überwachen Sie optional konfigurierte virtuelle Netzwerkkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Konfigurieren Sie nach Bedarf alle erforderl ichen Firewallregeln oder Schutzmaßnahmen für Kundenrechenzentren.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Verwaltung virtueller Speicher	Red Hat • Überwachen Sie virtuelle Speicherkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Verwenden Sie öffentliche AWS Tools für zusätzliche Überwachung und zusätzlic hen Schutz. • Konfigurieren Sie den ROSA Dienst so, dass die Volumendaten der Steuerungsebene, der Infrastruktur und des Workerknotens standardm äßig mit dem AWS verwaltet en KMS-Schlüssel verschlüs selt werden, der Folgendes Amazon EBS bereitstellt. • Konfigurieren Sie den ROSA Dienst so, dass persistente Kundendat enträger, die die Standards peicherklasse verwenden, mit dem AWS verwalteten KMS-Schlüssel verschlüs selt werden, Amazon EBS der Folgendes bereitstellt. • Bieten Sie dem Kunden die Möglichkeit, persisten te Volumes mit verwalteter	Kunde • Amazon EBS Bereitste llungsvolumen. • Verwalten Sie den Amazon EBS Volumenspeicher, um sicherzustellen, dass genügend Speicherplatz für die Bereitstellung als Volume zur Verfügung steht ROSA. • Erstellen Sie den Anspruch auf ein persistentes Volume und generieren Sie mithilfe des OpenShift Cluster-M anagers ein persistentes Volume.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
	KMS key Kundenverwaltung zu verschlüsseln. • Konfigurieren Sie die Container-Image-Registry so, dass die gespeicherten Image-Registrierungsdaten mithilfe serverseitiger Verschlüsselung mit Amazon S3 verwalteten Schlüsseln (SSE-3) verschlüsselt werden. • Bieten Sie dem Kunden die Möglichkeit, eine öffentliche oder private Amazon S3 Image-Registry zu erstellen, um seine Container-Images vor unbefugtem Benutzerzugriff zu schützen.	

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
AWS Software (öffentliche AWS Dienste)	AWS Datenverarbeitung • Bereitstellung Amazon EC2, die für die ROSA Steuerung sebene, die Infrastruktur und die Arbeitsknoten verwendet wird. Weitere Informationen finden Sie unter Infrastruktursicherheit Amazon EC2 im Amazon EC2 Benutzerhandbuch. Speicherung • Stellen Sie Volumes bereit Amazon EBS, die für die ROSA Steuerungsebene, die Infrastruktur und die Worker-Node-Volume s sowie für persistente Kubernetes-Volumes verwendet werden. Weitere Informationen finden Sie unter Datenschutz Amazon EC2 im Amazon EC2 Benutzerhandbuch. • Provide AWS KMS, das zur ROSA Verschlüsselung von Volumes und persistenten Volumes auf Kontrollebene, Infrastruktur und Worker-No de verwendet wird. Weitere	Kunde • Stellen Sie sicher, dass bewährte Sicherhei tsmethoden und das Prinzip der geringsten Rechte eingehalten werden, um die Daten auf der Amazon EC2 Instance zu schützen. Weitere Informationen finden Sie unter Infrastru ktursicherheit in Amazon EC2 und Datenschutz in Amazon EC2. • Überwachen Sie optional konfigurierte virtuelle Netzwerkkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Konfigurieren Sie nach Bedarf alle erforderl ichen Firewallregeln oder Schutzmaßnahmen für Kundenrechenzentren. • Erstellen Sie einen optionale n, vom Kunden verwaltet en KMS-Schlüssel und verschlüsseln Sie das Amazon EBS persistente Volume mithilfe des KMS-Schlüssels. • Überwachen Sie die Kundendaten im virtuelle

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
	Informationen finden Sie im Amazon EC2 Benutzerhandbuch unter Amazon EBS Verschlüsselung. • Provide Amazon S3, wird für die integrierte Container-Image-Registrierung des ROSA-Dienstes verwendet. Weitere Informationen finden Sie im Amazon S3 Benutzerhandbuch unter Amazon S3 Sicherheit. Netzwerkfunktionen • Stellen Sie Sicherheitsfunktionen und -dienste bereit, um den Datenschutz zu erhöhen und den Netzwerkzugriff auf die AWS globale Infrastruktur zu kontrollieren, einschließlich integrierter Netzwerk-Firewalls Amazon VPC, privater oder dedizierter Netzwerkverbindungen und automatischer Verschlüsselung des gesamten Datenverkehrs in den AWS globalen und regionalen Netzwerken zwischen AWS gesicherten Einrichtungen. Weitere Informationen finden Sie unter Modell	n Speicher auf potenzielle Probleme und Sicherheitsbedrohungen. Weitere Informationen finden Sie unter AWS -Modell der geteilten Verantwortung.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
	der AWS gemeinsamen Verantwortung und Infrastruktursicherheit im Whitepaper Einführung in die AWS Sicherheit.	
Hardware/globale Infrastruktur AWS	AWS • Stellen Sie die AWS globale Infrastruktur bereit, die zur Bereitstellung von ROSA Servicefunktionen verwendet wird. Weitere Informationen zu AWS Sicherheitskontrollen finden Sie im AWS Whitepaper unter Sicherheit der AWS Infrastruktur. • Stellen Sie dem Kunden Unterlagen zur Verfügung, um die Compliance-Anforderungen zu verwalten und seinen Sicherheitsstatus AWS mithilfe von Tools wie AWS Artifact AWS Security Hub zu überprüfen.	Kunde • Konfigurieren, verwalten und überwachen Sie Kundenanwendungen und -daten, um sicherzustellen, dass die Anwendungs- und Datensicherheitskontrollen ordnungsgemäß durchgesetzt werden. • Verwenden Sie IAM Tools, um die entsprechenden Berechtigungen auf AWS Ressourcen im Kundenkonto anzuwenden.

Notfallwiederherstellung

Die Notfallwiederherstellung umfasst Daten- und Konfigurationssicherungen, Datenreplikation und Konfiguration der Notfallwiederherstellungsumgebung sowie Failover bei Notfällen.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
Verwaltung virtueller Netzwerke	Red Hat • Stellen Sie die betroffen en virtuellen Netzwerkk omponenten wieder her oder erstellen Sie sie neu, die für das Funktionieren der Plattform erforderlich sind.	Kunde • Konfigurieren Sie virtuelle Netzwerkverbindungen nach Möglichkeit mit mehr als einem Tunnel, um sich vor Ausfällen zu schützen. • Behalten Sie Failover-DNS und Load Balancing bei, wenn Sie einen globalen Load Balancer mit mehreren Clustern verwenden.
Verwaltung virtueller Rechenleistung	Red Hat • Überwachen Sie den Cluster und ersetzen Sie ausgefallene Amazon EC2 Steuerungsebene oder Infrastrukturknoten. • Bieten Sie dem Kunden die Möglichkeit, ausgefallene Worker-Knoten manuell oder automatisch zu ersetzen.	Kunde • Ersetzen Sie ausgefall ene Amazon EC2 Worker-Knoten, indem Sie die Maschinenpool-Konf iguration über den OpenShift Cluster Manager oder die ROSA CLI bearbeiten.
Verwaltung virtueller Speicher	Red Hat • Bei ROSA Clustern, die mit AWS IAM Benutzera nmeldedaten erstellt wurden, sichern Sie alle Kubernetes-Objekte auf dem Cluster anhand	Kunde • Sichern Sie Kundenanw endungen und Anwendung sdaten.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
	stündlicher, täglicher und wöchentlicher Volume-Snapshots.	

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
AWS Software (öffentliche AWS Dienste)	AWS Datenverarbeitung • Stellen Sie Amazon EC2 Funktionen bereit, die die Datenstabilität unterstützen, z. B. Amazon EBS Snapshots und. Amazon EC2 Auto Scaling Weitere Informationen finden Sie unter Resilienz Amazon EC2 im Amazon EC2 Benutzerhandbuch. Speicherung • Bieten Sie dem ROSA Service und den Kunden die Möglichkeit, das Amazon EBS Volume auf dem Cluster mithilfe von Amazon EBS Volume-Snapshots zu sichern. • Informationen zu Amazon S3 Funktionen, die Datenstabilität unterstützen, finden Sie unter Resilienz in. Amazon S3 Netzwerkfunktionen • Informationen zu Amazon VPC Funktionen, die	Kunde • Konfigurieren Sie ROSA Multi-AZ-Cluster, um die Fehlertoleranz und Cluster-Verfügbarkeit zu verbessern. • Stellen Sie persistente Volumes mithilfe des Amazon EBS CSI-Treibers bereit, um Volume-Snapshots zu ermöglichen. • Erstellen Sie CSI-Volume-Snapshots von Amazon EBS persistenten Volumes.

Ressource	Verantwortlichkeiten im Service	Pflichten des Kunden
	Datenresilienz unterstützen, finden Sie unter Resilienz Amazon Virtual Private Cloud im Amazon VPC Benutzerhandbuch.	
Hardware/globale Infrastruktur AWS	AWS • Stellen Sie eine AWS globale Infrastruktur bereit, die es ermöglich t ROSA , die Kontrolle bene, die Infrastruktur und die Worker-Knoten in allen Availability Zones zu skalieren. Diese Funktiona lität ermöglicht ROSA die Orchestrierung eines automatischen Failovers zwischen Zonen ohne Unterbrechung. • Weitere Informationen zu bewährten Methoden für die Notfallwiederherstellung finden Sie unter Disaster Recovery-Optionen in der Cloud im AWS Well-Arch itected Framework.	Kunde • Konfigurieren Sie ROSA Multi-AZ-Cluster, um die Fehlertoleranz und Cluster-Verfügbarkeit zu verbesser n.

Verantwortung des Kunden für Daten und Anwendungen

Der Kunde ist für die Anwendungen, Workloads und Daten verantwortlich, für die er sie bereitstellt. Red Hat OpenShift Service in AWS RedHat stellt jedoch AWS verschiedene Tools zur Verfügung, die den Kunden bei der Verwaltung von Daten und Anwendungen auf der Plattform unterstützen.

Ressource	Wie AWS und Red Hat hilft	Pflichten des Kunden
Kundendaten	Red Hat • Halten Sie Standards auf Plattformebene für Datenverschlüsselung ein, wie sie in den Sicherheits- und Compliance-Standards der Branche definiert sind. • Stellen Sie OpenShift Komponenten zur Verwaltung von Anwendungsdaten bereit, z. B. geheime Daten. • Ermöglichen Sie die Integration mit Datendiensten Amazon RDS , z. B. zum Speichern und Verwalten von Daten außerhalb des Clusters und/oder AWS. AWS • Stellen Amazon RDS Sie sicher, dass Kunden Daten außerhalb des Clusters speichern und verwalten können.	Kunde • Behalten Sie die Verantwortung für alle auf der Plattform gespeicherten Kundendaten und dafür, wie Kundenanwendungen diese Daten nutzen und offenlegen.
Kundenanwendungen	Red Hat • Stellen Sie Cluster mit installierten OpenShift Komponenten bereit, sodass Kunden auf Kubernetes zugreifen	Kunde • Behalten Sie die Verantwortung für Anwendungen, Daten und den gesamten Anwendungslebenszyklus

Ressource	Wie AWS und Red Hat hilft	Pflichten des Kunden
	können, um APIs container isierte Anwendungen bereitzustellen und zu verwalten. OpenShift • Erstellen Sie Cluster mit geheimen Image-Pull-Secrets, sodass Kundenber eitstellungen Images aus der Red Hat Container Catalog-Registry abrufen können. • Bieten Sie dem Kunden Zugriff OpenShift APIs darauf, damit er Operatore n einrichten kann, um Community- AWS, Drittanbi eter- und RedHat-Services zum Cluster hinzuzufügen. • Stellen Sie Speicherk lassen und Plugins zur Unterstützung persistenter Volumes zur Verwendung mit Kundenanwendungen bereit. • Stellen Sie eine Container-Image-Registrierung bereit, damit Kunden Anwendung scontainer-Images sicher auf dem Cluster speichern können, um Anwendung en bereitzustellen und zu verwalten.	von Kunden und Drittanbi etern bei. • Wenn ein Kunde Red Hat-, Community-, Drittanbieter-, eigene oder andere Dienste mithilfe von Operatoren oder externen Images zum Cluster hinzufügt, ist der Kunde für diese Services und für die Zusammenarbeit mit dem entsprechenden Anbieter (einschließlich Red Hat) verantwortlich, um etwaige Probleme zu beheben. • Verwenden Sie die bereitgestellten Tools und Funktionen, um sie zu konfigurieren und bereitzus tellen, auf dem Laufenden zu bleiben, Ressource nanforderungen und -limits einzurichten, den Cluster so zu dimensionieren, dass er über genügend Ressourcen für die Ausführung von Apps verfügt, Berechtigungen einzurichten, in andere Dienste zu integrieren, alle vom Kunden bereitges tellten Image-Streams oder Vorlagen zu verwalten , extern bereitzustellen, Daten zu speichern, zu

Ressource	Wie AWS und Red Hat hilft	Pflichten des Kunden
	AWS • Sorgen Sie für Amazon EBS die Unterstützung persisten ter Volumes zur Verwendun g mit Kundenanwendungen. • Bereitstellung Amazon S3 zur Unterstützung der Bereitstellung der Container -Image-Registry durch Red Hat.	sichern und wiederher zustellen und anderweitig die hochverfügbaren und belastbaren Workloads zu verwalten. • Behalten Sie die Verantwor tung für die Überwachung der Anwendungen Red Hat OpenShift Service in AWS, auf denen sie ausgeführt werden, einschließlich der Installation und des Betriebs von Software zur Erfassung von Messdaten, zur Erstellung von Warnmeldu ngen und zum Schutz von Geheimnissen in der Anwendung.

ROSA Architektur

Red Hat OpenShift Service in AWS (ROSA) hat die folgenden Cluster-Topologien:

- Gehostete Steuerungsebene (HCP) — Die Kontrollebene wird bei Red Hat gehostet AWS-Konto und von Red Hat verwaltet. Worker-Knoten werden beim Kunden eingesetzt. AWS-Konto
- Klassisch — Die Steuerungsebene und die Worker-Knoten werden beim Kunden bereitgestellt AWS-Konto.

ROSA mit HCP bietet eine effizientere Architektur der Steuerungsebene, die dazu beiträgt, die beim Betrieb anfallenden AWS Infrastrukturgebühren zu reduzieren ROSA und die Clustererstellung zu beschleunigen. Sowohl ROSA mit HCP als auch ROSA Classic können in der AWS ROSA Konsole aktiviert werden. Sie haben die Wahl, welche Architektur Sie verwenden möchten, wenn Sie ROSA Cluster mithilfe der ROSA CLI bereitstellen.

> **Note**
>
> ROSA mit Hosted Control Planes (HCP) bietet FedRAMP High- und HIPAA-Qualified-Compliance-Zertifizierungen an. Weitere Informationen finden Sie unter Compliance in der Red Hat-Dokumentation.

Vergleich von ROSA mit HCP und ROSA Classic

In der folgenden Tabelle wird ROSA mit den klassischen Architekturmodellen HCP und ROSA verglichen.

	ROSA mit HCP	ROSA-Klassiker
Hosting der Cluster-Infrastruktur	Komponenten der Steuerungsebene, wie etcd, API-Server und OAuth, werden in einem Unternehmen von Red Hat gehostet. AWS-Konto	Komponenten der Steuerungsebene, wie etcd, API-Server und OAuth, werden in einem kundeneigenen Unternehmen gehostet. AWS-Konto
Amazon VPC	Worker-Knoten kommunizieren mit der Steuerungsebene über. AWS PrivateLink	Worker Nodes und Control Plane Nodes werden in der VPC des Kunden bereitgestellt.
AWS Identity and Access Management	Verwendet AWS verwaltete Richtlinien.	Verwendet vom Kunden verwaltete Richtlinien, die vom Service definiert werden.
Bereitstellung in mehreren Zonen	Die Steuerungsebene wird in mehreren Availability Zones (AZs) eingesetzt.	Die Kontrollebene kann innerhalb einer einzelnen AZ oder in mehreren AZ bereitgestellt werden AZs.
Infrastrukturknoten	Verwendet keine dedizierten Infrastrukturknoten. Plattformkomponenten werden auf Worker-Knoten bereitgestellt.	Verwendet zwei dedizierte Single-AZ- oder drei dedizierte Multi-AZ-Knoten zum Hosten von Plattformkomponenten.

	ROSA mit HCP	ROSA-Klassiker
OpenShift Fähigkeiten	Plattformüberwachung, Image-Registrierung und der Ingress-Controller werden in den Worker-Knoten bereitgestellt.	Plattformüberwachung, Image-Registrierung und der Ingress-Controller werden in spezielle n Infrastrukturknoten bereitges tellt.
Cluster-Upgrades	Die Steuerungsebene und jeder Maschinenpool können separat aktualisiert werden.	Der gesamte Cluster muss gleichzeitig aktualisiert werden.
Minimaler Amazon EC2 Platzbedarf	Zwei Amazon EC2 Instanzen sind erforderlich, um einen Cluster zu erstellen.	Sieben Single-AZ- oder neun Amazon EC2 Multi-AZ-Instances sind erforderlich, um einen Cluster zu erstellen.
AWS-Regionen	Informationen zur AWS-Regio n Verfügbarkeit finden Sie unter Red Hat OpenShift Service in AWS Endpunkte und Kontingente im AWS Allgemeinen Referenzh andbuch.	Informationen zur AWS-Regio n Verfügbarkeit finden Sie unter Red Hat OpenShift Service in AWS Endpunkte und Kontingente im AWS Allgemeinen Referenzh andbuch.

Fangen Sie an mit ROSA

Red Hat OpenShift Service in AWS (ROSA) ist ein verwalteter Service, mit dem Sie containerisierte Anwendungen mit der Red Hat OpenShift Enterprise Kubernetes-Plattform erstellen, skalieren und bereitstellen können. AWS

Sie können die folgenden Anleitungen verwenden, um Ihren ersten ROSA Cluster zu erstellen, Benutzerzugriff zu gewähren, Ihre erste Anwendung bereitzustellen und zu erfahren, wie Sie den Benutzerzugriff widerrufen und Ihren Cluster löschen können.

- the section called “Einen ROSA HCP-Cluster erstellen — CLI”- Erstellen Sie Ihre erste ROSA mit HCP-Cluster AWS STS und der ROSA CLI.
- the section called “Erstellen Sie einen klassischen ROSA-Cluster - AWS PrivateLink ”- Erstellen Sie Ihren ersten klassischen ROSA-Cluster mit AWS PrivateLink.
- the section called “Erstellen Sie einen klassischen ROSA-Cluster - CLI”- Erstellen Sie Ihren ersten ROSA Classic-Cluster mit AWS STS und der ROSA CLI.

Zur Verwendung eingerichtet ROSA

Um Ihre Umgebung für die Erstellung eines ROSA Clusters vorzubereiten, müssen Sie die folgenden Aktionen ausführen.

Voraussetzungen

Die folgenden Voraussetzungen müssen erfüllt sein, um die ROSA Clustererstellung zu ermöglichen.

- Installieren und konfigurieren Sie die neueste Version AWS CLI. Weitere Informationen finden Sie unter Installieren oder Aktualisierung auf die neueste Version von AWS CLI.
- Installieren und konfigurieren Sie die neueste ROSA CLI und OpenShift Container Platform CLI. Weitere Informationen finden Sie unter Erste Schritte mit der ROSA CLI.
- Sie müssen die erforderlichen Dienstkontingente für Amazon EC2, Amazon VPC Amazon EBS, und festgelegt haben Elastic Load Balancing. AWS oder Red Hat kann in Ihrem Namen eine Erhöhung der Servicekontingenten beantragen, sofern dies zur Problemlösung erforderlich ist. Informationen zu den erforderlichen Servicekontingenten ROSA finden Sie unter Red Hat OpenShift Service in AWS Endpunkte und Kontingente in der AWS Allgemeinen Referenz.

- Um AWS Support für zu erhalten ROSA, müssen Sie die AWS Supportpläne Business, Enterprise On-Ramp oder Enterprise aktivieren. Red Hat kann in Ihrem Namen AWS Support anfordern, sofern dies zur Problemlösung erforderlich ist. Weitere Informationen finden Sie unter the section called “Supportanfragen”. Informationen zur Aktivierung Support finden Sie Support auf der Seite.
- Wenn Sie den Service AWS Organizations zur Verwaltung des AWS-Konten Dienstes verwenden, muss die ROSA Service Control Policy (SCP) der Organisation so konfiguriert sein, dass Red Hat die im SCP aufgeführten Richtlinienaktionen ohne Einschränkungen ausführen kann. Weitere Informationen hierzu finden Sie unter the section called “AWS Organizations Die Dienststeuerungsrichtlinie verweigert die erforderlichen Berechtigungen AWS Marketplace”. Weitere Informationen SCPs dazu finden Sie unter Servicesteuerungsrichtlinien () SCPs.
- Wenn Sie ein ROSA Cluster mit AWS STS einem aktivierten Token bereitstellen, AWS-Region das standardmäßig deaktiviert ist, müssen Sie das Sicherheitstoken AWS-Konto mit dem folgenden Befehl für alle Regionen in der auf Version 2 aktualisieren.

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

  Weitere Informationen zur Aktivierung von Regionen finden Sie unter dem Link: accounts/latest/reference/manage

AWS Voraussetzungen aktivieren ROSA und konfigurieren

Um einen zu erstellen ROSA Cluster, müssen Sie den ROSA Dienst in der AWS ROSA Konsole aktivieren. Die AWS ROSA Konsole überprüft, ob Sie AWS-Konto über die erforderlichen AWS Marketplace Berechtigungen, Dienstkontingente und die benannte Elastic Load Balancing (ELB) - Serviceverknüpfte Rolle verfügen. `AWSServiceRoleForElasticLoadBalancing` Wenn eine dieser Voraussetzungen fehlt, finden Sie in der Konsole Anleitungen zur Konfiguration Ihres Kontos, sodass es die Voraussetzungen erfüllt.

1. Navigieren Sie zur ROSA -Konsole.
2. Wählen Sie Erste Schritte.
3. Wählen Sie auf der Seite ROSA Voraussetzungen überprüfen die Option Ich stimme zu, meine Kontaktinformationen an Red Hat weiterzugeben.
4. Wählen Sie Aktivieren ROSA .

5. Sobald auf der Seite überprüft wurde, ob Ihre Dienstkontingente die ROSA Voraussetzungen erfüllen, und die mit dem ELB-Dienst verknüpfte Rolle erstellt wurde, öffnen Sie eine neue Terminalsitzung, um Ihre erste ROSA Cluster mit der ROSA CLI zu erstellen.

Erstellen Sie einen ROSA mit HCP-Cluster mithilfe der ROSA CLI

In den folgenden Abschnitten werden die ersten Schritte mit ROSA mit gehosteten Steuerungsebenen (ROSA mit HCP) AWS STS und der ROSA CLI beschrieben. Schritte zur Erstellung eines ROSA mit HCP-Clusters mithilfe von Terraform finden Sie in der Red Hat-Dokumentation. Weitere Informationen über den Terraform-Anbieter für die Erstellung von ROSA Clustern finden Sie in der Terraform-Dokumentation.

Die ROSA CLI verwendet `auto` Modus oder `manual` Modus, um die IAM Ressourcen und die OpenID Connect (OIDC) -Konfiguration zu erstellen, die zum Erstellen eines erforderlich sind. ROSA Cluster`auto`mode erstellt automatisch die erforderlichen IAM Rollen und Richtlinien sowie den OIDC-Anbieter. `manual`mode gibt die AWS CLI Befehle aus, die zum manuellen Erstellen der IAM Ressourcen erforderlich sind. Wenn Sie `manual` den Modus verwenden, können Sie die generierten AWS CLI Befehle überprüfen, bevor Sie sie manuell ausführen. `manual`Im Modus können Sie die Befehle auch an einen anderen Administrator oder eine andere Gruppe in Ihrer Organisation weitergeben, sodass dieser die Ressourcen erstellen kann.

Die Verfahren in diesem Dokument verwenden den `auto` Modus der ROSA CLI, um die erforderlichen IAM Ressourcen und die OIDC-Konfiguration für ROSA mit HCP zu erstellen. Weitere Optionen für den Einstieg finden Sie unter. Fangen Sie an mit ROSA

Themen

- Stellen Sie eine Anwendung aus dem Entwicklerkatalog bereit
- Widerrufen cluster-admin Sie die Berechtigungen eines Benutzers
- Widerrufen dedicated-admin Sie die Berechtigungen eines Benutzers
- Widerrufen Sie den Benutzerzugriff auf eine Cluster
- Löschen Sie einen Cluster und AWS STS Ressourcen

Voraussetzungen

Führen Sie die erforderlichen Aktionen aus, die unter aufgeführt sindthe section called “Einrichten”.

Amazon VPC Architektur erstellen

Mit dem folgenden Verfahren wird eine Amazon VPC Architektur erstellt, die zum Hosten eines Clusters verwendet werden kann. Alle Cluster Ressourcen werden im privaten Subnetz gehostet. Das öffentliche Subnetz leitet ausgehenden Verkehr vom privaten Subnetz über ein NAT-Gateway zum öffentlichen Internet weiter. In diesem Beispiel wird der CIDR-Block für die verwendet. `10.0.0.0/16` Amazon VPC Sie können jedoch einen anderen CIDR-Block wählen. Weitere Informationen finden Sie unter Dimensionierung der VPC.

> **Important**
>
> Wenn die Amazon VPC Anforderungen nicht erfüllt sind, schlägt die Clustererstellung fehl.

Example

Terraform

1. Installieren Sie die Terraform-CLI. Weitere Informationen finden Sie in den Installationsanweisungen in der Terraform-Dokumentation.
2. Öffnen Sie eine Terminalsitzung und klonen Sie das Terraform VPC-Repository.

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

3. Navigieren Sie zum erstellten Verzeichnis.

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

4. Initiieren Sie die Terraform-Datei.

```
terraform init
```

   Sobald der Vorgang abgeschlossen ist, gibt die CLI eine Meldung zurück, dass Terraform erfolgreich initialisiert wurde.

5. Führen Sie den folgenden Befehl aus, um einen Terraform-Plan auf der Grundlage der vorhandenen Vorlage zu erstellen. Der AWS-Region muss angegeben werden. Optional können Sie einen Clusternamen angeben.

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

   Sobald der Befehl ausgeführt wurde, wird dem `hypershift-tf` Verzeichnis eine `rosa.tfplan` Datei hinzugefügt. Ausführlichere Optionen finden Sie in der README-Datei des Terraform VPC-Repositorys.

6. Wenden Sie die Plandatei an, um die VPC zu erstellen.

```
terraform apply rosa.tfplan
```

   Nach Abschluss des Vorgangs gab die CLI eine Erfolgsmeldung zurück, in der die hinzugefügten Ressourcen überprüft wurden.

   a. (Optional) Erstellen Sie Umgebungsvariablen für das von Terraform bereitgestellte private, öffentliche und Machinepool-Subnetz, die Sie bei der Erstellung Ihres ROSA mit HCP-Clusters verwenden IDs können.

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

   b. (Optional) Stellen Sie sicher, dass die Umgebungsvariablen korrekt festgelegt wurden.

```
echo $SUBNET_IDS
```

Amazon VPC console

1. Öffnen Sie die Amazon VPC -Konsole.
2. Wählen Sie auf dem VPC-Dashboard Create VPC (VPC erstellen) aus.
3. Wählen Sie unter Zu erstellende Ressourcen die Option VPC und mehr aus.

4. Lassen Sie die automatische Generierung von Namenstags aktiviert, um Namenstags für die VPC-Ressourcen zu erstellen, oder deaktivieren Sie sie, um Ihre eigenen Namenstags für die VPC-Ressourcen bereitzustellen.
5. Geben Sie für IPv4 CIDR-Block einen IPv4 Adressbereich für die VPC ein. Eine VPC muss über einen IPv4 Adressbereich verfügen.
6. (Optional) Um den IPv6 Datenverkehr zu unterstützen, wählen Sie IPv6 CIDR-Block, von Amazon bereitgestellter IPv6 CIDR-Block.
7. Belassen Sie Tenancy als. `Default`
8. Wählen Sie unter Anzahl der Availability Zones (AZs) die Anzahl aus, die Sie benötigen. Für Multi-AZ-Bereitstellungen sind drei Availability Zones ROSA erforderlich. Erweitern Sie Anpassen, um die AZs für Ihre Subnetze auszuwählen. AZs

   > **Note**
   >
   > Einige ROSA Instance-Typen sind nur in ausgewählten Availability Zones verfügbar. Sie können den ROSA `rosa list instance-types` CLI-Befehlsbefehl verwenden, um alle verfügbaren ROSA Instanztypen aufzulisten. Verwenden Sie den AWS CLI Befehl, um zu überprüfen, ob ein Instance-Typ für eine bestimmte Availability Zone verfügbar ist`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

9. Um Ihre Subnetze zu konfigurieren, wählen Sie Werte für Anzahl der öffentlichen Subnetze und Anzahl der privaten Subnetze. Um die IP-Adressbereiche für Ihre Subnetze auszuwählen, erweitern Sie die Option CIDR-Blöcke für Subnetze anpassen.

   > **Note**
   >
   > ROSA mit HCP erfordert, dass Kunden mindestens ein öffentliches und ein privates Subnetz pro Availability Zone konfigurieren, das zur Erstellung von Clustern verwendet wird.

10. Um Ressourcen im privaten Subnetz Zugriff auf das öffentliche Internet zu gewähren IPv4, wählen Sie für NAT-Gateways die Anzahl der Gateways aus, AZs in der NAT-Gateways erstellt werden sollen. In der Produktion empfehlen wir, in jeder AZ ein NAT-Gateway mit Ressourcen bereitzustellen, die Zugriff auf das öffentliche Internet benötigen.

11. (Optional) Wenn Sie Amazon S3 direkt von Ihrer VPC aus zugreifen müssen, wählen Sie VPC-Endpoints, S3 Gateway.
12. Lassen Sie die Standard-DNS-Optionen ausgewählt. ROSA erfordert Unterstützung für DNS-Hostnamen auf der VPC.
13. Erweitern Sie Zusätzliche Tags, wählen Sie Neues Tag hinzufügen und fügen Sie die folgenden Tag-Schlüssel hinzu. ROSA verwendet automatische Preflight-Checks, die überprüfen, ob diese Tags verwendet werden.
    - Schlüssel: `kubernetes.io/role/elb`
    - Schlüssel: `kubernetes.io/role/internal-elb`
14. Wählen Sie VPC erstellen aus.

AWS CLI

1. Erstellen Sie eine VPC mit dem CIDR-Block `10.0.0.0/16`.

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

   Der vorherige Befehl gibt die VPC-ID zurück. Im Folgenden finden Sie eine Beispielausgabe.

```
vpc-1234567890abcdef0
```

2. Speichern Sie die VPC-ID in einer Umgebungsvariablen.

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

3. Erstellen Sie mithilfe der `VPC_ID` Umgebungsvariablen ein `Name` Tag für die VPC.

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

4. Aktivieren Sie die Unterstützung für DNS-Hostnamen auf der VPC.

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

5. Erstellen Sie ein öffentliches und privates Subnetz in der VPC und geben Sie die Availability Zones an, in denen die Ressourcen erstellt werden sollen.

> **Important**
>
> ROSA mit HCP erfordert, dass Kunden mindestens ein öffentliches und ein privates Subnetz pro Availability Zone konfigurieren, die zur Erstellung von Clustern verwendet wird. Für Multi-AZ-Bereitstellungen sind drei Availability Zones erforderlich. Wenn diese Anforderungen nicht erfüllt sind, schlägt die Clustererstellung fehl.

> **Note**
>
> Einige ROSA Instanztypen sind nur in ausgewählten Availability Zones verfügbar. Sie können den ROSA `rosa list instance-types` CLI-Befehlsbefehl verwenden, um alle verfügbaren ROSA Instanztypen aufzulisten. Verwenden Sie den AWS CLI Befehl, um zu überprüfen, ob ein Instance-Typ für eine bestimmte Availability Zone verfügbar ist`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. Speichern Sie das öffentliche und private Subnetz IDs in Umgebungsvariablen.

```
export PUBLIC_SUB=subnet-1234567890abcdef0
```

```
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. Erstellen Sie die folgenden Tags für Ihre VPC-Subnetze. ROSA verwendet automatische Preflight-Prüfungen, die sicherstellen, dass diese Tags verwendet werden.

> **Note**
>
> Sie müssen mindestens ein privates Subnetz und gegebenenfalls ein öffentliches Subnetz taggen.

```
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. Erstellen Sie ein Internet-Gateway und eine Routing-Tabelle für ausgehenden Verkehr. Erstellen Sie eine Routentabelle und eine elastische IP-Adresse für privaten Datenverkehr.

```
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. Speichern Sie die Variablen IDs in der Umgebung.

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

10. Verbinden Sie das Internet-Gateway mit der VPC.

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

11. Ordnen Sie die Tabelle für öffentliche Routen dem öffentlichen Subnetz zu und konfigurieren Sie den Datenverkehr so, dass er zum Internet-Gateway weitergeleitet wird.

```
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. Erstellen Sie das NAT-Gateway und ordnen Sie es der elastischen IP-Adresse zu, um den Verkehr zum privaten Subnetz zu ermöglichen.

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

13. Ordnen Sie die private Routing-Tabelle dem privaten Subnetz zu und konfigurieren Sie den Datenverkehr so, dass er zum NAT-Gateway weitergeleitet wird.

```
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. (Optional) Wiederholen Sie bei Multi-AZ-Bereitstellungen die obigen Schritte, um zwei weitere Availability Zones mit öffentlichen und privaten Subnetzen zu konfigurieren.

Erstellen Sie die erforderlichen IAM Rollen und die OpenID Connect-Konfiguration

Bevor Sie einen ROSA mit HCP-Cluster erstellen, müssen Sie die erforderlichen IAM Rollen und Richtlinien sowie die OpenID Connect (OIDC) -Konfiguration erstellen. Weitere Informationen zu IAM Rollen und Richtlinien für ROSA mit HCP finden Sie unter. the section called “ AWS verwaltete Richtlinien”

Dieses Verfahren verwendet den `auto` Modus der ROSA CLI, um automatisch die OIDC-Konfiguration zu erstellen, die für die Erstellung eines ROSA mit HCP-Clusters erforderlich ist.

1. Erstellen Sie die erforderlichen IAM Kontorollen und Richtlinien. Der `--force-policy-creation` Parameter aktualisiert alle vorhandenen Rollen und Richtlinien. Wenn keine Rollen und Richtlinien vorhanden sind, erstellt der Befehl stattdessen diese Ressourcen.

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

   > **Note**
   >
   > Wenn Ihr Offline-Zugriffstoken abgelaufen ist, gibt die ROSA CLI eine Fehlermeldung aus, die besagt, dass Ihr Autorisierungstoken aktualisiert werden muss. Schritte zur Fehlerbehebung finden Sie unterthe section called “Fehlerbehebung bei abgelaufenen Offline-Zugriffstoken für ROSA CLI”.

2. Erstellen Sie die OpenID Connect (OIDC) -Konfiguration, die die Benutzerauthentifizierung für den Cluster ermöglicht. Diese Konfiguration ist für die Verwendung mit OpenShift Cluster Manager (OCM) registriert.

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

3. Kopieren Sie die in der ROSA CLI-Ausgabe angegebene OIDC-Konfigurations-ID. Die OIDC-Konfigurations-ID muss später bereitgestellt werden, um den ROSA mit HCP-Cluster zu erstellen.
4. Führen Sie den folgenden Befehl aus, um die OIDC-Konfigurationen zu überprüfen, die für Cluster verfügbar sind, die Ihrer Benutzerorganisation zugeordnet sind.

   ```
   rosa list oidc-config
   ```

5. Erstellen Sie die erforderlichen IAM Operatorrollen und <OIDC_CONFIG_ID> ersetzen Sie sie durch die zuvor kopierte OIDC-Konfigurations-ID.

   Example

   > **Important**
   >
   > <PREFIX_NAME>Bei der Erstellung der Operatorrollen müssen Sie ein Präfix angeben. Wenn Sie dies nicht tun, wird ein Fehler ausgegeben.

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

6. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die IAM Operatorrollen erstellt wurden:

   ```
   rosa list operator-roles
   ```

Erstellen Sie einen ROSA mit HCP-Cluster mithilfe der ROSA CLI und AWS STS

Sie können eine ROSA mit HCP Cluster mithilfe von AWS -Security-Token-Service (AWS STS) und dem in der ROSA CLI bereitgestellten `auto` Modus erstellen. Sie haben die Möglichkeit, einen Cluster mit einer öffentlichen API und Ingress oder einer privaten API und Ingress zu erstellen.

Sie können eine Cluster mit einer einzigen Availability Zone (Single-AZ) oder mehreren Availability Zones (Multi-AZ) erstellen. In beiden Fällen muss der CIDR-Wert Ihrer Maschine mit dem CIDR-Wert Ihrer VPC übereinstimmen.

Im folgenden Verfahren wird der `rosa create cluster --hosted-cp` Befehl verwendet, um eine Single-AZ-ROSA mit HCP zu erstellen. Cluster Um ein Multi-AZ zu erstellen Cluster, geben Sie `multi-az` im Befehl das private Subnetz IDs für jedes private Subnetz an, in dem Sie die Bereitstellung durchführen möchten.

1. Erstellen Sie mit einem der folgenden Befehle einen ROSA-Cluster mit HCP.

- Erstellen Sie einen ROSA mit HCP-Cluster mit einer öffentlichen API und Ingress und geben Sie dabei den Clusternamen, das Operatorrollenpräfix, die OIDC-Konfigurations-ID sowie das öffentliche und private Subnetz an. 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>
```

- Erstellen Sie einen ROSA mit HCP-Cluster mit einer privaten API und Ingress und geben Sie dabei den Clusternamen, das Operatorrollenpräfix, die OIDC-Konfigurations-ID und das private Subnetz an. IDs

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

2. Überprüfen Sie den Status Ihres. Cluster

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

> **Note**
>
> Wenn der Erstellungsvorgang fehlschlägt oder das `State` Feld nach 10 Minuten nicht den Status „Bereit“ annimmt, finden Sie weitere Informationen unterFehlerbehebung.
> Wenn Sie Hilfe benötigen, Support wenden Sie sich an unseren Red Hat Support, siehethe section called “Supportanfragen”.

3. Verfolgen Sie den Fortschritt der Cluster Erstellung, indem Sie sich die OpenShift Installationsprotokolle ansehen.

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

Konfigurieren Sie einen Identitätsanbieter und gewähren Cluster Sie Zugriff

ROSA beinhaltet einen integrierten OAuth Server. Nachdem Sie Ihren Cluster erstellt haben, müssen Sie ihn OAuth für die Verwendung eines Identitätsanbieters konfigurieren. Anschließend können Sie Benutzer zu Ihrem konfigurierten Identitätsanbieter hinzufügen, um ihnen Zugriff auf Ihren

zu gewähren Cluster. Sie können diesen Benutzern `cluster-admin` oder `dedicated-admin` Berechtigungen nach Bedarf gewähren.

Sie können verschiedene Identitätsanbietertypen für Ihren konfigurieren ROSA Cluster. Zu den unterstützten Typen gehören GitHub Enterprise GitHub GitLab, Google, LDAP, OpenID Connect und HTPasswd Identitätsanbieter.

> **Important**
>
> Der HTPasswd Identitätsanbieter ist nur enthalten, um die Erstellung eines einzelnen statischen Administratorbenutzers zu ermöglichen. HTPasswd wird nicht als allgemein verwendbarer Identitätsanbieter für unterstützt. ROSA

Das folgende Verfahren konfiguriert als Beispiel einen GitHub Identitätsanbieter. Anweisungen zur Konfiguration der einzelnen unterstützten Identitätsanbietertypen finden Sie unter Konfiguration von Identitätsanbietern für AWS STS.

1. Navigieren Sie zu github.com und melden Sie sich bei Ihrem GitHub Konto an.
2. Wenn Sie keine GitHub Organisation haben, die Sie für die Bereitstellung von Identitäten verwenden können Cluster, erstellen Sie eine. Weitere Informationen finden Sie in den Schritten in der GitHub Dokumentation.
3. Konfigurieren Sie im interaktiven Modus der ROSA CLI einen Identitätsanbieter für Ihren Cluster.

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

4. Folgen Sie den Konfigurationsanweisungen in der Ausgabe, um den Cluster Zugriff auf Mitglieder Ihrer GitHub Organisation zu beschränken.

```
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. Öffnen Sie die URL in der Ausgabe und ersetzen Sie sie durch den Namen Ihrer GitHub Organisation.
6. Wählen Sie auf der GitHub Webseite Anwendung registrieren aus, um eine neue OAuth Anwendung in Ihrer GitHub Organisation zu registrieren.
7. Verwenden Sie die Informationen GitHub OAuth auf der Seite, um die verbleibenden `rosa create idp` interaktiven Eingabeaufforderungen auszufüllen, indem Sie den folgenden Befehl ausführen. Ersetzen Sie <GITHUB_CLIENT_ID> und <GITHUB_CLIENT_SECRET> durch die Anmeldeinformationen aus Ihrer GitHub OAuth Anwendung.

```
...
? 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**
>
> Es kann ungefähr zwei Minuten dauern, bis die Identity Provider-Konfiguration aktiv wird. Wenn Sie einen `cluster-admin` Benutzer konfiguriert haben, können Sie ihn ausführen, `oc get pods -n openshift-authentication --watch` um zu beobachten, wie die OAuth Pods mit der aktualisierten Konfiguration erneut bereitgestellt werden.

8. Stellen Sie sicher, dass der Identitätsanbieter korrekt konfiguriert ist.

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

Gewähren Sie dem Benutzer Zugriff auf eine Cluster

Sie können einem Benutzer Zugriff auf Ihre gewähren, Cluster indem Sie ihn dem konfigurierten Identitätsanbieter hinzufügen.

Das folgende Verfahren fügt einen Benutzer zu einer GitHub Organisation hinzu, die für die Identitätsbereitstellung im Cluster konfiguriert ist.

1. Navigieren Sie zu github.com und melden Sie sich bei Ihrem GitHub Konto an.
2. Laden Sie Benutzer ein, die Cluster Zugriff auf Ihre GitHub Organisation benötigen. Weitere Informationen finden Sie in der GitHub Dokumentation unter Benutzer einladen, Ihrer Organisation beizutreten.

Konfigurieren von **`cluster-admin`**-Berechtigungen

1. Erteilen Sie die `cluster-admin` Berechtigungen, indem Sie den folgenden Befehl ausführen. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer- und Clusternamen.

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

2. Stellen Sie sicher, dass der Benutzer als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Konfigurieren von **`dedicated-admin`**-Berechtigungen

1. Erteilen Sie die `dedicated-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer und Cluster Namen, indem Sie den folgenden Befehl ausführen.

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

2. Stellen Sie sicher, dass der Benutzer als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Greifen Sie Cluster über die Red Hat Hybrid Cloud Console auf a zu

Melden Sie sich Cluster über die Red Hat Hybrid Cloud Console bei Ihrem an.

1. Rufen Sie die Konsolen-URL für Sie Cluster mit dem folgenden Befehl ab. `<CLUSTER_NAME>`Ersetzen Sie durch den Namen Ihres Cluster.

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

2. Navigieren Sie in der Ausgabe zur Konsolen-URL und melden Sie sich an.

   Wählen Sie im Dialogfeld Anmelden mit... den Namen des Identitätsanbieters und füllen Sie alle Autorisierungsanfragen Ihres Anbieters aus.

Stellen Sie eine Anwendung aus dem Entwicklerkatalog bereit

Von der Red Hat Hybrid Cloud Console aus können Sie eine Developer Catalog-Testanwendung bereitstellen und sie mit einer Route verfügbar machen.

1. Navigieren Sie zur Red Hat Hybrid Cloud Console und wählen Sie den Cluster aus, in dem Sie die App bereitstellen möchten.
2. Wählen Sie auf der Seite des Clusters Open Console aus.
3. Wählen Sie in der Administratorperspektive Startseite > Projekte > Projekt erstellen aus.
4. Geben Sie einen Namen für Ihr Projekt ein und fügen Sie optional einen Anzeigenamen und eine Beschreibung hinzu.
5. Wählen Sie Erstellen, um das Projekt zu erstellen.
6. Wechseln Sie zur Entwicklerperspektive und wählen Sie +Hinzufügen. Stellen Sie sicher, dass das ausgewählte Projekt das ist, das gerade erstellt wurde.
7. Wählen Sie im Dialogfeld „Entwicklerkatalog“ die Option Alle Dienste aus.
8. Wählen Sie auf der Seite mit dem Entwicklerkatalog im Menü Sprachen > JavaScriptaus.
9. Wählen Sie Node.js und dann Anwendung erstellen, um die Seite „ Source-to-ImageAnwendung erstellen“ zu öffnen.

> **Note**
>
> Möglicherweise müssen Sie Alle Filter löschen auswählen, um die Option Node.js anzuzeigen.

10. Wählen Sie im Abschnitt Git die Option Try Sample aus.
11. Fügen Sie im Feld Name einen eindeutigen Namen hinzu.
12. Wählen Sie Erstellen aus.

> **Note**
>
> Die Bereitstellung der neuen Anwendung dauert mehrere Minuten.

13. Wenn die Bereitstellung abgeschlossen ist, wählen Sie die Route-URL für die Anwendung aus.

    Im Browser wird eine neue Registerkarte mit einer Meldung geöffnet, die der folgenden ähnelt.

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

14. (Optional) Löschen Sie die Anwendung und bereinigen Sie die Ressourcen:
    a. Wählen Sie in der Administratorperspektive „Startseite“ > „Projekte“.
    b. Öffnen Sie das Aktionsmenü für Ihr Projekt und wählen Sie Projekt löschen.

Widerrufen **`cluster-admin`** Sie die Berechtigungen eines Benutzers

1. Widerrufen Sie die `cluster-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer und Cluster Namen.

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

2. Stellen Sie sicher, dass der Benutzer nicht als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Widerrufen **`dedicated-admin`** Sie die Berechtigungen eines Benutzers

1. Widerrufen Sie die `dedicated-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer und Cluster Namen.

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

2. Stellen Sie sicher, dass der Benutzer nicht als Mitglied der `dedicated-admins` Gruppe aufgeführt ist.

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

Widerrufen Sie den Benutzerzugriff auf eine Cluster

Sie können einem Identity Provider-Benutzer den Cluster Zugriff entziehen, indem Sie ihn aus dem konfigurierten Identity Provider entfernen.

Sie können verschiedene Arten von Identitätsanbietern für Ihren konfigurieren Cluster. Mit dem folgenden Verfahren wird einem Mitglied einer GitHub Organisation der Cluster Zugriff entzogen.

1. Navigieren Sie zu github.com und melden Sie sich bei Ihrem GitHub Konto an.
2. Entferne den Benutzer aus deiner GitHub Organisation. Weitere Informationen finden Sie in der GitHub Dokumentation unter Ein Mitglied aus Ihrer Organisation entfernen.

Löschen Sie einen Cluster und AWS STS Ressourcen

Sie können die ROSA CLI verwenden, um eine zu löschen Cluster , die AWS -Security-Token-Service (AWS STS) verwendet. Sie können die ROSA CLI auch verwenden, um die IAM Rollen und den OIDC-Anbieter zu löschen, die von erstellt wurden. ROSA Um die von erstellten IAM Richtlinien zu löschen ROSA, können Sie die IAM Konsole verwenden.

> **Note**
>
> IAM Rollen und Richtlinien, die von erstellt wurden, ROSA können von anderen ROSA Clustern im selben Konto verwendet werden.

1. Löschen Sie die Cluster und sehen Sie sich die Protokolle an. <CLUSTER_NAME>Ersetzen Sie durch den Namen oder die ID Ihres Cluster.

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

> **Important**
>
> Sie müssen warten Cluster , bis der vollständig gelöscht ist, bevor Sie die IAM Rollen, Richtlinien und den OIDC-Anbieter entfernen. Die IAM-Rollen des Kontos sind erforderlich, um die vom Installationsprogramm erstellten Ressourcen zu löschen. Die Operator-IAM-Rollen sind erforderlich, um die von den Operatoren erstellten Ressourcen zu bereinigen. OpenShift Die Operatoren verwenden den OIDC-Anbieter zur Authentifizierung.

2. Löschen Sie den OIDC-Anbieter, den die Cluster Operatoren zur Authentifizierung verwenden, indem Sie den folgenden Befehl ausführen.

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

3. Löschen Sie die clusterspezifischen Operatorrollen. IAM

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

4. Löschen Sie die IAM-Rollen des Kontos mithilfe des folgenden Befehls. <PREFIX>Ersetzen Sie es durch das Präfix der zu löschenden Konto-IAM-Rollen. Wenn Sie bei der Erstellung der Account-IAM-Rollen ein benutzerdefiniertes Präfix angegeben haben, geben Sie das `ManagedOpenShift` Standardpräfix an.

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

5. Löschen Sie die IAM Richtlinien, die von ROSA erstellt wurden.
   a. Melden Sie sich bei der IAM -Konsole an.
   b. Wählen Sie im linken Menü unter Zugriffsverwaltung die Option Richtlinien aus.
   c. Wählen Sie die Richtlinie aus, die Sie löschen möchten, und wählen Sie Aktionen > Löschen.
   d. Geben Sie den Richtliniennamen ein und wählen Sie Löschen aus.
   e. Wiederholen Sie diesen Schritt, um alle IAM-Richtlinien für zu löschen. Cluster

Erstellen Sie mit der ROSA CLI einen klassischen ROSA-Cluster

In den folgenden Abschnitten wird beschrieben, wie Sie mit der Verwendung von ROSA classic AWS STS und der ROSA CLI beginnen. Die Schritte zur Erstellung eines klassischen ROSA Clusters mit Terraform finden Sie in der Red Hat-Dokumentation. Weitere Informationen über den Terraform-Anbieter für die Erstellung von ROSA Clustern finden Sie in der Terraform-Dokumentation.

Die ROSA CLI verwendet `auto` Modus oder `manual` Modus, um die IAM Ressourcen zu erstellen, die für die Bereitstellung von a erforderlich sind ROSA Cluster. `auto`mode erstellt sofort die erforderlichen IAM Rollen und Richtlinien sowie einen OpenID Connect (OIDC) -Anbieter. `manual`mode gibt die AWS CLI Befehle aus, die zum Erstellen der Ressourcen benötigt werden. IAM Wenn Sie `manual` den Modus verwenden, können Sie die generierten AWS CLI Befehle überprüfen, bevor Sie sie manuell ausführen. `manual`Im Modus können Sie die Befehle auch an einen anderen Administrator oder eine andere Gruppe in Ihrer Organisation weitergeben, sodass dieser die Ressourcen erstellen kann.

Weitere Optionen für den Einstieg finden Sie unterFangen Sie an mit ROSA .

Themen

Voraussetzungen

Führen Sie die erforderlichen Aktionen aus, die unter aufgeführt sindthe section called “Einrichten”.

Erstellen Sie mit der ROSA CLI einen klassischen ROSA-Cluster und AWS STS

Sie können einen ROSA-Klassiker Cluster mit der ROSA CLI und erstellen AWS STS.

1. Erstellen Sie die erforderlichen IAM Kontorollen und Richtlinien mit `--mode auto` oder`--mode manual`.

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

   > **Note**
   >
   > Wenn Ihr Offline-Zugriffstoken abgelaufen ist, gibt die ROSA CLI eine Fehlermeldung aus, die besagt, dass Ihr Autorisierungstoken aktualisiert werden muss. Schritte zur Fehlerbehebung finden Sie unterthe section called “Fehlerbehebung bei abgelaufenen Offline-Zugriffstoken für ROSA CLI”.

2. Erstellen Sie eine Cluster mit `--mode auto` oder`--mode manual`. `auto`Im Modus können Sie schneller einen Cluster erstellen. `manual`mode fordert Sie auf, benutzerdefinierte Einstellungen für Ihren Cluster anzugeben.

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

   > **Note**
   >
   > Wenn Sie angeben`--mode auto`, erstellt der `rosa create cluster` Befehl automatisch die clusterspezifischen IAM Operatorrollen und den OIDC-Anbieter. Die Operatoren verwenden den OIDC-Anbieter zur Authentifizierung.

> **Note**
>
> Bei Verwendung der `--mode auto` Standardeinstellungen wird die neueste stabile OpenShift Version installiert.

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

> **Important**
>
> Wenn Sie die etcd-Verschlüsselung im `manual` Modus aktivieren, entsteht ein Leistungsaufwand von ca. 20%. Der Mehraufwand ist auf die Einführung dieser zweiten Verschlüsselungsebene zusätzlich zur standardmäßigen Amazon EBS-Verschlüsselung zurückzuführen, die die etcd-Volumes verschlüsselt.

> **Note**
>
> Nach dem `manual` Ausführungsmodus zum Erstellen des Clusters müssen Sie clusterspezifische Operator-IAM-Rollen und den OpenID Connect-Anbieter, den Clusterbetreiber zur Authentifizierung verwenden, manuell erstellen.

3. Überprüfen Sie den Status Ihres. Cluster

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

> **Note**
>
> Wenn der Bereitstellungsvorgang fehlschlägt oder das `State` Feld nach 40 Minuten nicht den Status „Bereit“ annimmt, finden Sie weitere Informationen unterFehlerbehebung. Wenn Sie Hilfe benötigen, Support wenden Sie sich an unseren Red Hat Support, siehethe section called “Supportanfragen”.

4. Verfolgen Sie den Fortschritt der Cluster Erstellung, indem Sie sich die OpenShift Installationsprotokolle ansehen.
```

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

Konfigurieren Sie einen Identitätsanbieter und gewähren Cluster Sie Zugriff

ROSA beinhaltet einen integrierten OAuth Server. Nachdem Sie Ihren Cluster erstellt haben, müssen Sie ihn OAuth für die Verwendung eines Identitätsanbieters konfigurieren. Anschließend können Sie Benutzer zu Ihrem konfigurierten Identitätsanbieter hinzufügen, um ihnen Zugriff auf Ihren zu gewähren Cluster. Sie können diesen Benutzern `cluster-admin` oder `dedicated-admin` Berechtigungen nach Bedarf gewähren.

Sie können verschiedene Identitätsanbietertypen für Ihren konfigurieren ROSA Cluster. Zu den unterstützten Typen gehören GitHub Enterprise GitHub GitLab, Google, LDAP, OpenID Connect und HTPasswd Identitätsanbieter.

> **Important**
>
> Der HTPasswd Identitätsanbieter ist nur enthalten, um die Erstellung eines einzelnen statischen Administratorbenutzers zu ermöglichen. HTPasswd wird nicht als allgemein verwendbarer Identitätsanbieter für unterstützt. ROSA

Im folgenden Verfahren wird ein GitHub Identitätsanbieter als Beispiel konfiguriert. Anweisungen zur Konfiguration der einzelnen unterstützten Identitätsanbietertypen finden Sie unter Konfiguration von Identitätsanbietern für AWS STS.

1. Navigieren Sie zu github.com und melden Sie sich bei Ihrem GitHub Konto an.
2. Wenn Sie keine GitHub Organisation haben, die Sie für die Identitätsbereitstellung verwenden können Cluster, erstellen Sie eine. Weitere Informationen finden Sie in den Schritten in der GitHub Dokumentation.
3. Konfigurieren Sie im interaktiven Modus der ROSA CLI einen Identitätsanbieter für Ihren Cluster.

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

4. Folgen Sie den Konfigurationsanweisungen in der Ausgabe, um den Cluster Zugriff auf Mitglieder Ihrer GitHub Organisation zu beschränken.

   ```
   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. Öffnen Sie die URL in der Ausgabe und ersetzen Sie sie durch den Namen Ihrer GitHub Organisation.
6. Wählen Sie auf der GitHub Webseite Anwendung registrieren aus, um eine neue OAuth Anwendung in Ihrer GitHub Organisation zu registrieren.
7. Verwenden Sie die Informationen GitHub OAuth auf der Seite, um die verbleibenden `rosa create idp` interaktiven Eingabeaufforderungen auszufüllen, indem Sie den folgenden Befehl ausführen. Ersetzen Sie <GITHUB_CLIENT_ID> und <GITHUB_CLIENT_SECRET> durch die Anmeldeinformationen aus Ihrer GitHub OAuth Anwendung.

```
...
? 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**
>
> Es kann ungefähr zwei Minuten dauern, bis die Identity Provider-Konfiguration aktiv wird. Wenn Sie einen `cluster-admin` Benutzer konfiguriert haben, können Sie ihn ausführen, `oc get pods -n openshift-authentication --watch` um zu beobachten, wie die OAuth Pods mit der aktualisierten Konfiguration erneut bereitgestellt werden.

8. Stellen Sie sicher, dass der Identitätsanbieter korrekt konfiguriert ist.

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

Gewähren Sie dem Benutzer Zugriff auf eine Cluster

Sie können einem Benutzer Zugriff auf Ihre gewähren, Cluster indem Sie ihn dem konfigurierten Identitätsanbieter hinzufügen.

Das folgende Verfahren fügt einen Benutzer zu einer GitHub Organisation hinzu, die für die Identitätsbereitstellung im Cluster konfiguriert ist.

1. Navigieren Sie zu github.com und melden Sie sich bei Ihrem GitHub Konto an.
2. Laden Sie Benutzer ein, die Cluster Zugriff auf Ihre GitHub Organisation benötigen. Weitere Informationen finden Sie in der GitHub Dokumentation unter Benutzer einladen, Ihrer Organisation beizutreten.

Konfigurieren von **`cluster-admin`**-Berechtigungen

1. Erteilen Sie die `cluster-admin` Berechtigungen, indem Sie den folgenden Befehl ausführen. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer- und Clusternamen.

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

2. Stellen Sie sicher, dass der Benutzer als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Konfigurieren von **`dedicated-admin`**-Berechtigungen

1. Erteilen Sie die `dedicated-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer und Cluster Namen, indem Sie den folgenden Befehl ausführen.

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

2. Stellen Sie sicher, dass der Benutzer als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Greifen Sie Cluster über die Red Hat Hybrid Cloud Console auf a zu

Nachdem Sie einen Cluster Administratorbenutzer erstellt oder einen Benutzer zu Ihrem konfigurierten Identity Provider hinzugefügt haben, können Sie sich Cluster über die Red Hat Hybrid Cloud Console bei Ihrem anmelden.

1. Rufen Sie die Konsolen-URL für Sie Cluster mit dem folgenden Befehl ab. `<CLUSTER_NAME>`Ersetzen Sie durch den Namen Ihres Cluster.

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

2. Navigieren Sie in der Ausgabe zur Konsolen-URL und melden Sie sich an.
   - Wenn Sie einen `cluster-admin` Benutzer erstellt haben, melden Sie sich mit den angegebenen Anmeldeinformationen an.
   - Wenn Sie einen Identitätsanbieter für Ihren konfiguriert haben Cluster, wählen Sie den Namen des Identitätsanbieters im Dialogfeld Anmelden mit... aus und füllen Sie alle Autorisierungsanfragen Ihres Anbieters aus.

Stellen Sie eine Anwendung aus dem Entwicklerkatalog bereit

Von der Red Hat Hybrid Cloud Console aus können Sie eine Developer Catalog-Testanwendung bereitstellen und sie mit einer Route verfügbar machen.

1. Navigieren Sie zur Red Hat Hybrid Cloud Console und wählen Sie den Cluster aus, in dem Sie die App bereitstellen möchten.

2. Wählen Sie auf der Seite des Clusters Open Console aus.
3. Wählen Sie in der Administratorperspektive Startseite > Projekte > Projekt erstellen aus.
4. Geben Sie einen Namen für Ihr Projekt ein und fügen Sie optional einen Anzeigenamen und eine Beschreibung hinzu.
5. Wählen Sie Erstellen, um das Projekt zu erstellen.
6. Wechseln Sie zur Entwicklerperspektive und wählen Sie +Hinzufügen. Stellen Sie sicher, dass das ausgewählte Projekt das ist, das gerade erstellt wurde.
7. Wählen Sie im Dialogfeld „Entwicklerkatalog“ die Option Alle Dienste aus.
8. Wählen Sie auf der Seite mit dem Entwicklerkatalog im Menü Sprachen > JavaScriptaus.
9. Wählen Sie Node.js und dann Anwendung erstellen, um die Seite „ Source-to-ImageAnwendung erstellen“ zu öffnen.

> **Note**
>
> Möglicherweise müssen Sie Alle Filter löschen auswählen, um die Option Node.js anzuzeigen.

10. Wählen Sie im Abschnitt Git die Option Try Sample aus.
11. Fügen Sie im Feld Name einen eindeutigen Namen hinzu.
12. Wählen Sie Erstellen aus.

> **Note**
>
> Die Bereitstellung der neuen Anwendung dauert mehrere Minuten.

13. Wenn die Bereitstellung abgeschlossen ist, wählen Sie die Route-URL für die Anwendung aus.

    Im Browser wird eine neue Registerkarte mit einer Meldung geöffnet, die der folgenden ähnelt.

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

14. (Optional) Löschen Sie die Anwendung und bereinigen Sie die Ressourcen:
    a. Wählen Sie in der Administratorperspektive „Startseite“ > „Projekte“.
    b. Öffnen Sie das Aktionsmenü für Ihr Projekt und wählen Sie Projekt löschen.

Widerrufen **`cluster-admin`** Sie die Berechtigungen eines Benutzers

1. Widerrufen Sie die `cluster-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer und Cluster Namen.

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

2. Stellen Sie sicher, dass der Benutzer nicht als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Widerrufen **`dedicated-admin`** Sie die Berechtigungen eines Benutzers

1. Widerrufen Sie die `dedicated-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer und Cluster Namen.

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

2. Stellen Sie sicher, dass der Benutzer nicht als Mitglied der `dedicated-admins` Gruppe aufgeführt ist.

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

Widerrufen Sie den Benutzerzugriff auf eine Cluster

Sie können einem Identity Provider-Benutzer den Cluster Zugriff entziehen, indem Sie ihn aus dem konfigurierten Identity Provider entfernen.

Sie können verschiedene Arten von Identitätsanbietern für Ihren konfigurieren Cluster. Mit dem folgenden Verfahren wird einem Mitglied einer GitHub Organisation der Cluster Zugriff entzogen.

1. Navigieren Sie zu github.com und melden Sie sich bei Ihrem GitHub Konto an.
2. Entferne den Benutzer aus deiner GitHub Organisation. Weitere Informationen finden Sie in der GitHub Dokumentation unter Ein Mitglied aus Ihrer Organisation entfernen.

Löschen Sie einen Cluster und AWS STS Ressourcen

Sie können die ROSA CLI verwenden, um eine zu löschen Cluster , die AWS -Security-Token-Service (AWS STS) verwendet. Sie können die ROSA CLI auch verwenden, um die IAM Rollen und den OIDC-Anbieter zu löschen, die von erstellt wurden. ROSA Um die von erstellten IAM Richtlinien zu löschen ROSA, können Sie die IAM Konsole verwenden.

> **Important**
>
> IAM Rollen und Richtlinien, die von erstellt wurden, ROSA können von anderen ROSA Clustern im selben Konto verwendet werden.

1. Löschen Sie die Cluster und sehen Sie sich die Protokolle an. `<CLUSTER_NAME>`Ersetzen Sie durch den Namen oder die ID Ihres Cluster.

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

> **Important**
>
> Sie müssen warten Cluster , bis der vollständig gelöscht ist, bevor Sie die IAM Rollen, Richtlinien und den OIDC-Anbieter entfernen. Die IAM-Rollen des Kontos sind erforderlich, um die vom Installationsprogramm erstellten Ressourcen zu löschen. Die Operator-IAM-Rollen sind erforderlich, um die von den Operatoren erstellten Ressourcen zu bereinigen. OpenShift Die Operatoren verwenden den OIDC-Anbieter zur Authentifizierung.

2. Löschen Sie den OIDC-Anbieter, den die Cluster Operatoren zur Authentifizierung verwenden, indem Sie den folgenden Befehl ausführen.

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

3. Löschen Sie die clusterspezifischen Operatorrollen. IAM

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

4. Löschen Sie die IAM-Rollen des Kontos mithilfe des folgenden Befehls. `<PREFIX>`Ersetzen Sie es durch das Präfix der zu löschenden Konto-IAM-Rollen. Wenn Sie bei der Erstellung der Account-

IAM-Rollen ein benutzerdefiniertes Präfix angegeben haben, geben Sie das `ManagedOpenShift` Standardpräfix an.

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

5. Löschen Sie die IAM Richtlinien, die von ROSA erstellt wurden.
   a. Melden Sie sich bei der IAM -Konsole an.
   b. Wählen Sie im linken Menü unter Zugriffsverwaltung die Option Richtlinien aus.
   c. Wählen Sie die Richtlinie aus, die Sie löschen möchten, und wählen Sie Aktionen > Löschen.
   d. Geben Sie den Richtliniennamen ein und wählen Sie Löschen aus.
   e. Wiederholen Sie diesen Schritt, um alle IAM-Richtlinien für zu löschen. Cluster

Erstellen Sie einen klassischen ROSA-Cluster, der Folgendes verwendet AWS PrivateLink

Die klassischen ROSA-Cluster können auf verschiedene Arten bereitgestellt werden: öffentlich, privat oder privat mit AWS PrivateLink. Weitere Informationen zu ROSA classic finden Sie unterthe section called “Architektur”. Sowohl bei öffentlichen als auch bei privaten Cluster Konfigurationen OpenShift Cluster hat der Zugriff auf das Internet, und der Datenschutz für die Anwendungs-Workloads wird auf der Anwendungsebene festgelegt.

Wenn Sie möchten, dass Cluster sowohl die Workloads als auch die Anwendungs-Workloads privat sind, können Sie sie AWS PrivateLink mit ROSA classic konfigurieren. AWS PrivateLink ist eine hochverfügbare, skalierbare Technologie, ROSA mit der eine private Verbindung zwischen den ROSA Service- und Clusterressourcen im AWS Kundenkonto hergestellt wird. Damit AWS PrivateLink kann das RedHat Site Reliability Engineering (SRE) -Team zu Support- und Problembehebungszwecken auf den Cluster zugreifen, indem es ein privates Subnetz verwendet, das mit dem Endpunkt des Clusters verbunden ist AWS PrivateLink .

Weitere Informationen zu finden Sie AWS PrivateLink unter Was ist? AWS PrivateLink

Themen

- Voraussetzungen
- Amazon VPC Architektur erstellen
- Erstellen Sie einen klassischen ROSA-Cluster mit der ROSA CLI und AWS PrivateLink

- Konfigurieren Sie die AWS PrivateLink DNS-Weiterleitung
- Konfigurieren Sie einen Identitätsanbieter und gewähren Cluster Sie Zugriff
- Gewähren Sie dem Benutzer Zugriff auf eine Cluster
- Konfigurieren von cluster-admin-Berechtigungen
- Konfigurieren von dedicated-admin-Berechtigungen
- Greifen Sie Cluster über die Red Hat Hybrid Cloud Console auf a zu
- Stellen Sie eine Anwendung aus dem Entwicklerkatalog bereit
- Widerrufen cluster-admin Sie die Berechtigungen eines Benutzers
- Widerrufen dedicated-admin Sie die Berechtigungen eines Benutzers
- Widerrufen Sie den Benutzerzugriff auf eine Cluster
- Löschen Sie einen Cluster und AWS STS Ressourcen

Voraussetzungen

Führen Sie die erforderlichen Aktionen aus, die unter aufgeführt sindthe section called “Einrichten”.

Amazon VPC Architektur erstellen

Mit dem folgenden Verfahren wird eine Amazon VPC Architektur erstellt, die zum Hosten eines Clusters verwendet werden kann. Alle Cluster Ressourcen werden im privaten Subnetz gehostet. Das öffentliche Subnetz leitet ausgehenden Verkehr vom privaten Subnetz über ein NAT-Gateway zum öffentlichen Internet weiter. In diesem Beispiel wird der CIDR-Block für die verwendet. `10.0.0.0/16` Amazon VPC Sie können jedoch einen anderen CIDR-Block wählen. Weitere Informationen finden Sie unter Dimensionierung der VPC.

> **Important**
>
> Wenn die Amazon VPC Anforderungen nicht erfüllt sind, schlägt die Clustererstellung fehl.

Example

Amazon VPC console

1. Öffnen Sie die Amazon VPC -Konsole.

2. Wählen Sie auf dem VPC-Dashboard Create VPC (VPC erstellen) aus.
3. Wählen Sie unter Zu erstellende Ressourcen die Option VPC und mehr aus.
4. Lassen Sie die automatische Generierung von Namenstags aktiviert, um Namenstags für die VPC-Ressourcen zu erstellen, oder deaktivieren Sie sie, um Ihre eigenen Namenstags für die VPC-Ressourcen bereitzustellen.
5. Geben Sie für IPv4 CIDR-Block einen IPv4 Adressbereich für die VPC ein. Eine VPC muss über einen IPv4 Adressbereich verfügen.
6. (Optional) Um den IPv6 Datenverkehr zu unterstützen, wählen Sie IPv6 CIDR-Block, von Amazon bereitgestellter IPv6 CIDR-Block.
7. Belassen Sie Tenancy als. `Default`
8. Wählen Sie unter Anzahl der Availability Zones (AZs) die Anzahl aus, die Sie benötigen. Für Multi-AZ-Bereitstellungen sind drei Availability Zones ROSA erforderlich. Erweitern Sie Anpassen, um die AZs für Ihre Subnetze auszuwählen. AZs

   > **Note**
   >
   > Einige ROSA Instance-Typen sind nur in ausgewählten Availability Zones verfügbar. Sie können den ROSA `rosa list instance-types` CLI-Befehlsbefehl verwenden, um alle verfügbaren ROSA Instanztypen aufzulisten. Verwenden Sie den AWS CLI Befehl, um zu überprüfen, ob ein Instance-Typ für eine bestimmte Availability Zone verfügbar ist`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

9. Um Ihre Subnetze zu konfigurieren, wählen Sie Werte für Anzahl der öffentlichen Subnetze und Anzahl der privaten Subnetze. Um die IP-Adressbereiche für Ihre Subnetze auszuwählen, erweitern Sie die Option CIDR-Blöcke für Subnetze anpassen.

   > **Note**
   >
   > ROSA erfordert, dass Kunden mindestens ein privates Subnetz pro Availability Zone konfigurieren, das zur Erstellung von Clustern verwendet wird.

10. Um Ressourcen im privaten Subnetz Zugriff auf das öffentliche Internet zu gewähren IPv4, wählen Sie für NAT-Gateways die Anzahl der Gateways aus, AZs in denen NAT-Gateways

erstellt werden sollen. In der Produktion empfehlen wir, in jeder AZ ein NAT-Gateway mit Ressourcen bereitzustellen, die Zugriff auf das öffentliche Internet benötigen.

11. (Optional) Wenn Sie Amazon S3 direkt von Ihrer VPC aus zugreifen müssen, wählen Sie VPC-Endpoints, S3 Gateway.
12. Lassen Sie die Standard-DNS-Optionen ausgewählt. ROSA erfordert Unterstützung für DNS-Hostnamen auf der VPC.
13. Wählen Sie VPC erstellen aus.

AWS CLI

1. Erstellen Sie eine VPC mit dem CIDR-Block `10.0.0.0/16`.

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

Der vorherige Befehl gibt die VPC-ID zurück. Im Folgenden finden Sie eine Beispielausgabe.

```
vpc-1234567890abcdef0
```

2. Speichern Sie die VPC-ID in einer Umgebungsvariablen.

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

3. Erstellen Sie mithilfe der `VPC_ID` Umgebungsvariablen ein `Name` Tag für die VPC.

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

4. Aktivieren Sie die Unterstützung für DNS-Hostnamen auf der VPC.

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

5. Erstellen Sie ein öffentliches und privates Subnetz in der VPC und geben Sie die Availability Zones an, in denen die Ressourcen erstellt werden sollen.

> **Important**
>
> ROSA erfordert, dass Kunden mindestens ein privates Subnetz pro Availability Zone konfigurieren, die zur Erstellung von Clustern verwendet wird. Für Multi-AZ-Bereitstellungen sind drei Availability Zones erforderlich. Wenn diese Anforderungen nicht erfüllt sind, schlägt die Clustererstellung fehl.

> **Note**
>
> Einige ROSA Instanztypen sind nur in ausgewählten Availability Zones verfügbar. Sie können den ROSA `rosa list instance-types` CLI-Befehlsbefehl verwenden, um alle verfügbaren ROSA Instanztypen aufzulisten. Verwenden Sie den AWS CLI Befehl, um zu überprüfen, ob ein Instance-Typ für eine bestimmte Availability Zone verfügbar ist`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. Speichern Sie das öffentliche und private Subnetz IDs in Umgebungsvariablen.

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

7. Erstellen Sie ein Internet-Gateway und eine Routing-Tabelle für ausgehenden Verkehr. Erstellen Sie eine Routentabelle und eine elastische IP-Adresse für privaten Datenverkehr.

```
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. Speichern Sie die Variablen IDs in der Umgebung.

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

9. Verbinden Sie das Internet-Gateway mit der VPC.

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

10. Ordnen Sie die Tabelle für öffentliche Routen dem öffentlichen Subnetz zu und konfigurieren Sie den Datenverkehr so, dass er zum Internet-Gateway weitergeleitet wird.

```
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. Erstellen Sie das NAT-Gateway und ordnen Sie es der elastischen IP-Adresse zu, um den Verkehr zum privaten Subnetz zu ermöglichen.

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

12. Ordnen Sie die private Routing-Tabelle dem privaten Subnetz zu und konfigurieren Sie den Datenverkehr so, dass er zum NAT-Gateway weitergeleitet wird.

```
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. (Optional) Wiederholen Sie bei Multi-AZ-Bereitstellungen die obigen Schritte, um zwei weitere Availability Zones mit öffentlichen und privaten Subnetzen zu konfigurieren.

Erstellen Sie einen klassischen ROSA-Cluster mit der ROSA CLI und AWS PrivateLink

Sie können die ROSA CLI verwenden und AWS PrivateLink eine Cluster mit einer einzigen Availability Zone (Single-AZ) oder mehreren Availability Zones (Multi-AZ) erstellen. In beiden Fällen muss der CIDR-Wert Ihrer Maschine mit dem CIDR-Wert Ihrer VPC übereinstimmen.

Im folgenden Verfahren wird der `rosa create cluster` Befehl verwendet, um einen ROSA-Klassiker zu erstellen. Cluster Um ein Multi-AZ zu erstellen Cluster, geben Sie dies `--multi-az` im Befehl an und wählen Sie dann das private Subnetz aus, IDs das Sie verwenden möchten, wenn Sie dazu aufgefordert werden.

> **Note**
>
> Wenn Sie eine Firewall verwenden, müssen Sie sie so konfigurieren, dass sie auf die Websites zugreifen ROSA kann, die für ihren Betrieb erforderlich sind.

Weitere Informationen finden Sie unter Anforderungen für die Verwendung von AWS PrivateLink Clustern in der Red Hat-Dokumentation.

1. Erstellen Sie die erforderlichen IAM Kontorollen und Richtlinien mit `--mode auto` oder`--mode manual`.

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

   > **Note**
   >
   > Wenn Ihr Offline-Zugriffstoken abgelaufen ist, gibt die ROSA CLI eine Fehlermeldung aus, die besagt, dass Ihr Autorisierungstoken aktualisiert werden muss. Schritte zur Fehlerbehebung finden Sie unterthe section called “Fehlerbehebung bei abgelaufenen Offline-Zugriffstoken für ROSA CLI”.

2. Erstellen Sie eine, Cluster indem Sie einen der folgenden Befehle ausführen.

   - 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**
   >
   > Um einen Cluster zu erstellen, der AWS PrivateLink mit AWS -Security-Token-Service (AWS STS) kurzlebige Anmeldeinformationen verwendet, fügen Sie `--sts --mode auto` oder `--sts --mode manual` an das Ende des `rosa create cluster` Befehls an.

3. Erstellen Sie die Cluster IAM Operatorrollen, indem Sie den interaktiven Anweisungen folgen.

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

4. Erstellen Sie den OpenID Connect (OIDC) -Anbieter, den die Cluster Betreiber zur Authentifizierung verwenden.

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

5. Überprüfen Sie den Status Ihres. Cluster

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

> **Note**
>
> Es kann bis zu 40 Minuten dauern, bis das Cluster `State` Feld den `ready` Status anzeigt. Wenn die Bereitstellung fehlschlägt oder nicht `ready` nach 40 Minuten angezeigt wird, finden Sie weitere Informationen unterFehlerbehebung. Wenn Sie Hilfe benötigen Support oder den Red Hat Support kontaktieren möchten, finden Sie unterthe section called “Supportanfragen”.

6. Verfolgen Sie den Fortschritt der Cluster Erstellung, indem Sie sich die OpenShift Installationsprotokolle ansehen.

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

Konfigurieren Sie die AWS PrivateLink DNS-Weiterleitung

Cluster, die verwenden, AWS PrivateLink erstellen eine öffentliche gehostete Zone und eine private gehostete Zone in Route 53. Datensätze innerhalb der Route 53 privaten Hosting-Zone können nur in der VPC aufgelöst werden, der sie zugewiesen sind.

Für die DNS-01-Validierung von Let's Encrypt ist eine öffentliche Zone erforderlich, damit gültige und öffentlich vertrauenswürdige Zertifikate für die Domain ausgestellt werden können. Die Validierungsdatensätze werden gelöscht, nachdem die Let's Encrypt-Validierung abgeschlossen ist. Die Zone ist weiterhin für die Ausstellung und Erneuerung dieser Zertifikate erforderlich, die in der Regel alle 60 Tage erforderlich sind. Obwohl diese Zonen normalerweise leer erscheinen, spielt eine öffentliche Zone eine entscheidende Rolle im Validierungsprozess.

Weitere Informationen zu AWS privaten gehosteten Zonen finden Sie unter Arbeiten mit privaten Zonen. Weitere Informationen zu öffentlich gehosteten Zonen finden Sie unter Arbeiten mit öffentlich gehosteten Zonen.

Konfigurieren Sie einen Route 53 Resolver eingehenden Endpunkt

1. Um Datensätze wie `api.<cluster_domain>` und deren Auflösung außerhalb der VPC `*.apps.<cluster_domain>` zuzulassen, konfigurieren Sie einen Route 53 Resolver eingehenden Endpunkt.

   > **Note**
   >
   > Wenn Sie einen Eingangsendpunkt konfigurieren, müssen Sie aus Redundanzgründen mindestens zwei IP-Adressen angeben. Wir empfehlen, IP-Adressen in mindestens zwei Availability Zones festzulegen. Wahlweise können Sie zusätzliche IP-Adressen in diesen oder anderen Availability Zones angeben.

2. Wählen Sie bei der Konfiguration des Eingangsendpunkts die VPC und die privaten Subnetze aus, die bei der Erstellung des Clusters verwendet wurden.

Konfigurieren Sie die DNS-Weiterleitung für den Cluster

Nachdem der Route 53 Resolver interne Endpunkt zugeordnet und betriebsbereit ist, konfigurieren Sie die DNS-Weiterleitung, sodass DNS-Anfragen von den dafür vorgesehenen Servern in Ihrem Netzwerk bearbeitet werden können.

1. Konfigurieren Sie Ihr Unternehmensnetzwerk so, dass DNS-Anfragen an die IP-Adressen für die Top-Level-Domain weitergeleitet werden, z. B. `drow-pl-01.htno.p1.openshiftapps.com`
2. Wenn Sie DNS-Abfragen von einer VPC an eine andere VPC weiterleiten, folgen Sie den Anweisungen unter Weiterleitungsregeln verwalten.
3. Wenn Sie Ihren DNS-Server im Remote-Netzwerk konfigurieren, finden Sie in der Dokumentation Ihres jeweiligen DNS-Servers Informationen zur Konfiguration der selektiven DNS-Weiterleitung für die installierte Clusterdomäne.

Konfigurieren Sie einen Identitätsanbieter und gewähren Cluster Sie Zugriff

ROSA beinhaltet einen integrierten OAuth Server. Nachdem Sie Ihren ROSA Cluster erstellt haben, müssen Sie ihn OAuth für die Verwendung eines Identitätsanbieters konfigurieren. Anschließend können Sie Benutzer zu Ihrem konfigurierten Identitätsanbieter hinzufügen, um ihnen Zugriff auf Ihren zu gewähren Cluster. Sie können diesen Benutzern `cluster-admin` oder `dedicated-admin` Berechtigungen nach Bedarf gewähren.

Sie können verschiedene Identitätsanbietertypen für Ihren konfigurieren Cluster. Zu den unterstützten Typen gehören GitHub Enterprise GitHub, Google GitLab, LDAP, OpenID Connect und HTPasswd Identitätsanbieter.

> **Important**
>
> Der HTPasswd Identitätsanbieter ist nur enthalten, um die Erstellung eines einzelnen statischen Administratorbenutzers zu ermöglichen. HTPasswd wird nicht als allgemein verwendbarer Identitätsanbieter für unterstützt. ROSA

Das folgende Verfahren konfiguriert als Beispiel einen GitHub Identitätsanbieter. Anweisungen zur Konfiguration der einzelnen unterstützten Identitätsanbietertypen finden Sie unter Konfiguration von Identitätsanbietern für AWS STS.

1. Navigieren Sie zu github.com und melden Sie sich bei Ihrem GitHub Konto an.
2. Wenn Sie keine GitHub Organisation haben, die Sie für die Bereitstellung von Identitäten verwenden können ROSA Cluster, erstellen Sie eine. Weitere Informationen finden Sie in den Schritten in der GitHub Dokumentation.
3. Konfigurieren Sie im interaktiven Modus der ROSA CLI einen Identitätsanbieter für Ihren Cluster, indem Sie den folgenden Befehl ausführen.

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

4. Folgen Sie den Konfigurationsanweisungen in der Ausgabe, um den Cluster Zugriff auf Mitglieder Ihrer GitHub Organisation zu beschränken.

   ```
   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. Öffnen Sie die URL in der Ausgabe und ersetzen Sie sie durch den Namen Ihrer GitHub Organisation.
6. Wählen Sie auf der GitHub Webseite Anwendung registrieren aus, um eine neue OAuth Anwendung in Ihrer GitHub Organisation zu registrieren.
7. Verwenden Sie die Informationen GitHub OAuth auf der Seite, um die verbleibenden `rosa create idp` interaktiven Eingabeaufforderungen zu füllen, <GITHUB_CLIENT_ID> und <GITHUB_CLIENT_SECRET> ersetzen Sie dabei die Anmeldeinformationen aus Ihrer GitHub OAuth Anwendung.

```
...
? 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**
>
> Es kann etwa zwei Minuten dauern, bis die Identity Provider-Konfiguration aktiv wird. Wenn Sie einen `cluster-admin` Benutzer konfiguriert haben, können Sie den `oc get pods`

`-n openshift-authentication --watch` Befehl ausführen, um zu beobachten, wie die OAuth Pods mit der aktualisierten Konfiguration erneut bereitgestellt werden.

8. Stellen Sie sicher, dass der Identitätsanbieter korrekt konfiguriert wurde.

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

Gewähren Sie dem Benutzer Zugriff auf eine Cluster

Sie können einem Benutzer Zugriff auf Ihre gewähren, Cluster indem Sie ihn dem konfigurierten Identitätsanbieter hinzufügen.

Das folgende Verfahren fügt einen Benutzer zu einer GitHub Organisation hinzu, die für die Identitätsbereitstellung im Cluster konfiguriert ist.

1. Navigieren Sie zu github.com und melden Sie sich bei Ihrem GitHub Konto an.
2. Laden Sie Benutzer ein, die Cluster Zugriff auf Ihre GitHub Organisation benötigen. Weitere Informationen finden Sie in der GitHub Dokumentation unter Benutzer einladen, Ihrer Organisation beizutreten.

Konfigurieren von **`cluster-admin`**-Berechtigungen

1. Erteilen Sie die `cluster-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer- und Clusternamen.

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

2. Stellen Sie sicher, dass der Benutzer als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Konfigurieren von **`dedicated-admin`**-Berechtigungen

1. Erteilen Sie die `dedicated-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer und Cluster Namen.

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

2. Stellen Sie sicher, dass der Benutzer als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Greifen Sie Cluster über die Red Hat Hybrid Cloud Console auf a zu

Nachdem Sie einen Cluster Administratorbenutzer erstellt oder einen Benutzer zu Ihrem konfigurierten Identity Provider hinzugefügt haben, können Sie sich Cluster über die Red Hat Hybrid Cloud Console bei Ihrem anmelden.

1. Rufen Sie die Konsolen-URL für Sie Cluster mit dem folgenden Befehl ab. `<CLUSTER_NAME>`Ersetzen Sie durch den Namen Ihres Cluster.

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

2. Navigieren Sie in der Ausgabe zur Konsolen-URL und melden Sie sich an.
   - Wenn Sie einen `cluster-admin` Benutzer erstellt haben, melden Sie sich mit den angegebenen Anmeldeinformationen an.
   - Wenn Sie einen Identitätsanbieter für Ihren konfiguriert haben Cluster, wählen Sie den Namen des Identitätsanbieters im Dialogfeld Anmelden mit... und füllen Sie alle Autorisierungsanfragen Ihres Anbieters aus.

Stellen Sie eine Anwendung aus dem Entwicklerkatalog bereit

Von der Red Hat Hybrid Cloud Console aus können Sie eine Developer Catalog-Testanwendung bereitstellen und sie mit einer Route verfügbar machen.

1. Navigieren Sie zur Red Hat Hybrid Cloud Console und wählen Sie den Cluster aus, in dem Sie die App bereitstellen möchten.
2. Wählen Sie auf der Seite des Clusters Open Console aus.
3. Wählen Sie in der Administratorperspektive Startseite > Projekte > Projekt erstellen aus.
4. Geben Sie einen Namen für Ihr Projekt ein und fügen Sie optional einen Anzeigenamen und eine Beschreibung hinzu.

5. Wählen Sie Erstellen, um das Projekt zu erstellen.
6. Wechseln Sie zur Entwicklerperspektive und wählen Sie +Hinzufügen. Stellen Sie sicher, dass das ausgewählte Projekt das ist, das gerade erstellt wurde.
7. Wählen Sie im Dialogfeld „Entwicklerkatalog“ die Option Alle Dienste aus.
8. Wählen Sie auf der Seite mit dem Entwicklerkatalog im Menü Sprachen > JavaScriptaus.
9. Wählen Sie Node.js und dann Anwendung erstellen, um die Seite „ Source-to-ImageAnwendung erstellen“ zu öffnen.

> **Note**
>
> Möglicherweise müssen Sie Alle Filter löschen auswählen, um die Option Node.js anzuzeigen.

10. Wählen Sie im Abschnitt Git die Option Try Sample aus.
11. Fügen Sie im Feld Name einen eindeutigen Namen hinzu.
12. Wählen Sie Erstellen aus.

> **Note**
>
> Die Bereitstellung der neuen Anwendung dauert mehrere Minuten.

13. Wenn die Bereitstellung abgeschlossen ist, wählen Sie die Route-URL für die Anwendung aus.

    Im Browser wird eine neue Registerkarte mit einer Meldung geöffnet, die der folgenden ähnelt.

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

14. (Optional) Löschen Sie die Anwendung und bereinigen Sie die Ressourcen.
    a. Wählen Sie in der Administratorperspektive „Startseite“ > „Projekte“.
    b. Öffnen Sie das Aktionsmenü für Ihr Projekt und wählen Sie Projekt löschen.

Widerrufen **`cluster-admin`** Sie die Berechtigungen eines Benutzers

1. Widerrufen Sie die `cluster-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer und Cluster Namen.

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

2. Stellen Sie sicher, dass der Benutzer nicht als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Widerrufen **`dedicated-admin`** Sie die Berechtigungen eines Benutzers

1. Widerrufen Sie die `dedicated-admin` Berechtigungen mit dem folgenden Befehl. Ersetzen Sie `<IDP_USER_NAME>` und `<CLUSTER_NAME>` durch Ihren Benutzer und Cluster Namen.

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

2. Stellen Sie sicher, dass der Benutzer nicht als Mitglied der `dedicated-admins` Gruppe aufgeführt ist.

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

Widerrufen Sie den Benutzerzugriff auf eine Cluster

Sie können einem Identity Provider-Benutzer den Cluster Zugriff entziehen, indem Sie ihn aus dem konfigurierten Identity Provider entfernen.

Sie können verschiedene Arten von Identitätsanbietern für Ihren konfigurieren Cluster. Mit dem folgenden Verfahren wird einem Mitglied einer GitHub Organisation der Cluster Zugriff entzogen.

1. Navigieren Sie zu github.com und melden Sie sich bei Ihrem GitHub Konto an.
2. Entferne den Benutzer aus deiner GitHub Organisation. Weitere Informationen finden Sie in der GitHub Dokumentation unter Ein Mitglied aus Ihrer Organisation entfernen.

Löschen Sie einen Cluster und AWS STS Ressourcen

Sie können die ROSA CLI verwenden, um eine zu löschen Cluster , die AWS -Security-Token-Service (AWS STS) verwendet. Sie können die ROSA CLI auch verwenden, um die IAM Rollen und

den OIDC-Anbieter zu löschen, die von erstellt wurden. ROSA Um die von erstellten IAM Richtlinien zu löschen ROSA, können Sie die IAM Konsole verwenden.

> **Important**
>
> IAM Rollen und Richtlinien, die von erstellt wurden, ROSA können von anderen ROSA Clustern im selben Konto verwendet werden.

1. Löschen Sie die Cluster und sehen Sie sich die Protokolle an. `<CLUSTER_NAME>`Ersetzen Sie durch den Namen oder die ID Ihres Cluster.

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

   > **Important**
   >
   > Sie müssen warten Cluster , bis der vollständig gelöscht ist, bevor Sie die IAM Rollen, Richtlinien und den OIDC-Anbieter entfernen. Die IAM-Rollen des Kontos sind erforderlich, um die vom Installationsprogramm erstellten Ressourcen zu löschen. Die Operator-IAM-Rollen sind erforderlich, um die von den Operatoren erstellten Ressourcen zu bereinigen. OpenShift Die Operatoren verwenden den OIDC-Anbieter zur Authentifizierung.

2. Löschen Sie den OIDC-Anbieter, den die Cluster Operatoren zur Authentifizierung verwenden, indem Sie den folgenden Befehl ausführen.

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

3. Löschen Sie die clusterspezifischen Operatorrollen. IAM

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

4. Löschen Sie die IAM-Rollen des Kontos mithilfe des folgenden Befehls. `<PREFIX>`Ersetzen Sie es durch das Präfix der zu löschenden Konto-IAM-Rollen. Wenn Sie bei der Erstellung der Account-IAM-Rollen ein benutzerdefiniertes Präfix angegeben haben, geben Sie das `ManagedOpenShift` Standardpräfix an.

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

5. Löschen Sie die IAM Richtlinien, die von ROSA erstellt wurden.

a. Melden Sie sich bei der IAM -Konsole an.
b. Wählen Sie im linken Menü unter Zugriffsverwaltung die Option Richtlinien aus.
c. Wählen Sie die Richtlinie aus, die Sie löschen möchten, und wählen Sie Aktionen > Löschen.
d. Geben Sie den Richtliniennamen ein und wählen Sie Löschen aus.
e. Wiederholen Sie diesen Schritt, um alle IAM-Richtlinien für zu löschen. Cluster

Sicherheit in ROSA

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Im Modell der übergreifenden Verantwortlichkeit wird Folgendes mit „Sicherheit der Cloud“ bzw. „Sicherheit in der Cloud“ umschrieben:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für gelten ROSA, finden Sie AWS-Services unter Umfang nach Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS-Service , was Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung anwenden können ROSA. Es zeigt Ihnen, wie Sie die Konfiguration vornehmen ROSA , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere verwenden können AWS-Services , die Ihnen bei der Überwachung und Sicherung Ihrer ROSA Ressourcen helfen.

Inhalt

Datenschutz in ROSA

Die the section called “Verantwortlichkeiten” Dokumentation und das Modell der AWS gemeinsamen Verantwortung definieren den Datenschutz in ROSA. AWS ist verantwortlich für den Schutz der globalen Infrastruktur, die alle betreibt AWS Cloud. Red Hat ist verantwortlich für den Schutz der Cluster-Infrastruktur und der zugrunde liegenden Serviceplattform. Der Kunde ist dafür verantwortlich, die Kontrolle über Inhalte zu behalten, die auf dieser Infrastruktur gehostet werden. Dieser Inhalt umfasst die Sicherheitskonfiguration und die Verwaltungsaufgaben für die AWS-Services , die Sie verwenden. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen über den Datenschutz in Europa finden Sie im Blog-Beitrag AWS Modell der geteilten Verantwortlichkeit und die DSGVO im Blog zur -Sicherheit AWS .

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsdienste wie Amazon Macie, die Sie bei der Erkennung und Sicherung sensibler Daten unterstützen, die in gespeichert sind Amazon S3.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Name keine sensiblen, identifizierenden Informationen wie Kontonummern von Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der ROSA API oder auf andere AWS-Services Weise arbeiten oder diese verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Dienste ROSA oder andere Dienste eingeben, werden möglicherweise zur Aufnahme in Diagnoseprotokolle aufgenommen. Wenn Sie eine URL für einen externen Server

bereitstellen, schließen Sie keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL ein.

Themen

Datenschutz durch Verschlüsselung

Datenschutz bezieht sich auf den Schutz von Daten während der Übertragung (beim Hin- und ROSA Hersenden) und im Ruhezustand (während sie auf Festplatten in AWS Rechenzentren gespeichert werden).

Red Hat OpenShift Service in AWS bietet sicheren Zugriff auf Amazon Elastic Block Store (Amazon EBS) Speichervolumes, die an Amazon EC2 Instanzen für die ROSA Steuerungsebene, die Infrastruktur und die Worker-Knoten angeschlossen sind, sowie auf persistente Kubernetes-Volumes für persistenten Speicher. ROSA verschlüsselt Volumendaten im Ruhezustand und bei der Übertragung und verwendet AWS Key Management Service (AWS KMS), um Ihre verschlüsselten Daten zu schützen. Der Dienst verwendet den Registryspeicher Amazon S3 für Container-Images, der im Ruhezustand standardmäßig verschlüsselt ist.

> **Important**
>
> Weil es ROSA sich um einen verwalteten Service handelt, AWS und Red Hat verwaltet die Infrastruktur, die ROSA verwendet wird. Kunden sollten nicht versuchen, die ROSA verwendeten Amazon EC2 Instances über die AWS Konsole oder CLI manuell herunterzufahren. Diese Aktion kann zum Verlust von Kundendaten führen.

Datenverschlüsselung für Amazon EBS-gestützte Speichervolumes

Red Hat OpenShift Service in AWS verwendet das Kubernetes Persistent Volume (PV) -Framework, um Clusteradministratoren die Bereitstellung eines Clusters mit persistentem Speicher zu ermöglichen. Persistente Volumes sowie die Kontrollebene, die Infrastruktur und die Worker-Knoten werden durch Amazon Elastic Block Store (Amazon EBS) Speichervolumes unterstützt, die an Amazon EC2 Instanzen angehängt sind.

Bei ROSA persistenten Volumes und Nodes, die von unterstützt werden Amazon EBS, finden Verschlüsselungsvorgänge auf den Servern statt, die EC2-Instances hosten. Dadurch wird die

Sicherheit sowohl der ruhenden Daten als auch der Daten bei der Übertragung zwischen einer Instance und dem zugehörigen Speicher gewährleistet. Weitere Informationen finden Sie im Amazon EC2 Benutzerhandbuch unter Amazon EBS Verschlüsselung.

Datenverschlüsselung für den Amazon EBS CSI-Treiber und den Amazon EFS CSI-Treiber

ROSA verwendet standardmäßig den Amazon EBS CSI-Treiber zur Amazon EBS Speicherbereitstellung. Der Amazon EBS CSI-Treiber und der Amazon EBS CSI Driver Operator sind standardmäßig im `openshift-cluster-csi-drivers` Namespace auf dem Cluster installiert. Mit dem Amazon EBS CSI-Treiber und -Operator können Sie persistente Volumes dynamisch bereitstellen und Volume-Snapshots erstellen.

ROSA ist auch in der Lage, persistente Volumes mithilfe des Amazon EFS CSI-Treibers und des Amazon EFS CSI-Treiberoperators bereitzustellen. Der Amazon EFS Treiber und der Operator ermöglichen es Ihnen auch, Dateisystemdaten zwischen Pods oder mit anderen Anwendungen innerhalb oder außerhalb von Kubernetes gemeinsam zu nutzen.

Volumendaten werden während der Übertragung sowohl für den CSI-Treiber als auch für Amazon EBS den CSI-Treiber gesichert Amazon EFS . Weitere Informationen finden Sie unter Using Container Storage Interface (CSI) in der Red Hat-Dokumentation.

> **Important**
>
> Bei der dynamischen Bereitstellung ROSA persistenter Volumes mithilfe des Amazon EFS CSI-Treibers sollten bei der Bewertung der Dateisystemberechtigungen die Benutzer-ID, Gruppen-ID (GID) und die sekundäre Gruppe IDs des Access Points Amazon EFS berücksichtigt werden. Amazon EFS ersetzt den Benutzer und die Gruppe IDs in Dateien durch den Benutzer und die Gruppe IDs auf dem Access Point und ignoriert den NFS-Client. IDs Dies hat zur Folge, dass Einstellungen im Amazon EFS Hintergrund ignoriert werden. `fsGroup` ROSA ist nicht in der Lage, die Dateien mithilfe GIDs von zu ersetzen. `fsGroup` Jeder Pod, der auf einen bereitgestellten Amazon EFS Access Point zugreifen kann, kann auf jede Datei auf dem Volume zugreifen. Weitere Informationen finden Sie im Amazon EFS Benutzerhandbuch unter Arbeiten mit Amazon EFS Access Points.

etcd-Verschlüsselung

ROSA bietet die Option, die Verschlüsselung von `etcd` Schlüsselwerten innerhalb des `etcd` Volumes während der Clustererstellung zu aktivieren, wodurch eine zusätzliche

Verschlüsselungsebene hinzugefügt wird. Sobald die Verschlüsselung abgeschlossen `etcd` ist, entsteht ein zusätzlicher Leistungsaufwand von ca. 20%. Wir empfehlen, die `etcd` Verschlüsselung nur zu aktivieren, wenn Sie sie speziell für Ihren Anwendungsfall benötigen. Weitere Informationen finden Sie unter etcd-Verschlüsselung in der ROSA Dienstdefinition.

Schlüsselverwaltung

ROSA dient KMS keys zur sicheren Verwaltung von Datenmengen auf Steuerungsebene, Infrastruktur und Mitarbeitern sowie persistente Volumes für Kundenanwendungen. Bei der Clustererstellung haben Sie die Wahl, den standardmäßigen AWS verwalteten Schlüssel zu verwenden, der von KMS key bereitgestellt wird Amazon EBS, oder Sie können Ihren eigenen, vom Kunden verwalteten Schlüssel angeben. Weitere Informationen finden Sie unter the section called “Schlüsselverwaltung”.

Datenverschlüsselung für die integrierte Image-Registry

ROSA bietet eine integrierte Container-Image-Registrierung zum Speichern, Abrufen und Teilen von Container-Images über den Amazon S3 Bucket-Speicher. Die Registrierung wird vom OpenShift Image Registry Operator konfiguriert und verwaltet. Es bietet Benutzern eine out-of-the-box Lösung zur Verwaltung der Images, auf denen ihre Workloads ausgeführt werden, und wird auf der vorhandenen Cluster-Infrastruktur ausgeführt. Weitere Informationen finden Sie unter Registry in der Red Hat-Dokumentation.

ROSA bietet öffentliche und private Image-Registries. Für Unternehmensanwendungen empfehlen wir die Verwendung einer privaten Registrierung, um Ihre Bilder vor der Verwendung durch unbefugte Benutzer zu schützen. ROSA Verwendet standardmäßig serverseitige Verschlüsselung mit Amazon S3 verwalteten Schlüsseln (SSE-S3), um die Daten Ihrer Registrierung im Ruhezustand zu schützen. Dies erfordert kein Eingreifen Ihrerseits und wird ohne zusätzliche Kosten angeboten. Weitere Informationen finden Sie im Benutzerhandbuch unter Schützen von Daten mithilfe serverseitiger Verschlüsselung mit Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3). Amazon S3

ROSA verwendet das Transport Layer Security (TLS) -Protokoll, um Daten bei der Übertragung zur und von der Image-Registry zu sichern. Weitere Informationen finden Sie unter Registry in der Red Hat-Dokumentation.

Richtlinie für den Datenverkehr zwischen Netzwerken

Red Hat OpenShift Service in AWS verwendet Amazon Virtual Private Cloud (Amazon VPC), um Grenzen zwischen Ressourcen in Ihrem ROSA Cluster zu erstellen und den Verkehr zwischen ihnen,

Ihrem lokalen Netzwerk und dem Internet zu kontrollieren. Weitere Informationen zur Amazon VPC Sicherheit finden Sie unter Datenschutz im Netzwerkdatenverkehr Amazon VPC im Amazon VPC Benutzerhandbuch.

Innerhalb der VPC können Sie Ihre ROSA Cluster so konfigurieren, dass sie einen HTTP- oder HTTPS-Proxyserver verwenden, um den direkten Internetzugang zu verweigern. Wenn Sie ein Clusteradministrator sind, können Sie auch Netzwerkrichtlinien auf Pod-Ebene definieren, die den Netzwerkverkehr auf Pods in Ihrem ROSA Cluster beschränken. Weitere Informationen finden Sie unter the section called “Sicherheit der Infrastruktur”.

Datenverschlüsselung mit KMS

ROSA verwendet AWS KMS , um Schlüssel für verschlüsselte Daten sicher zu verwalten. Die Volumes der Steuerungsebene, der Infrastruktur und der Worker-Knoten werden standardmäßig mit den von AWS verwalteten KMS key Datenträgern verschlüsselt Amazon EBS. Das KMS key hat den Alias`aws/ebs`. Persistente Volumes, die die Standard-GP3-Speicherklasse verwenden, werden damit KMS key standardmäßig ebenfalls verschlüsselt.

Neu erstellte ROSA Cluster sind so konfiguriert, dass sie die Standard-GP3-Speicherklasse verwenden, um persistente Volumes zu verschlüsseln. Persistente Volumes, die mit einer anderen Speicherklasse erstellt wurden, werden nur verschlüsselt, wenn die Speicherklasse für die Verschlüsselung konfiguriert ist. Weitere Informationen zu ROSA vorgefertigten Speicherklassen finden Sie unter Konfiguration von persistentem Speicher in der Red Hat-Dokumentation.

Während der Clustererstellung können Sie wählen, ob Sie die persistenten Volumes in Ihrem Cluster mit dem standardmäßig Amazon EBS bereitgestellten Schlüssel verschlüsseln oder Ihren eigenen, vom Kunden verwalteten symmetrischen Schlüssel angeben möchten. KMS keyWeitere Informationen zum Erstellen von Schlüsseln finden Sie unter KMS-Schlüssel für symmetrische Verschlüsselung erstellen im Entwicklerhandbuch. AWS KMS

Sie können persistente Volumes auch für einzelne Container innerhalb eines Clusters verschlüsseln, indem Sie eine definieren. KMS key Dies ist nützlich, wenn Sie bei der Bereitstellung auf explizite Compliance- und Sicherheitsrichtlinien festgelegt haben. AWS Weitere Informationen finden Sie unter Encrypting container persistent volumes on AWS with a KMS key in der Red Hat-Dokumentation.

Die folgenden Punkte sollten beachtet werden, wenn Sie persistente Volumes mit Ihren eigenen verschlüsseln: KMS keys

- Wenn Sie die KMS-Verschlüsselung mit Ihrer eigenen Verschlüsselung verwenden KMS key, muss sich der Schlüssel in demselben AWS-Region Cluster befinden.

- Die Erstellung und Verwendung Ihres eigenen Systems ist mit Kosten verbunden KMS keys. Weitere Informationen finden Sie unter AWS Key Management Service Preise.

Identitäts- und Zugriffsmanagement für ROSA

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um ROSA Ressourcen zu verwenden. IAM ist eine AWS-Service , die Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie arbeiten ROSA.

Dienstbenutzer — Wenn Sie den ROSA Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr ROSA Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie in nicht auf eine Funktion zugreifen können ROSA, finden Sie weitere Informationen unterthe section called “Fehlerbehebung”.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für ROSA Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf ROSA. Es ist Ihre Aufgabe, zu bestimmen, auf welche ROSA Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer

zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehen IAM.

IAM Administrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr über die Richtlinien erfahren, die zur Verwaltung des Zugriffs auf verwendet werden ROSA. Beispiele für ROSA identitätsbasierte Richtlinien, die Sie in verwenden können IAM, finden Sie unter. the section called “ ROSA Beispiele für identitätsbasierte politische Maßnahmen”

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als AWS-Konto Root-Benutzer authentifiziert (angemeldet AWS) sein IAM-Benutzer, oder indem Sie eine IAM Rolle übernehmen.

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS-Managementkonsole oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie unter So melden Sie sich bei Ihrem an AWS-Konto im AWS Anmelde-Benutzerhandbuch. AWS

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mit Ihren Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise auch zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Factor Authentication im AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) User Guide und Using Multi-Factor Authentication (MFA) AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer einzigen Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für alltägliche Aufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im Benutzerhandbuch für AWS IAM Identity Center (Nachfolger von AWS Single Sign-On).

IAM-Benutzer und Gruppen

Eine IAM-Benutzerist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Zugangsdaten zu verlassen IAM-Benutzer , anstatt solche mit langfristigen Zugangsdaten wie Passwörtern und Zugangsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen erforderlich sind, empfehlen wir IAM-Benutzer, dass Sie die Zugriffsschlüssel rotieren. Weitere Informationen finden Sie

unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM Gruppe ist eine Identität, die eine Sammlung von angibt IAM-Benutzer. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen erleichtern die Verwaltung von Berechtigungen für große Benutzergruppen. Sie könnten beispielsweise einer Gruppe einen Namen geben IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer sind nicht dasselbe wie Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Wann sollte eine Rolle IAM-Benutzer (statt einer Rolle) erstellt werden?

IAM Rollen

Eine IAM Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einer IAM-Benutzer, ist aber keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS-Managementkonsole indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter IAM Rollen verwenden im IAM-Benutzerhandbuch.

IAM Rollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Föderierter Benutzerzugriff — Um einer föderierten Identität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu steuern, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch (Nachfolger von AWS Single Sign-On).
- Temporäre IAM-Benutzer Berechtigungen — Ein Benutzer IAM-Benutzer kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.

- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um jemandem (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Unterschiede zwischen IAM Rollen und ressourcenbasierten Richtlinien.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise in einem Dienst einen Anruf tätigen, ist es üblich, dass dieser Dienst Anwendungen ausführt Amazon EC2 oder Objekte darin Amazon S3 speichert. Ein Service kann dies mithilfe der Berechtigungen des aufrufenden Prinzipals, einer Servicerolle oder einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie eine IAM-Benutzer OR-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle — Eine Servicerolle ist eine IAM Rolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschen IAM. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen werden in Ihrem IAM Konto angezeigt und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen einsehen, aber nicht bearbeiten.
- Anwendungen, die auf einer Instanz ausgeführt werden Amazon EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer Amazon EC2 Instanz ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der Amazon EC2 Instanz vorzuziehen. Um einer Amazon EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen

zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der Amazon EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2 Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im IAM-Benutzerhandbuch unter Wann eine IAM Rolle (anstelle eines Benutzers) erstellt werden sollte.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAM Richtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS-Managementkonsole AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität, z. B. eine Rolle oder Gruppe IAM-Benutzer, anhängen können. Diese Richtlinien steuern,

welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter Erstellen von IAM Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Eingebundene Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM -Rollen-Vertrauensrichtlinien und Amazon S3 -Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 AWS WAF, und Amazon VPC sind Beispiele für Dienste, die Unterstützung bieten. ACLs Weitere Informationen finden Sie in der Übersicht über ACLs die Access Control List (ACL) im Amazon Simple Storage Service-Benutzerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Mit diesen Richtlinientypen können Sie die maximalen Berechtigungen festlegen, die Ihnen durch die gängigeren Richtlinientypen gewährt werden.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAM-Benutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die resultierenden Berechtigungen sind die Schnittmenge der identitätsbasierten Richtlinien der Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in AWS Organizations festlegen. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich jedes AWS-Konto Root-Benutzers. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung (SCPs) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind die Schnittmenge der identitätsbasierten Richtlinien des Benutzers oder der Rolle und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine

Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

ROSA Beispiele für identitätsbasierte Richtlinien

Standardmäßig sind Rollen nicht berechtigt, IAM-Benutzer Ressourcen zu erstellen oder zu ändern AWS . Sie können auch keine Aufgaben mit der AWS-Managementkonsole AWS CLI, oder AWS API ausführen. Ein IAM Administrator muss IAM Richtlinien erstellen, die Benutzern und Rollen die Erlaubnis gewähren, bestimmte API-Operationen mit den angegebenen Ressourcen auszuführen, die sie benötigen. Der Administrator muss diese Richtlinien dann den Gruppen IAM-Benutzer oder Gruppen zuordnen, für die diese Berechtigungen erforderlich sind.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie mithilfe dieser Beispieldokumente zu JSON-Richtlinien finden Sie im IAM-Benutzerhandbuch unter Erstellen von Richtlinien auf der Registerkarte JSON.

Verwenden der Konsole ROSA

Um ROSA von der Konsole aus abonnieren zu können, muss Ihr IAM-Principal über die erforderlichen AWS Marketplace Berechtigungen verfügen. Die Berechtigungen ermöglichen es dem Prinzipal, das ROSA Produktangebot in Abonnements zu abonnieren und abzubestellen AWS Marketplace und AWS Marketplace Abonnements anzusehen. Um die erforderlichen Berechtigungen hinzuzufügen, rufen Sie die ROSA Konsole auf und hängen Sie die AWS verwaltete Richtlinie `ROSAManageSubscription` an Ihren IAM-Prinzipal an. Mehr über `ROSAManageSubscription` erfahren Sie unter the section called “AWS verwaltete Richtlinie: ROSAManage Abonnement”.

Autorisieren von ROSA mit HCP zur Verwaltung von Ressourcen AWS

ROSA mit Hosted Control Planes (HCP) verwendet AWS verwaltete Richtlinien mit Berechtigungen, die für den Betrieb und Support der Dienste erforderlich sind. Sie verwenden die ROSA CLI oder IAM Konsole, um diese Richtlinien an Servicerollen in Ihrem anzuhängen AWS-Konto.

Weitere Informationen finden Sie unter the section called “ AWS verwaltete Richtlinien”.

Autorisierung von ROSA classic zur Verwaltung von Ressourcen AWS

ROSA classic verwendet vom Kunden verwaltete IAM-Richtlinien mit vom Service vordefinierten Berechtigungen. Sie verwenden die ROSA CLI, um diese Richtlinien zu erstellen und sie an Servicerollen in Ihrem anzuhängen AWS-Konto. ROSA erfordert, dass diese Richtlinien so

konfiguriert sind, wie sie vom Service definiert wurden, um einen kontinuierlichen Betrieb und Servicesupport zu gewährleisten.

> **Note**
>
> Sie sollten die Richtlinien von ROSA Classic nicht ändern, ohne vorher Red Hat konsultiert zu haben. Andernfalls kann das Service-Level-Agreement von Red Hat für eine Verfügbarkeit von 99,95% für Cluster unwirksam werden. ROSA mit gehosteten Kontrollebenen verwendet AWS verwaltete Richtlinien mit eingeschränkteren Berechtigungen. Weitere Informationen finden Sie unter the section called “ AWS verwaltete Richtlinien”.

Es gibt zwei Arten von vom Kunden verwalteten Richtlinien für ROSA: Kontorichtlinien und Betreiberrichtlinien. Kontorichtlinien sind IAM Rollen zugeordnet, die der Service verwendet, um eine Vertrauensbeziehung mit Red Hat für den Support durch Site Reliability Engineer (SRE), die Clustererstellung und Rechenfunktionen aufzubauen. Operator-Richtlinien sind IAM Rollen zugeordnet, die OpenShift Operatoren für Cluster-Operationen in den Bereichen Ingress, Speicherung, Image-Registry und Node-Management verwenden. Kontorichtlinien werden einmal pro Cluster erstellt AWS-Konto, wohingegen Betreiberrichtlinien einmal pro Cluster erstellt werden.

Weitere Informationen erhalten Sie unter the section called “Klassische Kontorichtlinien von ROSA” und the section called “Richtlinien für klassische ROSA-Betreiber”.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es ermöglicht, IAM-Benutzer die internen und verwalteten Richtlinien anzuzeigen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von. 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": "*"
        }
    ]
}
```

Klassische Kontorichtlinien von ROSA

Dieser Abschnitt enthält Einzelheiten zu den Kontorichtlinien, die für ROSA classic erforderlich sind. Diese Berechtigungen sind für ROSA classic erforderlich, um die AWS Ressourcen zu verwalten, auf denen Cluster ausgeführt werden, und um den Red Hat Site Reliability Engineer Support für Cluster zu aktivieren. Sie können den Richtliniennamen ein benutzerdefiniertes Präfix zuweisen, aber diese Richtlinien sollten ansonsten wie auf dieser Seite definiert benannt werden (z. B.`ManagedOpenShift-Installer-Role-Policy`).

Die Kontorichtlinien gelten nur für eine OpenShift Nebenversion und sind abwärtskompatibel. Bevor Sie einen Cluster erstellen oder aktualisieren, sollten Sie überprüfen, ob die Richtlinienversion und die Clusterversion identisch sind, indem Sie Folgendes ausführen`rosa list account-roles`. Wenn die Richtlinienversion niedriger als die Clusterversion ist, führen Sie die Ausführung aus, `rosa upgrade account-roles` um die Rollen und die angehängten Richtlinien zu aktualisieren. Sie können dieselben Kontorichtlinien und Rollen für mehrere Cluster derselben Nebenversion verwenden.

[Präfix] -Installer-Role-Policy

Sie können `[Prefix]-Installer-Role-Policy` an Ihre IAM-Entitäten anhängen. Bevor Sie einen klassischen ROSA-Cluster erstellen können, müssen Sie diese Richtlinie zunächst einer IAM-Rolle mit dem Namen zuordnen. `[Prefix]-Installer-Role` Diese Richtlinie gewährt die erforderlichen Berechtigungen, mit denen das ROSA Installationsprogramm die AWS Ressourcen verwalten kann, die für die Clustererstellung benötigt werden.

Berechtigungsrichtlinie

Die in diesem Richtliniendokument definierten Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

```
{
    "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"
                }
```

```
            }
        }
    ]
}
```

[Präfix] — ControlPlane -Role-Policy

Sie können `[Prefix]-ControlPlane-Role-Policy` an Ihre IAM-Entitäten anhängen. Bevor Sie einen klassischen ROSA-Cluster erstellen können, müssen Sie diese Richtlinie zunächst einer IAM-Rolle mit dem Namen zuordnen. `[Prefix]-ControlPlane-Role` Diese Richtlinie gewährt ROSA classic die erforderlichen Berechtigungen zur Verwaltung Amazon EC2 und zum Hosten der ROSA Steuerungsebene sowie zum Lesen KMS keys von Elastic Load Balancing Ressourcen.

Berechtigungsrichtlinie

Die in diesem Richtliniendokument definierten Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

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

[Präfix] -Worker-Role-Policy

Sie können `[Prefix]-Worker-Role-Policy` an Ihre IAM-Entitäten anhängen. Bevor Sie einen klassischen ROSA-Cluster erstellen können, müssen Sie diese Richtlinie zunächst einer IAM-Rolle mit dem Namen zuordnen. `[Prefix]-Worker-Role` Diese Richtlinie gewährt ROSA classic die erforderlichen Berechtigungen, um die EC2-Instances zu beschreiben, die als Worker-Knoten ausgeführt werden.

Berechtigungsrichtlinie

Die in diesem Richtliniendokument definierten Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

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

```
                "ec2:DescribeInstances",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Präfix] -Support-Role-Policy

Sie können `[Prefix]-Support-Role-Policy` an Ihre IAM-Entitäten anhängen. Bevor Sie einen klassischen ROSA-Cluster erstellen können, müssen Sie diese Richtlinie zunächst einer IAM-Rolle mit dem Namen zuordnen. `[Prefix]-Support-Role` Diese Richtlinie gewährt Red Hat Site Reliability Engineering die erforderlichen Berechtigungen zur Beobachtung, Diagnose und Unterstützung der AWS Ressourcen, die von den klassischen ROSA-Clustern verwendet werden, einschließlich der Möglichkeit, den Status von Clusterknoten zu ändern.

Berechtigungsrichtlinie

Die in diesem Richtliniendokument definierten Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

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

Die klassischen ROSA-Betreiberrichtlinien

Dieser Abschnitt enthält Einzelheiten zu den Betreiberrichtlinien, die für ROSA classic erforderlich sind. Bevor Sie einen ROSA Classic-Cluster erstellen können, müssen Sie diese Richtlinien zunächst den entsprechenden Operatorrollen zuordnen. Für jeden Cluster ist ein eigener Satz von Operatorrollen erforderlich.

Diese Berechtigungen werden benötigt, damit die OpenShift Betreiber die klassischen ROSA-Clusterknoten verwalten können. Sie können den Richtliniennamen ein benutzerdefiniertes Präfix zuweisen, um die Richtlinienverwaltung zu vereinfachen (z. B.`ManagedOpenShift-openshift-ingress-operator-cloud-credentials`).

[Präfix] openshift-ingress-operator-cloud — Anmeldeinformationen

Sie können `[Prefix]-openshift-ingress-operator-cloud-credentials` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt dem Ingress-Operator die erforderlichen Berechtigungen zur Bereitstellung und Verwaltung von Load Balancers und DNS-Konfigurationen für den externen Clusterzugriff. Die Richtlinie ermöglicht es dem Ingress-Operator auch, Route 53 Ressourcen-Tag-Werte zu lesen und zu filtern, um gehostete Zonen zu ermitteln. Weitere Informationen zum Operator finden Sie in der Dokumentation unter OpenShift Ingress-Operator. OpenShift GitHub

Berechtigungsrichtlinie

In diesem Richtliniendokument definierte Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

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

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

Sie können `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt dem Amazon EBS CSI-Treiberoperator die erforderlichen Berechtigungen zur Installation und Wartung des Amazon EBS CSI-Treibers auf einem ROSA Classic-Cluster. Weitere Informationen zum Operator finden Sie in der OpenShift GitHub Dokumentation unter aws-ebs-csi-driver-operator.

Berechtigungsrichtlinie

In diesem Richtliniendokument definierte Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

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

[Präfix] — openshift-machine-api-aws -cloud-credentials

Sie können `[Prefix]-openshift-machine-api-aws-cloud-credentials` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt dem Machine Config Operator die erforderlichen Berechtigungen, um Amazon EC2 Instanzen zu beschreiben, auszuführen und zu beenden, die als Worker-Knoten verwaltet werden. Diese Richtlinie gewährt auch Berechtigungen für die Festplattenverschlüsselung des Root-Volumes des Worker-Knotens mithilfe von AWS KMS keys. Weitere Informationen zum Operator finden Sie machine-config-operatorin der OpenShift GitHub Dokumentation.

Berechtigungsrichtlinie

In diesem Richtliniendokument definierte Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

```
{
    "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
```

```
                }
            }
        }
    ]
}
```

[Präfix] — openshift-cloud-credential-operator -cloud-credentials

Sie können `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt dem Cloud Credential Operator die erforderlichen Berechtigungen zum Abrufen von IAM-Benutzer Details, einschließlich des Zugriffsschlüssels IDs, angehängter Inline-Richtliniendokumente, des Erstellungsdatums, des Pfads, der Benutzer-ID und des Amazon-Ressourcennamens (ARN). Weitere Informationen zum Betreiber finden Sie cloud-credential-operatorin der OpenShift GitHub Dokumentation.

Berechtigungsrichtlinie

In diesem Richtliniendokument definierte Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

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

[Präfix] — openshift-image-registry-installer -cloud-credentials

Sie können `[Prefix]-openshift-image-registry-installer-cloud-credentials` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt dem Image Registry Operator die erforderlichen Berechtigungen zur Bereitstellung und Verwaltung von Ressourcen für die Cluster-interne Image-Registry und die abhängigen Dienste von ROSA classic, darunter. Amazon S3 Dies ist

erforderlich, damit der Betreiber die interne Registrierung eines ROSA Classic-Clusters installieren und verwalten kann. Weitere Informationen zum Operator finden Sie in der OpenShift GitHub Dokumentation unter Image Registry Operator.

Berechtigungsrichtlinie

In diesem Richtliniendokument definierte Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

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

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

Sie können `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt dem Cloud Network Config Controller Operator

die erforderlichen Berechtigungen zur Bereitstellung und Verwaltung von Netzwerkressourcen für die Verwendung durch das ROSA Classic Cluster Networking Overlay. Der Betreiber verwendet diese Berechtigungen, um private IP-Adressen für Amazon EC2 Instanzen als Teil des ROSA Classic-Clusters zu verwalten. Weitere Informationen zum Operator finden Sie loud-network-config-controller in der OpenShift GitHub Dokumentation unter C.

Berechtigungsrichtlinie

In diesem Richtliniendokument definierte Berechtigungen geben an, welche Aktionen zulässig oder verweigert werden.

```
{
    "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 verwaltete Richtlinien für ROSA

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur

Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden. Weitere Informationen finden Sie im IAM Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAManage Abonnement

Sie können die `ROSAManageSubscription` Richtlinie an Ihre IAM Entitäten anhängen. Bevor Sie sie ROSA in der AWS ROSA Konsole aktivieren, müssen Sie diese Richtlinie zunächst einer IAM-Rolle zuordnen.

Diese Richtlinie gewährt Ihnen die AWS Marketplace Berechtigungen, die Sie zur Verwaltung des ROSA Abonnements benötigen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `aws-marketplace:Subscribe`- Erteilt die Erlaubnis, das AWS Marketplace Produkt zu abonnieren für ROSA.
- `aws-marketplace:Unsubscribe`- Ermöglicht Prinzipalen, Abonnements für AWS Marketplace Produkte zu entfernen.
- `aws-marketplace:ViewSubscriptions`- Ermöglicht Prinzipalen das Anzeigen von Abonnements von. AWS Marketplace Dies ist erforderlich, damit der IAM Principal die verfügbaren AWS Marketplace Abonnements einsehen kann.

Das vollständige JSON-Richtliniendokument finden Sie unter ROSAManageAbonnement im Referenzhandbuch für AWS verwaltete Richtlinien.

ROSA mit HCP-Kontorichtlinien

Dieser Abschnitt enthält Einzelheiten zu den Kontorichtlinien, die für ROSA mit Hosted Control Planes (HCP) erforderlich sind. Diese AWS verwalteten Richtlinien fügen Berechtigungen hinzu, die von ROSA mit HCP-IAM-Rollen verwendet werden. Die Berechtigungen sind für den technischen Support

von Red Hat Site Reliability Engineering (SRE), die Cluster-Installation sowie die Funktionen der Steuerungsebene und der Rechenleistung erforderlich.

> **Note**
>
> AWS verwaltete Richtlinien sind für die Verwendung durch ROSA mit Hosted Control Planes (HCP) vorgesehen. Die klassischen ROSA-Cluster verwenden vom Kunden verwaltete IAM-Richtlinien. Weitere Informationen zu den klassischen ROSA-Richtlinien finden Sie unter the section called “Klassische Kontorichtlinien von ROSA” undthe section called “Richtlinien für klassische ROSA-Betreiber”.

AWS verwaltete Richtlinie: ROSAWorker InstancePolicy

Sie können sie `ROSAWorkerInstancePolicy` an Ihre IAM Entitäten anhängen. Bevor Sie einen Cluster erstellen, müssen Sie über eine IAM-Rolle verfügen, der diese Richtlinie zugewiesen ist. Ein ROSA-Dienst ruft in Ihrem Namen andere AWS-Services an. Sie tun dies, um die Ressourcen zu verwalten, die Sie mit den einzelnen Clustern verwenden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen die ROSA-Worker-Knoten die folgenden Aufgaben ausführen können:

- `ec2`— Evaluierung AWS-Region und Amazon EC2 Instanzierung von Details im Rahmen des Lebenszyklusmanagements für ROSA-Cluster Worker Nodes.
- `ecr`- Evaluieren und Abrufen von Images aus ROSA-verwalteten ECR-Repositorys, die für die Cluster-Installation und das Worker-Node-Lebenszyklusmanagement erforderlich sind.

Das vollständige JSON-Richtliniendokument finden Sie ROSAWorkerInstancePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSASRESupport Richtlinie

Sie können `ROSASRESupportPolicy` an Ihre IAM-Entitäten anhängen.

Bevor Sie eine ROSA mit einem Cluster für gehostete Steuerungsebenen erstellen, müssen Sie diese Richtlinie zunächst einer IAM-Rolle zuordnen. Diese Richtlinie gewährt Red Hat Site Reliability Engineers (SREs) die erforderlichen Berechtigungen, um AWS Ressourcen im Zusammenhang mit

ROSA Clustern direkt zu beobachten, zu diagnostizieren und zu unterstützen, einschließlich der Möglichkeit, den Status von ROSA Clusterknoten zu ändern.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, die es Red Hat SREs ermöglichen, die folgenden Aufgaben auszuführen:

- `cloudtrail`— Lesen Sie AWS CloudTrail Ereignisse und Trails, die für den Cluster relevant sind.
- `cloudwatch`— Lesen Sie die für den Cluster relevanten Amazon CloudWatch Metriken.
- `ec2`— Lesen, beschreiben und überprüfen Sie Amazon EC2 Komponenten, die sich auf den Zustand des Clusters beziehen, wie Sicherheitsgruppen, VPC-Endpunktverbindungen und Volume-Status. Amazon EC2 Instances starten, stoppen, neu starten und beenden.
- `elasticloadbalancing`— Lesen, beschreiben und überprüfen Sie Elastic Load Balancing Parameter, die sich auf den Zustand des Clusters beziehen.
- `iam`— Evaluieren Sie IAM Rollen, die sich auf den Zustand des Clusters beziehen.
- `route53`— Überprüfen Sie die DNS-Einstellungen, die sich auf den Zustand des Clusters beziehen.
- `sts`— `DecodeAuthorizationMessage` — Lesen Sie IAM Nachrichten zu Debugging-Zwecken.

Das vollständige JSON-Richtliniendokument finden Sie unter ROSASRESupportRichtlinie im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAInstaller Richtlinie

Sie können sie `ROSAInstallerPolicy` an Ihre IAM Entitäten anhängen.

Bevor Sie eine ROSA mit einem Cluster für gehostete Steuerungsebenen erstellen, müssen Sie diese Richtlinie zunächst einer IAM-Rolle mit dem Namen `[Prefix]-ROSA-Worker-Role` zuordnen. Diese Richtlinie ermöglicht es Entitäten, einem Instanzprofil jede Rolle hinzuzufügen, die dem `[Prefix]-ROSA-Worker-Role` Muster folgt. Diese Richtlinie gewährt dem Installationsprogramm die erforderlichen Berechtigungen zur Verwaltung von AWS Ressourcen, die die ROSA Clusterinstallation unterstützen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen das Installationsprogramm die folgenden Aufgaben ausführen kann:

- `ec2`— Führen Sie Amazon EC2 Instances mithilfe von AMIs Hosted in aus, das AWS-Konten Eigentum von Red Hat ist und von Red Hat verwaltet wird. Beschreiben Sie Amazon EC2 Instanzen, Volumes und Netzwerkressourcen, die mit Amazon EC2 Knoten verknüpft sind. Diese Berechtigung ist erforderlich, damit die Kubernetes-Steuerebene Instanzen zu einem Cluster zusammenfügen kann und der Cluster ihre Präsenz innerhalb eines Clusters auswerten kann. Amazon VPC Sehen Sie sich Amazon EC2 Capacity Reservations an, um die neue Funktion für Kapazitätsreservierungen in ROSA zu unterstützen. Kennzeichnen und löschen Sie Tags in Subnetzen mithilfe von passenden Tag-Schlüsseln. `"kubernetes.io/cluster/*"` Dies ist erforderlich, um sicherzustellen, dass der für den Clustereingang verwendete Load Balancer nur in den entsprechenden Subnetzen erstellt wird, und um Kubernetes-Cluster-Identifikations-Tags zu verwalten.
- `elasticloadbalancing`— Fügen Sie Load Balancer zu Zielknoten in einem Cluster hinzu. Entfernen Sie Load Balancer von den Zielknoten auf einem Cluster. Diese Berechtigung ist erforderlich, damit die Kubernetes-Steuerebene Load Balancer dynamisch bereitstellen kann, die von Kubernetes-Diensten und Anwendungsdiensten angefordert werden. OpenShift
- `kms`— Lesen Sie einen AWS KMS Schlüssel, erstellen und verwalten Sie Zuschüsse für und geben Sie Amazon EC2 einen eindeutigen symmetrischen Datenschlüssel zur Verwendung außerhalb von zurück. AWS KMS Dies ist für die Verwendung verschlüsselter `etcd` Daten erforderlich, wenn die `etcd` Verschlüsselung bei der Clustererstellung aktiviert ist.
- `iam`— Überprüfen Sie die IAM-Rollen und -Richtlinien. Dynamische Bereitstellung und Verwaltung von Amazon EC2 Instanzprofilen, die für den Cluster relevant sind. Fügen Sie mithilfe der `iam:TagInstanceProfile` Berechtigung Tags zu einem IAM-Instanzprofil hinzu. Stellen Sie Fehlermeldungen für das Installationsprogramm bereit, wenn die Clusterinstallation aufgrund eines fehlenden kundenspezifischen Cluster-OIDC-Anbieters fehlschlägt.
- `route53`— Verwaltet die Route 53 Ressourcen, die zum Erstellen von Clustern benötigt werden.
- `servicequotas`— Evaluieren Sie die für die Erstellung eines Clusters erforderlichen Dienstkontingente.
- `sts`— Erstellen Sie temporäre AWS STS Anmeldeinformationen für ROSA Komponenten. Gehen Sie von den Anmeldeinformationen für die Clustererstellung aus.
- `secretsmanager`— Lesen Sie einen geheimen Wert, um die vom Kunden verwaltete OIDC-Konfiguration im Rahmen der Cluster-Bereitstellung sicher zu ermöglichen.

Das vollständige JSON-Richtliniendokument finden Sie unter ROSAInstallerRichtlinie im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAShared VPCRoute53 Richtlinie

Sie können sie `ROSASharedVPCRoute53Policy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie einer IAM-Rolle zuordnen, damit ein ROSA-Cluster Aufrufe an andere AWS-Services in gemeinsam genutzten VPC-Umgebungen tätigen kann.

Diese Richtlinie ermöglicht es dem ROSA-Installationsprogramm, Route 53 53-Datensätze zu konfigurieren. Diese Richtlinie ist für die Verwendung in einer gemeinsam genutzten VPC vorgesehen und bietet eine Teilmenge von Route 53 53-Berechtigungen, die auf gemeinsam genutzte VPC-Anwendungsfälle zugeschnitten sind.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen das ROSA-Installationsprogramm die folgenden Aufgaben ausführen kann:

- `route53`— Lesen Sie die DNS-Zoneninformationen und die vorhandenen DNS-Einträge, um die aktuelle DNS-Konfiguration zu verstehen. Erstellen, ändern und löschen Sie DNS-Einträge, jedoch nur für bestimmte ROSA-bezogene Domänenmuster`.hypershift.local`, einschließlich, `.openshiftapps.com` `.devshift.org.openshiftusgov.com`, und. `.devshiftusgov.com` Fügen Sie Tags auf Route 53 53-Ressourcen für die Ressourcenverwaltung und Organisation hinzu, ändern oder entfernen Sie sie.
- `tag`— Entdecken und Auflisten von AWS Ressourcen anhand ihrer Tags. Dies ist nützlich, um Ressourcen zu identifizieren, die von ROSA verwaltet werden.

Weitere Informationen zur Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie unter ROSASharedVPCRoute53Richtlinie im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAShared VPCEndpoint Richtlinie

Sie können sie `ROSASharedVPCEndpointPolicy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie einer IAM-Rolle zuordnen, damit ein ROSA-Cluster Aufrufe an andere AWS-Services in gemeinsam genutzten VPC-Umgebungen tätigen kann.

Diese Richtlinie ermöglicht es dem ROSA-Installationsprogramm, VPC-Endpunkte und Sicherheitsgruppen in gemeinsam genutzten VPC-Umgebungen zu konfigurieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, die es dem ROSA-Installationsprogramm ermöglichen, die folgenden Aufgaben auszuführen:

- `ec2`— Schreibgeschützte Berechtigungen zur Beschreibung von VPC-bezogenen Ressourcen, einschließlich VPC-Endpunkten, und Sicherheitsgruppen VPCs, um die Netzwerkumgebung zu verstehen. Sicherheitsgruppen mit tagbasierten Einschränkungen erstellen, löschen und ändern, sodass ROSA Sicherheitsgruppen für Clusternetzwerke erstellen und verwalten und gleichzeitig den Betrieb auf Ressourcen beschränken kann, die mit ROSA gekennzeichnet sind. Erstellen, ändern und löschen Sie VPC-Endpoints mit tagbasierten Einschränkungen, sodass ROSA VPC-Endpunkte für private Konnektivität in gemeinsam genutzten VPC-Umgebungen erstellen und verwalten kann AWS-Services . Wenden Sie während der Erstellung Tags auf neu erstellte VPC-Endpunkte und Sicherheitsgruppen an, um eine korrekte Identifizierung und Verwaltung der Ressourcen zu gewährleisten.

Weitere Informationen zur Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie unter ROSASharedVPCEndpointRichtlinie im Referenzhandbuch für AWS verwaltete Richtlinien.

ROSA mit HCP-Betreiberrichtlinien

Dieser Abschnitt enthält Einzelheiten zu den Betreiberrichtlinien, die für ROSA mit Hosted Control Planes (HCP) erforderlich sind. Sie können diese AWS verwalteten Richtlinien den Operatorrollen zuordnen, die für die Verwendung von ROSA mit HCP erforderlich sind. Die Berechtigungen sind erforderlich, damit OpenShift Betreiber ROSA mit HCP-Clusterknoten verwalten können.

> **Note**
>
> AWS verwaltete Richtlinien sind für die Verwendung durch ROSA mit Hosted Control Planes (HCP) vorgesehen. Die klassischen ROSA-Cluster verwenden vom Kunden verwaltete IAM-Richtlinien. Weitere Informationen zu den klassischen ROSA-Richtlinien finden Sie unter the section called “Klassische Kontorichtlinien von ROSA” undthe section called “Richtlinien für klassische ROSA-Betreiber”.

AWS verwaltete Richtlinie: ROSAAmazon EBSCSIDriver OperatorPolicy

Sie können sie `ROSAAmazonEBSCSIDriverOperatorPolicy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie einer Operator-IAM-Rolle zuordnen, damit ein ROSA-Cluster mit gehosteten

Steuerungsebenen Anrufe an andere AWS-Services vornehmen kann. Für jeden Cluster ist ein eigener Satz von Operatorrollen erforderlich.

Diese Richtlinie gewährt dem Amazon EBS CSI-Treiberoperator die erforderlichen Berechtigungen zur Installation und Wartung des Amazon EBS CSI-Treibers auf einem ROSA Cluster. Weitere Informationen zum Operator finden Sie in der OpenShift GitHub Dokumentation unter aws-ebs-csi-driver Operator.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen der Amazon EBS Fahreroperator die folgenden Aufgaben ausführen kann:

- `ec2`— Amazon EBS Volumes, die an Amazon EC2 Instanzen angehängt sind, erstellen, ändern, anhängen, trennen und löschen. Erstellen und löschen Sie Amazon EBS Volume-Snapshots und listen Sie Amazon EC2 Instances, Volumes und Snapshots auf.

Das vollständige JSON-Richtliniendokument finden Sie ROSAAmazonEBSCSIDriverOperatorPolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAIngress OperatorPolicy

Sie können sie `ROSAIngressOperatorPolicy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie einer Operator-IAM-Rolle zuordnen, damit ein ROSA-Cluster mit gehosteten Steuerungsebenen Anrufe an andere AWS-Services vornehmen kann. Für jeden Cluster ist ein eigener Satz von Operatorrollen erforderlich.

Diese Richtlinie gewährt dem Ingress-Operator die erforderlichen Berechtigungen zur Bereitstellung und Verwaltung von Load Balancern und DNS-Konfigurationen für ROSA Cluster. Die Richtlinie ermöglicht den Lesezugriff auf Tag-Werte. Der Operator filtert dann die Tag-Werte nach Route 53 Ressourcen, um gehostete Zonen zu erkennen. Weitere Informationen zum Operator finden Sie in der OpenShift GitHub Dokumentation unter OpenShift Ingress Operator.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, die es dem Ingress-Operator ermöglichen, die folgenden Aufgaben auszuführen:

- `elasticloadbalancing`— Beschreiben Sie den Status der bereitgestellten Load Balancer.

- `route53`— Route 53 Listet gehostete Zonen auf und bearbeitet Einträge, die das vom ROSA-Cluster kontrollierte DNS verwalten.
- `tag`— Verwaltet markierte Ressourcen mithilfe der entsprechenden `tag:GetResources` Berechtigung.

Das vollständige JSON-Richtliniendokument finden Sie ROSAIngressOperatorPolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAImage RegistryOperatorPolicy

Sie können sie `ROSAImageRegistryOperatorPolicy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie einer Operator-IAM-Rolle zuordnen, damit ein ROSA-Cluster mit gehosteten Steuerungsebenen Anrufe an andere AWS-Services vornehmen kann. Für jeden Cluster ist ein eigener Satz von Operatorrollen erforderlich.

Diese Richtlinie gewährt dem Image Registry Operator die erforderlichen Berechtigungen zur Bereitstellung und Verwaltung von Ressourcen für die ROSA Cluster-interne Image-Registry und abhängige Dienste, einschließlich S3. Dies ist erforderlich, damit der Betreiber die interne Registrierung eines ROSA Clusters installieren und verwalten kann. Weitere Informationen zum Operator finden Sie in der OpenShift GitHub Dokumentation unter Image Registry Operator.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen der Image Registry Operator die folgenden Aktionen ausführen kann:

- `s3`— Amazon S3 Buckets als persistenten Speicher für Container-Image-Inhalte und Cluster-Metadaten verwalten und auswerten.

Das vollständige JSON-Richtliniendokument finden Sie ROSAImageRegistryOperatorPolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSACloud NetworkConfigOperatorPolicy

Sie können sie `ROSACloudNetworkConfigOperatorPolicy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie einer Operator-IAM-Rolle zuordnen, damit ein ROSA-Cluster mit gehosteten Steuerungsebenen Anrufe an andere AWS-Services vornehmen kann. Für jeden Cluster ist ein eigener Satz von Operatorrollen erforderlich.

Diese Richtlinie gewährt dem Cloud Network Config Controller Operator die erforderlichen Berechtigungen zur Bereitstellung und Verwaltung von Netzwerkressourcen für das ROSA Cluster-Netzwerk-Overlay. Der Betreiber verwendet diese Berechtigungen, um private IP-Adressen für Amazon EC2 Instanzen als Teil des ROSA Clusters zu verwalten. Weitere Informationen zum Operator finden Sie loud-network-config-controller in der OpenShift GitHub Dokumentation unter C.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen der Cloud Network Config Controller Operator die folgenden Aufgaben ausführen kann:

- `ec2`— Lesen, Zuweisen und Beschreiben von Konfigurationen für die Verbindung von Amazon EC2 Instances, Amazon VPC Subnetzen und elastischen Netzwerkschnittstellen in einem ROSA Cluster.

Das vollständige JSON-Richtliniendokument finden Sie ROSACloudNetworkConfigOperatorPolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAKube ControllerPolicy

Sie können sie `ROSAKubeControllerPolicy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie einer Operator-IAM-Rolle zuordnen, damit ein ROSA-Cluster mit gehosteten Steuerungsebenen Anrufe an andere AWS-Services vornehmen kann. Für jeden Cluster ist ein eigener Satz von Operatorrollen erforderlich.

Diese Richtlinie gewährt dem Kube-Controller die erforderlichen Berechtigungen zur Verwaltung von Amazon EC2 Elastic Load Balancing, und AWS KMS Ressourcen für einen ROSA-Cluster mit gehosteten Steuerungsebenen. Weitere Informationen zu diesem Controller finden Sie in der OpenShift Dokumentation unter Controller-Architektur.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, die es dem Kube-Controller ermöglichen, die folgenden Aufgaben auszuführen:

- `ec2`— Amazon EC2 Instanz-Sicherheitsgruppen erstellen, löschen und Tags hinzufügen. Fügen Sie Sicherheitsgruppen Regeln für eingehenden Datenverkehr hinzu. Beschreiben Sie Availability Zones, Amazon EC2 Instanzen, Routing-Tabellen VPCs, Sicherheitsgruppen und Subnetze.
- `elasticloadbalancing`— Erstellen und verwalten Sie Load Balancer und deren Richtlinien. Erstellen und verwalten Sie Load Balancer-Listener. Registrieren und deregistrieren Sie Ziele bei

Zielgruppen und verwalten Sie Zielgruppen. Registrieren und deregistrieren Sie Amazon EC2 Instances bei einem Load Balancer und fügen Sie Tags zu Load Balancern hinzu.

- `kms`— Ruft detaillierte Informationen zu einem Schlüssel ab. AWS KMS Dies ist für die Verwendung verschlüsselter `etcd` Daten erforderlich, wenn die `etcd` Verschlüsselung bei der Clustererstellung aktiviert ist.

Das vollständige JSON-Richtliniendokument finden Sie ROSAKubeControllerPolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSANode PoolManagementPolicy

Sie können sie `ROSANodePoolManagementPolicy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie an die IAM-Rolle eines Operators anhängen, damit ein ROSA-Cluster mit gehosteten Steuerungsebenen Anrufe an andere AWS Dienste tätigen kann. Für jeden Cluster ist ein eigener Satz von Operatorrollen erforderlich.

Diese Richtlinie gewährt dem NodePool Controller die erforderlichen Berechtigungen zum Beschreiben, Ausführen und Beenden von Amazon EC2 Instanzen, die als Worker-Knoten verwaltet werden. Diese Richtlinie gewährt auch Berechtigungen zur Festplattenverschlüsselung des Worker-Knoten-Root-Volumes mithilfe von AWS KMS Schlüsseln, zur Kennzeichnung der elastic network interface, die mit dem Worker-Knoten verbunden ist, und zum Zugriff auf Amazon EC2 EC2-Kapazitätsreservierungen. Weitere Informationen zu diesem Controller finden Sie in der OpenShift Dokumentation unter Controller-Architektur.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen der NodePool Controller die folgenden Aufgaben ausführen kann:

- `ec2`— Führen Sie Amazon EC2 Instances mithilfe von AMIs Hosted in aus, das AWS-Konten Eigentum von Red Hat ist und von Red Hat verwaltet wird. Verwalten Sie EC2-Lebenszyklen im Cluster. ROSA Erstellen und integrieren Sie dynamisch Worker-Knoten mit Elastic Load Balancing,, Amazon VPC Route 53, Amazon EBS und. Amazon EC2 Greifen Sie auf Kapazitätsreservierungen zu und beschreiben Sie sie, um die Funktion zur Kapazitätsreservierung in ROSA zu unterstützen.
- `iam`— Verwendung Elastic Load Balancing über die angegebene serviceverknüpfte Rolle. `AWSServiceRoleForElasticLoadBalancing` Weisen Sie Amazon EC2 Instanzprofilen Rollen zu.

- `kms`— Lesen Sie einen AWS KMS Schlüssel, erstellen und verwalten Sie Zuschüsse für und geben Sie einen eindeutigen symmetrischen Datenschlüssel zur Verwendung außerhalb von AWS KMS zurück. Amazon EC2 Dies ist erforderlich, um die Festplattenverschlüsselung des Root-Volumes des Worker-Knotens zu ermöglichen.

Das vollständige JSON-Richtliniendokument finden Sie ROSANodePoolManagementPolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAKMSProvider Richtlinie

Sie können sie `ROSAKMSProviderPolicy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie einer Operator-IAM-Rolle zuordnen, damit ein ROSA-Cluster mit gehosteten Steuerungsebenen Anrufe an andere AWS-Services vornehmen kann. Für jeden Cluster ist ein eigener Satz von Operatorrollen erforderlich.

Diese Richtlinie gewährt dem integrierten AWS Encryption Provider die erforderlichen Berechtigungen zur Verwaltung von AWS KMS Schlüsseln, die `etcd` Datenverschlüsselung unterstützen. Diese Richtlinie ermöglicht Amazon EC2 die Verwendung von KMS-Schlüsseln, die der AWS Encryption Provider zur Verschlüsselung und Entschlüsselung von Daten bereitstellt. `etcd` Weitere Informationen zu diesem Anbieter finden Sie unter AWS Encryption Provider in der GitHub Kubernetes-Dokumentation.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, die es dem AWS Encryption Provider ermöglichen, die folgenden Aufgaben auszuführen:

- `kms`— Schlüssel verschlüsseln, entschlüsseln und abrufen. AWS KMS Dies ist für die Verwendung verschlüsselter `etcd` Daten erforderlich, wenn die `etcd` Verschlüsselung bei der Clustererstellung aktiviert ist.

Das vollständige JSON-Richtliniendokument finden Sie unter ROSAKMSProviderRichtlinie im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAControl PlaneOperatorPolicy

Sie können sie `ROSAControlPlaneOperatorPolicy` an Ihre IAM Entitäten anhängen. Sie müssen diese Richtlinie einer Operator-IAM-Rolle zuordnen, damit ein ROSA-Cluster mit gehosteten

Steuerungsebenen Anrufe an andere AWS-Services vornehmen kann. Für jeden Cluster ist ein eigener Satz von Operatorrollen erforderlich.

Diese Richtlinie gewährt dem Kontrollebenenbetreiber die erforderlichen Berechtigungen für die Verwaltung Amazon EC2 und die Route 53 Ressourcen für ROSA mit gehosteten Steuerungsebenen-Clustern. Weitere Informationen zu diesem Operator finden Sie in der OpenShift Dokumentation unter Controller-Architektur.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen der Bediener der Steuerungsebene die folgenden Aufgaben ausführen kann:

- `ec2`— Amazon VPC Endgeräte erstellen und verwalten.
- `route53`— Route 53 Datensätze auflisten und ändern und gehostete Zonen auflisten.

Das vollständige JSON-Richtliniendokument finden Sie ROSAControlPlaneOperatorPolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

ROSA Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die ROSA seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite.

Änderungen	Beschreibung	Date
ROSANodePoolManagementPolicy — Die Richtlinie wurde aktualisiert	ROSA hat die Richtlinie aktualisiert, um den Ressourcenzugriff für Amazon EC2 EC2-Kapazitätsreservierungen hinzuzufügen. Diese Änderung ermöglicht es dem NodePool Controller, auf Kapazitätsreservierungen zuzugreifen und diese zu beschreiben, um	3. September 2025

Änderungen	Beschreibung	Date
	das Ressourcenmanagement zu verbessern. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSANode PoolManagementPolicy”.	
ROSASharedVPCEndpointRichtlinie — Neue Richtlinie hinzugefügt	ROSA hat eine neue Richtlinie hinzugefügt, die es dem ROSA Installateur ermöglicht, VPC-Endpunkte und Sicherheitsgruppen in gemeinsam genutzten VPC-Umgebungen zu konfigurieren. Diese Richtlinie bietet eine Teilmenge von EC2-Berechtigungen, die auf gemeinsame VPC-Anwendungsfälle zugeschnitten sind. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAShared VPCEndpoint Richtlinie”.	7. August 2025

Änderungen	Beschreibung	Date
ROSASharedVPCRoute 53Richtlinie — Neue Richtlinie hinzugefügt	ROSA hat eine neue Richtlini e hinzugefügt, die es dem ROSA Installateur ermöglich t, Route 53 53-Datensätze in gemeinsam genutzten VPC-Umgebungen zu konfiguri eren. Diese Richtlinie bietet eine Teilmenge von Route 53 53-Berechtigungen, die auf gemeinsame VPC-Anwen dungsfälle zugeschnitten sind. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltet e Richtlinie: ROSAShared VPCRoute53 Richtlinie”.	7. August 2025

Änderungen	Beschreibung	Date
ROSAInstallerRichtlinie — Richtlinie aktualisiert	ROSA hat die Richtlinie aktualisiert, sodass der ROSA Installateur Amazon EC2 EC2-Kapazitätsreservierungen überprüfen kann, um die neue Funktion für Kapazitätsreservierungen in ROSA zu unterstützen. Dieses Update ermöglicht es dem Installationsprogramm auch, Tags in Subnetzen mithilfe von Tag-Schlüsseln zu löschen, um das Tag-Management im Kubernetes-Cluster zu verbessern. `"kubernetes.io/cluster/*"` Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAInstaller Richtlinie”.	7. August 2025

Änderungen	Beschreibung	Date
ROSAImageRegistryOperatorPolicy — Die Richtlinie wurde aktualisiert	ROSA hat die Richtlinie aktualisiert, sodass die Berechtigungen bis auf die Ressourcenebene des S3-Buckets beschränkt sind. Diese Änderung erfüllt die Speicheranforderungen von ROSA sowohl für AWS kommerzielle Zwecke als auch für Regionen. GovCloud Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAImage RegistryOperatorPolicy”.	19. Mai 2025
ROSANodePoolManagementPolicy — Richtlinie aktualisiert	ROSA hat die Richtlinie aktualisiert, um das Taggen der elastic network interface zu ermöglichen, die an den Worker-Knoten angeschlossen ist. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSANodePoolManagementPolicy”.	5. Mai 2025

Änderungen	Beschreibung	Date
ROSAImageRegistryOperatorPolicy — Die Richtlinie wurde aktualisiert	ROSA hat die Richtlinie aktualisiert, um es dem Red Hat OpenShift Image Registry Operator zu ermöglichen, Amazon S3 S3-Buckets und -Objekte in AWS GovCloud Regionen bereitzustellen und zu verwalten, damit sie von der ROSA In-Cluster-Image-Registry verwendet werden können. Diese Änderung erfüllt die ROSA-Speicheranforderungen für Regionen. AWS GovCloud Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAImage RegistryOperatorPolicy”.	16. April 2025
ROSAWorkerInstancePolicy — Richtlinie aktualisiert	ROSA hat die Richtlinie aktualisiert, sodass Worker-Knoten Bilder von ROSA-verwalteten ECR-Repositorys auswerten und abrufen können, die für die Cluster-Installation und das Worker-Node-Lebenszyklusmanagement erforderlich sind. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAWorker InstancePolicy”.	03. März 2025

Änderungen	Beschreibung	Date
ROSANodePoolManagementPolicy — Die Richtlinie wurde aktualisiert	ROSA hat die Richtlinie aktualisiert, sodass elastische Netzwerkschnittstellen ähnlich wie EC2-Instances nur bei ec2: RunInstances -Aufrufen gekennzeichnet werden können, wenn die Anfrage das Tag enthält. `red-hat-managed: true` Diese Berechtigungen sind erforderlich, um ROSA mit HCP 4.17-Clustern zu unterstützen. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSANodePoolManagementPolicy”.	24. Februar 2025
ROSAAmazonEBSCSIDriverOperatorPolicy — Richtlinie aktualisiert	ROSA hat die Richtlinie aktualisiert, um die neue Amazon EBS Snapshot-Autorisierungs-API zu unterstützen. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAAmazon EBSCSIDriverOperatorPolicy”.	17. Januar 2025

Änderungen	Beschreibung	Date
ROSANodePoolManagementPolicy — Richtlinie aktualisiert	ROSA hat die Richtlinie aktualisiert, sodass der ROSA Knotenpool-Manager DHCP-Optionssätze beschreiben kann, um die richtigen privaten DNS-Namen festzuleg en. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltet e Richtlinie: ROSANode PoolManagementPolicy”.	2. Mai 2024
ROSAInstallerRichtlinie — Richtlinie aktualisiert	ROSA hat die Richtlinie aktualisiert, sodass das ROSA Installationsprogramm mithilfe von Tagschlüsseln Tags zu Subnetzen hinzufügen kann. `"kubernetes.io/cluster/*"` Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAInstaller Richtlinie”.	24. April 2024
ROSASRESupportRichtlinie — Richtlinie aktualisiert	ROSA hat die Richtlinie aktualisiert, sodass die SRE-Rolle Informationen zu Instanzprofilen abrufen kann, die mit ROSA as gekennzeichnet wurden`red-hat-managed` . Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSASRESupport Richtlinie”.	10. April 2024

Änderungen	Beschreibung	Date
ROSAInstallerRichtlinie — Richtlinie aktualisiert	ROSA hat die Richtlinie aktualisiert, sodass das ROSA Installationsprogramm überprüfen kann, ob AWS verwaltete Richtlinien für an IAM Rollen angehängt ROSA sind, die von verwendet werden ROSA. Mit diesem Update kann das Installat ionsprogramm auch feststell en, ob vom Kunden verwaltet e Richtlinien an ROSA Rollen angehängt wurden. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAInstaller Richtlinie”.	10. April 2024

Änderungen	Beschreibung	Date
ROSAInstallerRichtlinie — Die Richtlinie wurde aktualisiert	ROSA hat die Richtlinie aktualisiert, sodass der Dienst Warnmeldungen für das Installationsprogramm ausgeben kann, wenn die Clusterinstallation aufgrund eines fehlenden kundenspezifischen Cluster-OIDC-Anbieters fehlschlägt. Dieses Update ermöglicht es dem Dienst auch, vorhandene DNS-Nameserver abzurufen, sodass Cluster-Bereitstellungsvorgänge idempotent sind. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAInstaller Richtlinie”.	26. Januar 2024
ROSASRESupportRichtlinie — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass der Dienst mithilfe der DescribeSecurityGroups API Lesevorgänge für Sicherheitsgruppen durchführen kann. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSASRESupport Richtlinie”.	22. Januar 2024

Änderungen	Beschreibung	Date
ROSAImageRegistryOperatorPolicy — Die Richtlinie wurde aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass der Image-Registry-Betreiber Maßnahmen für Amazon S3 Buckets in Regionen mit 14-stelligen Namen ergreifen kann. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAImageRegistryOperatorPolicy”.	12. Dezember 2023
ROSAKubeControllerPolicy — Die Richtlinie wurde aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass Availability Zones, Amazon EC2 Instances, Routing-Tabellen, Sicherheitsgruppen und Subnetze beschrieben werden können. kube-controller-manager VPCs Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAKube ControllerPolicy”.	16. Oktober 2023
ROSAManageAbonnement — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, um die ROSA mit gehosteten Steuerungsebenen hinzuzufügen ProductId. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAManage Abonnement”.	1. August 2023

Änderungen	Beschreibung	Date
ROSAKubeControllerPolicy — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass Network Load Balancer als Kubernetes-Dienst-Loadbalancer erstellt werden können. kube-controller-manager Network Load Balancer bieten eine bessere Fähigkeit, volatile Workloads zu bewältigen, und unterstützen statische IP-Adressen für den Load Balancer. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAKube ControllerPolicy”.	13. Juli 2023
ROSANodePoolManagementPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem NodePool Controller ermöglicht, als Worker-Knoten verwaltete Amazon EC2 Instanzen zu beschreiben, auszuführen und zu beenden. Diese Richtlinie ermöglicht auch die Festplattenverschlüsselung des Worker-Knoten-Root-Volumes mithilfe von AWS KMS Schlüsseln. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSANode PoolManagementPolicy”.	08. Juni 2023

Änderungen	Beschreibung	Date
ROSAInstallerRichtlinie — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Installationsprogramm ermöglicht, AWS Ressourcen zu verwalten, die die Clusterinstallation unterstützen. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAInstaller Richtlinie”.	6. Juni 2023
ROSASRESupportRichtlinie — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es Red Hat ermöglicht, AWS Ressourcen im Zusammenhang mit ROSA Clustern direkt SREs zu beobachten, zu diagnostizieren und zu unterstützen, einschließlich der Möglichkeit, den Status von ROSA Clusterknoten zu ändern. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSASRESupport Richtlinie”.	01. Juni 2023

Änderungen	Beschreibung	Date
ROSAKMSProviderRichtlinie — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem integrierten AWS Encryption Provider ermöglicht, AWS KMS Schlüssel zur Unterstützung der etcd-Datenverschlüsselung zu verwalten. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAKMSProviderRichtlinie”.	27. April 2023
ROSAKubeControllerPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Kube-Controller ermöglicht Amazon EC2 Elastic Load Balancing, AWS KMS Ressourcen für Cluster ROSA mit gehosteten Steuerungsebenen zu verwalten und zu verwalten. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAKubeControllerPolicy”.	27. April 2023

Änderungen	Beschreibung	Date
ROSAImageRegistryOperatorPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Image Registry Operator ermöglicht, Ressourcen für die ROSA Cluster-Image-Registry und abhängige Dienste, einschließlich S3, bereitzustellen und zu verwalten . Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAImageRegistryOperatorPolicy”.	27. April 2023
ROSAControlPlaneOperatorPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Bediener der Kontrollebene ermöglicht, Cluster ROSA mit gehosteten Steuerungsebenen zu verwalten Amazon EC2 und Route 53 Ressourcen zu verwalten. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAControl PlaneOperatorPolicy”.	24. April 2023

Änderungen	Beschreibung	Date
ROSACloudNetworkConfigOperatorPolicy — Neue Richtlinie hinzugefügt	ROSA hat eine neue Richtlinie hinzugefügt, die es dem Cloud Network Config Controller Operator ermöglicht, Netzwerkressourcen für das ROSA Cluster-Netzwerk-Overlay bereitzustellen und zu verwalten. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSACloud NetworkConfigOperatorPolicy”.	20. April 2023
ROSAIngressOperatorPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Ingress Operator ermöglicht, Load Balancer und DNS-Konfigurationen für ROSA Cluster bereitzustellen und zu verwalten. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAIngress OperatorPolicy”.	20. April 2023

Änderungen	Beschreibung	Date
ROSAAmazonEBSCSIDriverOperatorPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Amazon EBS CSI-Treiberoperator ermöglicht, den Amazon EBS CSI-Treiber auf einem ROSA Cluster zu installieren und zu warten. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAAmazon EBSCSIDriver OperatorPolicy”.	20. April 2023
ROSAWorkerInstancePolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Dienst ermöglicht, Clusterressourcen zu verwalten. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAWorker InstancePolicy”.	20. April 2023
ROSAManageAbonnement — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, um die AWS Marketplace für die Verwaltung des ROSA Abonnements erforderlichen Berechtigungen zu gewähren. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: ROSAManage Abonnement”.	11. April 2022

Änderungen	Beschreibung	Date
Red Hat OpenShift Service in AWS hat begonnen, Änderungen zu verfolgen	Red Hat OpenShift Service in AWS hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	2. März 2022

Fehlerbehebung bei ROSA Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit ROSA und auftreten können IAM.

AWS Organizations Die Dienststeuerungsrichtlinie verweigert die erforderlichen Berechtigungen AWS Marketplace

Wenn Ihre AWS Organizations Service Control Policy (SCP) die erforderlichen AWS Marketplace Abonnementberechtigungen nicht zulässt, wenn Sie versuchen ROSA, sie zu aktivieren, tritt der folgende Konsolenfehler auf.

```
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.
```

Wenn Sie diesen Fehler erhalten, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die die Konten für Ihre Organisation verwaltet. Bitten Sie diese Person, Folgendes zu tun:

1. Konfigurieren Sie den SCP so, dass er `aws-marketplace:Subscribeaws-marketplace:Unsubscribe`, und `aws-marketplace:ViewSubscriptions` Berechtigungen zulässt. Weitere Informationen finden Sie unter Aktualisieren eines SCP im AWS Organizations Benutzerhandbuch.
2. Aktivieren Sie ROSA diese Option im Verwaltungskonto der Organisation.
3. Teilen Sie das ROSA Abonnement mit Mitgliedskonten, für die innerhalb der Organisation Zugriff erforderlich ist. Weitere Informationen finden Sie im AWS Marketplace Buyer Guide unter Gemeinsame Nutzung von Abonnements in einer Organisation.

Der Benutzer oder die Rolle verfügt nicht über die erforderlichen AWS Marketplace Berechtigungen

Wenn Ihr IAM Principal beim Versuch, die Aktivierung durchzuführen, nicht über die erforderlichen AWS Marketplace Abonnementberechtigungen verfügt ROSA, tritt der folgende Konsolenfehler auf.

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

Um dieses Problem zu beheben, führen Sie die folgenden Schritte aus:

1. Rufen Sie die IAM Konsole auf und fügen Sie die AWS verwaltete Richtlinie `ROSAManageSubscription` Ihrer IAM-Identität hinzu. Weitere Informationen finden Sie unter ROSAManageAbonnement im Referenzhandbuch für AWS verwaltete Richtlinien.
2. Folgen Sie dem Verfahren unter the section called “AWS Voraussetzungen aktivieren ROSA und konfigurieren”.

Wenn Sie nicht berechtigt sind, Ihre in festgelegten Berechtigungen einzusehen oder zu aktualisieren, IAM oder wenn Sie eine Fehlermeldung erhalten, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Bitten Sie diese Person, Ihre IAM Identität als Anlage `ROSAManageSubscription` beizufügen, und folgen Sie den Anweisungen unterthe section called “AWS Voraussetzungen aktivieren ROSA und konfigurieren”. Wenn ein Administrator diese Aktion ausführt, wird sie aktiviert, ROSA indem er den Berechtigungssatz für alle IAM Identitäten unter dem AWS-Konto aktualisiert.

Erforderliche AWS Marketplace Berechtigungen, die von einem Administrator blockiert wurden

Wenn Ihr Kontoadministrator die erforderlichen AWS Marketplace Abonnementberechtigungen blockiert hat, tritt beim Versuch, sie zu aktivieren, der folgende Konsolenfehler auf 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.
```

Wenn Sie diesen Fehler erhalten, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Bitten Sie diese Person, Folgendes zu tun:

1. Rufen Sie die ROSA Konsole auf und fügen Sie die AWS verwaltete Richtlinie `ROSAManageSubscription` Ihrer IAM-Identität hinzu. Weitere Informationen finden Sie unter ROSAManageAbonnement im Referenzhandbuch für AWS verwaltete Richtlinien.
2. Folgen Sie zum Aktivieren the section called “AWS Voraussetzungen aktivieren ROSA und konfigurieren” den Anweisungen unter ROSA. Dieses Verfahren ermöglicht es, ROSA indem der Berechtigungssatz für alle IAM Identitäten unter dem AWS-Konto aktualisiert wird.

Fehler beim Erstellen des Load Balancers: AccessDenied

Wenn Sie keinen Load Balancer erstellt haben, ist die mit dem `AWSServiceRoleForElasticLoadBalacing` Dienst verknüpfte Rolle möglicherweise nicht in Ihrem Konto vorhanden. Der folgende Fehler tritt auf, wenn Sie versuchen, eine ROSA Cluster ohne die `AWSServiceRoleForElasticLoadBalacing` Rolle in Ihrem Konto zu erstellen.

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

Um dieses Problem zu beheben, führen Sie die folgenden Schritte aus:

1. Prüfen Sie, ob Ihr Konto die `AWSServiceRoleForElasticLoadBalancing` Rolle hat.

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

2. Wenn Sie diese Rolle nicht haben, folgen Sie den Anweisungen zum Erstellen der Rolle unter Erstellen der serviceverknüpften Rolle im Elastic Load Balancing Benutzerhandbuch.

Resilienz in ROSA

AWS Widerstandsfähigkeit der globalen Infrastruktur

Die AWS globale Infrastruktur basiert auf AWS-Regionen Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

ROSA bietet Kunden die Möglichkeit, die Kubernetes-Steuerungsebene und die Datenebene in einer einzigen AWS Availability Zone oder in mehreren Availability Zones auszuführen. Single-AZ-Cluster können zwar für Experimente nützlich sein, Kunden werden jedoch ermutigt, ihre Workloads in mehr als einer Availability Zone auszuführen. Dadurch wird sichergestellt, dass Anwendungen selbst einem kompletten Ausfall der Availability Zone standhalten können — ein an sich schon sehr seltenes Ereignis.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

ROSA Ausfallsicherheit von Clustern

Die ROSA Steuerungsebene besteht aus mindestens drei Knoten der OpenShift Steuerungsebene. Jeder Knoten der Steuerungsebene besteht aus einer API-Serverinstanz, einer `etcd` Instanz und Controllern. Bei einem Ausfall eines Knotens auf der Kontrollebene werden alle API-Anfragen automatisch an die anderen verfügbaren Knoten weitergeleitet, um die Verfügbarkeit des Clusters sicherzustellen.

Die ROSA Datenebene besteht aus mindestens zwei OpenShift Infrastrukturknoten und zwei OpenShift Worker-Knoten. Auf Infrastrukturknoten werden Pods ausgeführt, die OpenShift Cluster-Infrastrukturkomponenten wie den Standardrouter, die integrierte OpenShift Registrierung und die Komponenten für Cluster-Metriken und -Überwachung unterstützen. OpenShift Worker-Knoten führen Anwendungs-Pods für Endbenutzer aus.

Red Hat Site Reliability Engineers (SREs) verwalten die gesamte Steuerungsebene und die Infrastrukturknoten. Red Hat überwacht den ROSA Cluster SREs proaktiv und ist dafür verantwortlich, alle ausgefallenen Knoten der Steuerungsebene und Infrastrukturknoten zu ersetzen. Weitere Informationen finden Sie unter the section called “Verantwortlichkeiten”.

> **Important**
>
> Da es ROSA sich um einen verwalteten Service handelt, ist Red Hat für die Verwaltung der zugrunde liegenden AWS Infrastruktur verantwortlich, die ROSA verwendet wird. Kunden sollten nicht versuchen, die ROSA verwendeten Amazon EC2 Instances von der AWS Konsole oder aus manuell herunterzufahren AWS CLI. Diese Aktion kann zum Verlust von Kundendaten führen.

Wenn ein Worker-Knoten auf der Datenebene ausfällt, verlagert die Steuerungsebene ungeplante Pods auf die funktionierenden Worker-Knoten, bis der ausgefallene Knoten wiederhergestellt oder ersetzt ist. Ausgefallene Worker-Knoten können manuell oder automatisch ersetzt werden, indem die automatische Skalierung der Maschinen in einem Cluster aktiviert wird. Weitere Informationen finden Sie unter Cluster-Autoscaling in der Red Hat-Dokumentation.

Ausfallsicherheit von vom Kunden bereitgestellten Anwendungen

Es ROSA bietet zwar viele Schutzmaßnahmen, um eine hohe Verfügbarkeit des Service zu gewährleisten, aber die Kunden sind dafür verantwortlich, ihre bereitgestellten Anwendungen so zu gestalten, dass sie hochverfügbar sind, um Workloads vor Ausfallzeiten zu schützen. Weitere Informationen finden Sie unter About Availability for ROSA in der Red Hat-Dokumentation.

Sicherheit der Infrastruktur in ROSA

Als verwalteter Dienst Red Hat OpenShift Service in AWS wird er durch die AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der Best Practices für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar — AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff ROSA über das AWS Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS -Security-Token-Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Cluster-Netzwerkisolierung

Die Site Reliability Engineers von Red Hat (SREs) sind für das laufende Management und die Netzwerksicherheit des Clusters und der zugrunde liegenden Anwendungsplattform verantwortlich.

Weitere Informationen zu den Zuständigkeiten von Red Hat für ROSA finden Sie unterthe section called “Verantwortlichkeiten”.

Wenn Sie einen neuen Cluster erstellen, besteht die Möglichkeit ROSA , einen öffentlichen Kubernetes-API-Serverendpunkt und Anwendungsrouten oder einen privaten Kubernetes-API-Endpunkt und Anwendungsrouten zu erstellen. Diese Verbindung wird für die Kommunikation mit Ihrem Cluster verwendet (mithilfe von OpenShift Verwaltungstools wie der ROSA CLI und OpenShift CLI). Eine private Verbindung ermöglicht es, dass die gesamte Kommunikation zwischen Ihren Knoten und dem API-Server in Ihrer VPC bleibt. Wenn Sie den privaten Zugriff auf den API-Server und die Anwendungsrouten aktivieren, müssen Sie eine vorhandene VPC verwenden und AWS PrivateLink die VPC mit dem OpenShift Backend-Service verbinden.

Der Kubernetes-API-Serverzugriff wird durch eine Kombination aus AWS Identity and Access Management (IAM) und systemeigener rollenbasierter Zugriffskontrolle (RBAC) von Kubernetes gesichert. Weitere Informationen zu Kubernetes RBAC finden Sie unter Using RBAC Authorization in der Kubernetes-Dokumentation.

ROSA ermöglicht es Ihnen, sichere Anwendungsrouten mithilfe verschiedener Arten von TLS-Terminierung zu erstellen, um dem Client Zertifikate auszustellen. Weitere Informationen finden Sie unter Gesicherte Routen in der Red Hat-Dokumentation.

Wenn Sie einen ROSA Cluster in einer vorhandenen VPC erstellen, geben Sie die VPC-Subnetze und Availability Zones an, die Ihr Cluster verwenden soll. Sie definieren auch die CIDR-Bereiche, die das Cluster-Netzwerk verwenden soll, und ordnen diese CIDR-Bereiche den VPC-Subnetzen zu. Weitere Informationen finden Sie unter CIDR-Bereichsdefinitionen in der Red Hat-Dokumentation.

Für Cluster, die den öffentlichen API-Endpunkt verwenden, ROSA erfordert dies, dass Ihre VPC mit einem öffentlichen und privaten Subnetz für jede Availability Zone konfiguriert ist, in der der Cluster bereitgestellt werden soll. Für Cluster, die den privaten API-Endpunkt verwenden, sind nur private Subnetze erforderlich.

Wenn Sie eine vorhandene VPC verwenden, können Sie Ihre ROSA Cluster so konfigurieren, dass sie während oder nach der Clustererstellung einen HTTP- oder HTTPS-Proxyserver verwenden, um den Cluster-Webverkehr zu verschlüsseln und so eine weitere Sicherheitsebene für Ihre Daten hinzuzufügen. Wenn Sie einen Proxy aktivieren, wird den Kernkomponenten des Clusters der direkte Zugriff auf das Internet verweigert. Der Proxy verweigert Benutzerarbeitslasten nicht den Internetzugang. Weitere Informationen finden Sie unter Konfiguration eines clusterweiten Proxys in der Red Hat-Dokumentation.

Pod-Netzwerkisolierung

Wenn Sie ein Clusteradministrator sind, können Sie Netzwerkrichtlinien auf Pod-Ebene definieren, die den Datenverkehr auf Pods in Ihrem ROSA Cluster einschränken.

ROSA Dienstkontingente

Red Hat OpenShift Service in AWS (ROSA) verwendet Dienstkontingente für Amazon EC2, Amazon Virtual Private Cloud Amazon Elastic Block Store, und Elastic Load Balancing zur Bereitstellung von Clustern. Weitere Informationen finden Sie unter Red Hat OpenShift Service in AWS Endpunkte und Kontingente im AWS Allgemeinen Referenzhandbuch.

AWS Dienste integriert mit ROSA

ROSA arbeitet mit anderen zusammen AWS-Services , um zusätzliche Lösungen für Ihre geschäftlichen Herausforderungen bereitzustellen. In diesem Thema werden Dienste beschrieben, die entweder ROSA zum Hinzufügen von Funktionen verwendet werden, oder Dienste, die zur Ausführung von Aufgaben ROSA verwendet werden.

Themen

Wie ROSA funktioniert mit AWS Marketplace

AWS Marketplace ist ein kuratierter digitaler Katalog, mit dem Sie Software, Daten und Dienste von Drittanbietern finden, kaufen, bereitstellen und verwalten können, die Sie für die Entwicklung von Lösungen und den Betrieb Ihres Unternehmens benötigen. AWS Marketplace vereinfacht die Softwarelizenzierung und -beschaffung mit flexiblen Preisoptionen und verschiedenen Bereitstellungsmethoden.

ROSA wird AWS Marketplace zur Servicemessung und Abrechnung verwendet. ROSA Classic wird über ein auf AWS Marketplace Amazon Machine Image (AMI) basierendes Produkt berechnet und abgerechnet, während ROSA mit Hosted Control Planes (HCP) über ein AWS Marketplace Software-as-a-Service (SaaS) -basiertes Produkt abgerechnet und abgerechnet wird.

Auf dieser Seite wird erklärt, wie das AWS Marketplace bei Zahlungen, Fakturierungen, Abonnements und Vertragskäufen ROSA funktioniert.

Terminologie

Auf dieser Seite werden die folgenden Begriffe verwendet, wenn es um die Integration von ROSA geht AWS Marketplace.

Amazon Machine Image (AMI)

> Ein Bild eines Servers, einschließlich eines Betriebssystems und zusätzlicher Software, auf dem AWS.

AMI-Abonnement

In AWS Marketplace AMI-basierten Softwareprodukten wie ROSA Classic wird ein stündliches Preismodell mit Jahresabonnement verwendet. Die stündliche Preisgestaltung ist das Standardpreismodell, Sie haben jedoch die Möglichkeit, die Nutzung eines Jahres für einen Amazon EC2 Instance-Typ im Voraus zu erwerben.

SaaS-Abonnement

In AWS Marketplace software-as-a-service (SaaS) -Produkten wie ROSA with HCP verwenden ein nutzungsbasiertes Abonnementmodell. Der Softwareverkäufer verfolgt Ihre Nutzung und Sie zahlen nur für das, was Sie tatsächlich nutzen.

Öffentliches Angebot

Öffentliche Angebote ermöglichen es Ihnen, AWS Marketplace Software und Dienstleistungen direkt bei der zu erwerben AWS-Managementkonsole.

Privates Angebot

Private Angebote sind ein Einkaufsprogramm, das es Verkäufern und Käufern ermöglicht, individuelle Preise und Bedingungen der Endbenutzer-Lizenzvereinbarung (EULA) für Käufe in AWS Marketplace auszuhandeln.

ROSA Servicegebühren

ROSA Gebühren, die für das OpenShift Software- und Clustermanagement durch die Red Hat Site Reliability Engineers anfallen (SREs). ROSA Die Servicegebühren sind abgerechnet AWS Marketplace und werden auf Ihrer AWS Rechnung ausgewiesen.

AWS Gebühren für die Infrastruktur

AWS Standardgebühren, die für die AWS-Services zugrunde liegenden ROSA Cluster erhoben werden Amazon EC2, einschließlich Amazon EBS, Amazon S3, und Elastic Load Balancing. Die Gebühren werden je nach Nutzung berechnet und auf Ihrer AWS Rechnung AWS-Service ausgewiesen.

ROSA Zahlungen und Abrechnung

ROSA lässt sich integrieren AWS Marketplace , um die Erfassung und Abrechnung von ROSA Servicegebühren zu ermöglichen. ROSA Die Servicegebühren decken den Zugriff auf OpenShift Software und das Clustermanagement durch RedHat Site Reliability Engineers ab (SREs). ROSA Die

Servicegebühren sind in allen unterstützten AWS Standardregionen einheitlich. Die Servicegebühren für ROSA mit HCP fallen standardmäßig bei Bedarf zu einem pauschalen Stundensatz an, der auf der Anzahl der laufenden Cluster und dem Worker Node V, die in diesen Clustern CPUs ausgeführt werden, basiert. Die klassischen ROSA-Servicegebühren fallen bei Bedarf auf der Grundlage der Anzahl der Worker Node v an. CPUs ROSA classic erhebt keine Servicegebühren für die Kontrollebene oder die erforderlichen Infrastrukturknoten.

ROSA Kunden zahlen außerdem die üblichen AWS Infrastrukturgebühren für die AWS-Services zugrunde liegenden ROSA Cluster Amazon EC2, einschließlich Amazon EBS, Amazon S3, und Elastic Load Balancing. AWS Bei den Infrastrukturgebühren handelt es sich um einen separaten Abrechnungsposten von den ROSA Servicegebühren, die über AWS Marketplace die Gebühren abgerechnet werden. AWS Die Infrastrukturgebühren variieren je nach stündlicher Nutzung AWS-Region und basieren standardmäßig auf dieser. Für zusätzliche Einsparungen bei den AWS Infrastrukturkosten können Sie Amazon EC2 Sparpläne oder Reserved Instances erwerben. Weitere Informationen finden Sie unter Compute Savings Plans and Reserved Instances im Amazon EC2 Benutzerhandbuch.

ROSA erhebt keine Gebühren, bis Sie einen ROSA Cluster erstellt oder einen ROSA Vertrag abgeschlossen haben. Weitere Informationen finden Sie unter Red Hat OpenShift Service in AWS Preise.

In der AWS Billing Konsole können Sie ROSA Service- und AWS Infrastrukturgebühren einsehen und Zahlungen verwalten. Über die AWS Cost Explorer Service Benutzeroberfläche können Sie auch kostenlos Ihre Kosten einsehen und die Nutzung überwachen. Weitere Informationen finden Sie unter Ihre Rechnung anzeigen im AWS Fakturierung und Kostenmanagement Benutzerhandbuch und Analysieren Ihrer Kosten mit AWS Cost Explorer Service im AWS Cost Management-Benutzerhandbuch.

ROSA Marketplace-Angebote über die Konsole abonnieren

Wenn Sie die Option ROSA in der ROSA Konsole aktivieren, haben Sie AWS-Konto die Angebote ROSA classic und ROSA with HCP abonniert. AWS Marketplace Für die Aktivierung ROSA von Abonnements fallen keine Gebühren an.

Für AWS Organizations Benutzer ROSA ermöglicht es Ihnen, ROSA Classic-Abonnements mit anderen Konten in Ihrer Organisation zu teilen. Weitere Informationen finden Sie im AWS Marketplace Buyer Guide unter Gemeinsame Nutzung von Abonnements in einer Organisation.

Einen ROSA Vertrag abschließen

ROSA dient AWS Marketplace zur Bereitstellung optionaler Verträge für ROSA mit HCP und ROSA classic. Verträge ermöglichen Einsparungen bei den Servicegebühren für ROSA Worker Nodes. ROSA Verträge haben keinen Einfluss auf die für die AWS Infrastruktur erhobenen Gebühren.

Verträge mit einer Laufzeit von 12 Monaten

Sie können 12-monatige öffentliche Angebotsverträge für ROSA classic und ROSA mit HCP von der Konsole aus erwerben. ROSA

> **Note**
>
> ROSA classic muss auf Ihrem Konto aktiviert sein, bevor Sie 12-Monats-Verträge über die Konsole erwerben können.

> **Note**
>
> 12-Monats-Verträge können nicht auf ein Privatangebot übertragen werden.

Kauf eines 12-Monats-Vertrags von ROSA Classic

Wenn Sie einen 12-Monats-Vertrag mit ROSA Classic erwerben, zahlen Sie eine Vorauszahlung für eine jährliche Laufzeit und zahlen für die nächsten 12 Monate keine stündliche Servicegebühr für die abgedeckten Instanzen. Die Vertragskosten richten sich nach dem Amazon EC2 Instance-Typ und der Anzahl der Instances, die Sie auswählen. Der Vertrag deckt nicht die AWS Infrastrukturgebühren ab, die für die verwendeten AWS-Services Basiswerte ROSA anfallen. Weitere Informationen finden Sie unter Red Hat OpenShift Service in AWS – Preise.

Der Vertrag deckt nur die Instance-Typen ab, die Sie bei der Vertragserstellung angeben (z. B. m5.xlarge). Sie können zusätzliche 12-Monats-Verträge erwerben, um Kosten für mehr als einen Instance-Typ zu sparen. Amazon EC2 Für die Nutzung außerhalb Ihres 12-Monats-Vertrags fallen ROSA Servicegebühren zum On-Demand-Tarif an.

> **Note**
>
> Die klassischen 12-Monats-Verträge von ROSA verlängern sich nicht auto.

Um einen 12-Monats-Vertrag für ROSA classic zu erwerben

> **Note**
>
> Wenn Sie die ROSA Konsole in einer Region verwenden, die ROSA mit HCP noch nicht unterstützt, ist dieser Workflow noch nicht verfügbar. Eine Liste der Regionen, die ROSA mit HCP unterstützen, finden Sie unter. the section called “Vergleich von ROSA mit HCP und ROSA Classic”
> Um in Regionen ohne ROSA Classic-Verträge mit HCP-Support zu erwerben, wählen Sie in der ROSA Konsole die Option Softwarevertrag kaufen und bestehende Verträge anzeigen aus.

1. Rufen Sie die ROSA -Konsole auf.
2. Wählen Sie im linken Navigationsbereich Verträge aus.
3. Wählen Sie Verträge für ROSA classic.
4. Wählen Sie Kaufvertrag.
5. Wählen Sie den EC2 Instance-Typ und die Anzahl der benötigten Instances aus.
6. Wählen Sie „Vertrag überprüfen“.
7. Überprüfen Sie die Vertragsdetails und wählen Sie Kaufvertrag aus.

> **Note**
>
> ROSA 12-Monats-Verträge können nach der Erstellung über die Konsole nicht herabgestuft oder gekündigt werden. Wenn Sie den Vertrag während der aktiven Vertragslaufzeit herabstufen oder kündigen müssen, rufen Sie das Support Center auf und öffnen Sie eine Support-Anfrage.

Kauf einer ROSA mit HCP 12-Monats-Vertrag

Wenn Sie ROSA mit HCP in der Konsole aktivieren, wird zunächst auf Ihrem Konto ein kostenloser 12-Monats-ROSA-Vertrag mit HCP erstellt, um die Abrechnung auf Abruf zu ermöglichen. Wenn Sie sich für den Kauf eines ROSA-Vertrags mit HCP entscheiden, um Servicegebühren für Worker-Nodes zu sparen, wird der ursprüngliche Vertrag so geändert, dass er die Nutzungskosten für den Worker Node V CPUs und die von Ihnen angegebenen Kontrollebenen deckt.

Wenn Sie einen 12-Monats-Vertrag mit ROSA und HCP erwerben, zahlen Sie eine Vorauszahlung für eine jährliche Laufzeit und zahlen für die nächsten 12 Monate keine stündliche Nutzungsgebühr für den betroffenen Worker Node V CPUs und die Kontrollebenen. Die Vertragskosten richten sich nach der Anzahl der ausgewählten Worker Node V CPUs - und Kontrollebenen. Der Vertrag deckt nur den Arbeitsknoten V CPUs und die Kontrollebenen ab, die Sie bei der Vertragserstellung angeben. Der Vertrag deckt nicht die AWS Infrastrukturgebühren ab, die für die verwendeten AWS-Services Basiswerte ROSA anfallen. Weitere Informationen finden Sie unter Red Hat OpenShift Service in AWS – Preise.

Monatliches Nutzungskontingent

Beim Kauf werden Ihre Prepaid-Flugzeuge V CPUs und Control in ein monatliches Nutzungskontingent umgewandelt. Stündliche On-Demand-Nutzungsgebühren gelten für die Nutzung vCPU vCPUs und Steuerungsebenen, die das monatliche Kontingent überschreiten. ROSA with HCP verwendet die folgenden Formeln, um das mit dem Vertrag verknüpfte monatliche Kontingent zu berechnen:

- Worker-Knoten vCPUs: Anzahl von v CPUs x 24 Stunden x 365 Tage/ 12 Monate
- Kontrollebenen: Anzahl der Kontrollebenen x 24 Stunden x 365 Tage/12 Monate

Ein Kauf von 4.000 Worker-Knoten-V CPUs und 8 Steuerungsebenen würde beispielsweise zu einem monatlichen Kontingent von 2.920.000 Worker-Node-vCPU-Stunden und 5.840 Stunden verbrauchbarer Kontrollebene pro Monat führen.

Um eine ROSA mit einem 12-Monats-HCP-Vertrag zu erwerben

> **Note**
>
> Wenn Sie die Red Hat OpenShift Service in AWS Konsole in einer Region verwenden, die ROSA mit gehosteten Steuerungsebenen noch nicht unterstützt, ist dieser Workflow noch nicht verfügbar. Eine Liste der Regionen, die ROSA mit HCP unterstützen, finden Sie unterthe section called “Vergleich von ROSA mit HCP und ROSA Classic”.

1. Rufen Sie die ROSA -Konsole auf.
2. Wählen Sie im linken Navigationsbereich Verträge aus.
3. Wählen Sie Verträge für ROSA mit HCP aus.

4. Wählen Sie Kaufvertrag.
5. Geben Sie die Zahl von V einCPUs , die Sie kaufen möchten. Geben Sie diese Zahl in Vielfachen von 4 an.
6. Geben Sie die Anzahl der Steuerflugzeuge ein, die Sie kaufen möchten.
7. Wählen Sie „Vertrag überprüfen“.
8. Überprüfen Sie die Vertragsdetails und wählen Sie Kaufvertrag aus.

> **Note**
>
> ROSA 12-Monats-Verträge können nach der Erstellung über die Konsole nicht herabgestuft oder gekündigt werden. Wenn Sie den Vertrag während der aktiven Vertragslaufzeit herabstufen oder kündigen müssen, rufen Sie das Support Center auf und öffnen Sie eine Support-Anfrage.

Upgrade eines ROSA-Vertrags mit HCP für 12 Monate

Sie können Ihren aktiven 12-Monats-Vertrag mit ROSA und HCP jederzeit mit zusätzlichen Worker Node V CPUs - und Kontrollebenen aufrüsten. Wenn Sie Ihren 12-Monats-Vertrag mit ROSA und HCP aufrüsten, zahlen Sie die zusätzlichen Ressourcen anteilig im Voraus. Die anteiligen Beträge werden auf der Grundlage der Anzahl der verbleibenden Tage des Vertrags berechnet. Der Vertrag deckt nur den Worker-Knoten V CPUs und die Kontrollebenen ab, die Sie bei der Vertragserstellung angeben. Vertragsupgrades wirken sich nicht auf die für die AWS Infrastruktur erhobenen Gebühren aus.

Beim Upgrade werden die hinzugefügten V CPUs - und Control-Ebenen auf ein monatliches Nutzungskontingent umgerechnet, wobei dieselben Formeln wie beim ursprünglichen Vertragskauf verwendet werden. Stündliche On-Demand-Nutzungsgebühren gelten für die Nutzung vCPU vCPUs und Steuerungsebenen, die das monatliche Kontingent überschreiten. Weitere Informationen finden Sie unter the section called “Monatliches Nutzungskontingent”.

Um ein 12-Monats-Abonnement mit ROSA und HCP zu aktualisieren

1. Rufen Sie die ROSA -Konsole auf.
2. Wählen Sie im linken Navigationsbereich Verträge aus.
3. Wählen Sie Verträge für ROSA mit HCP aus.

4. Wählen Sie Upgrade.
5. Geben Sie die Zahl der V ein, die hinzugefügt CPUs werden sollen. Geben Sie diese Zahl in Vielfachen von 4 an.
6. Geben Sie die Anzahl der Steuerflugzeuge ein, die dem Vertrag hinzugefügt werden sollen.
7. Wählen Sie Upgrade überprüfen aus.
8. Überprüfen Sie die Vertragsdetails und wählen Sie Upgrade kaufen aus.

> **Note**
>
> 12-Monats-Verträge von ROSA Classic können nicht aktualisiert werden. Zusätzliche 12-Monats-ROSA-Classic-Verträge können jederzeit über die ROSA Konsole erworben werden.

Einholen eines privaten Angebots

Sie können ein AWS Marketplace privates Angebot für ROSA mit HCP oder ROSA classic anfordern, um Produktpreise und die mit Red Hat ausgehandelten Bedingungen der Endbenutzer-Lizenzvereinbarung (EULA) zu erhalten. Weitere Informationen finden Sie unter Private Angebote im AWS Marketplace Buyer Guide.

Um ein ROSA privates Angebot zu erhalten

> **Note**
>
> Wenn Sie ein AWS Organizations Nutzer sind und ein privates Angebot erhalten haben, das auf Ihre Zahler- und Mitgliedskonten ausgestellt wurde, gehen Sie wie folgt vor, um es ROSA direkt für jedes Konto in Ihrer Organisation zu abonnieren.
> Wenn Sie ein privates Angebot von ROSA Classic erhalten, das nur für das Konto des AWS Organizations Zahlers ausgestellt wurde, müssen Sie das Abonnement mit den Mitgliedskonten in Ihrer Organisation teilen. Weitere Informationen finden Sie im AWS Marketplace Buyer Guide unter Gemeinsame Nutzung von Abonnements in einer Organisation.

1. Sobald ein privates Angebot erstellt wurde, melden Sie sich bei der AWS Marketplace Konsole an.
2. Öffnen Sie die E-Mail mit einem Link zu einem ROSA privaten Angebot.

3. Folgen Sie dem Link, um direkt auf das private Angebot zuzugreifen.

> **Note**
>
> Wenn Sie diesem Link folgen, bevor Sie sich beim richtigen Konto anmelden, wird der Fehler Page note found (404) angezeigt.

4. Lesen Sie die Nutzungsbedingungen.
5. Wählen Sie Bedingungen akzeptieren.

> **Note**
>
> Wenn ein AWS Marketplace privates Angebot nicht angenommen wird, AWS Marketplace werden die ROSA Servicegebühren von weiterhin zum öffentlichen Stundensatz in Rechnung gestellt.

6. Um die Angebotsdetails zu überprüfen, wählen Sie im Produktangebot die Option Details anzeigen aus.
7. Um mit der Verwendung zu beginnen ROSA, wählen Sie Weiter zur Konfiguration. Sie werden zur ROSA Konsole weitergeleitet.

Private Marketplace

Private Marketplace ermöglicht es Administratoren, maßgeschneiderte digitale Kataloge mit zugelassenen Produkten zu erstellen. AWS Marketplace Administratoren können einzigartige Sets von geprüfter Software erstellen, die für bestimmte AWS Organisationseinheiten oder AWS Marketplace für andere AWS-Konten innerhalb ihrer Organisation zum Kauf verfügbar sind.

Wenn Ihre Organisation eine private Marketplace-Site verwendet, muss ein Administrator die AWS Marketplace Angebote für ROSA zur privaten Marketplace-Site hinzufügen, bevor Benutzer den Service aktivieren können. Weitere Informationen finden Sie unter Erste Schritte mit einer privaten Marketplace-Site im AWS Marketplace Einkaufsführer.

Fehlerbehebung

Auf der folgenden Seite werden einige häufig auftretende Probleme bei der Erstellung oder Verwaltung von ROSA Clustern beschrieben.

Themen

Greifen Sie auf ROSA Cluster-Debug-Protokolle zu

Um mit der Behebung von Problemen mit Ihrer Anwendung zu beginnen, überprüfen Sie zunächst die Debug-Logs. Die ROSA CLI-Debug-Protokolle enthalten Details zu den Fehlermeldungen, die ausgegeben werden, wenn ein Cluster nicht erstellt werden kann.

Führen Sie den folgenden ROSA CLI-Befehl aus, um Cluster Debug-Informationen anzuzeigen. Ersetzen Sie den Befehl `<cluster_name>` durch den Namen Ihres Cluster.

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

ROSA Der Cluster schlägt bei der Cluster Erstellung die Überprüfung des AWS Dienstkontingents fehl

Für die Nutzung ROSA müssen die Dienstkontingente für Ihr Konto möglicherweise erhöht werden. Weitere Informationen finden Sie unter Red Hat OpenShift Service in AWS -Endpunkte und -Kontingente.

1. Führen Sie den folgenden Befehl aus, um die Kontingente Ihres Kontos zu ermitteln.

```
rosa verify quota
```

> **Note**
>
> Kontingente sind unterschiedlich AWS-Regionen. Stellen Sie sicher, dass Sie jedes der Kontingente für Ihre Regionen überprüfen.

2. Wenn Sie Ihr Kontingent erhöhen müssen, navigieren Sie zur Service Quotas Konsole.
3. Wählen Sie im Navigationsbereich AWS Dienste aus.
4. Wählen Sie den Dienst aus, für den eine Kontingenterhöhung erforderlich ist.
5. Wählen Sie das Kontingent aus, das erhöht werden muss, und wählen Sie Kontingenterhöhung beantragen.
6. Geben Sie unter Kontingenterhöhung beantragen den Gesamtbetrag ein, auf den sich das Kontingent belaufen soll, und wählen Sie Beantragen aus.

Fehlerbehebung bei abgelaufenen Offline-Zugriffstoken für ROSA CLI

Wenn Sie die ROSA CLI verwenden und Ihr Offline-Zugriffstoken api.openshift.com abläuft, wird eine Fehlermeldung angezeigt. Dies passiert, wenn sso.redhat.com das Token ungültig macht.

1. Navigieren Sie zur Seite OpenShift Cluster Manager API Token und wählen Sie Load Token aus.
2. Kopieren Sie den folgenden Authentifizierungsbefehl und fügen Sie ihn in das Terminal ein.

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

Fehler beim Erstellen eines Cluster mit einem osdCcsAdmin Fehler

> **Note**
>
> Dieser Fehler tritt nur auf, wenn Sie die Methode der Clusterbereitstellung ROSA verwenden, die nicht von STS stammt. Um dieses Problem zu vermeiden, stellen Sie Ihre ROSA Cluster mithilfe von bereit. AWS STS Weitere Informationen finden Sie unter the section called “Erstellen Sie einen klassischen ROSA-Cluster - CLI”.

Wenn Ihre Erstellung Cluster fehlschlägt, erhalten Sie möglicherweise die folgende Fehlermeldung:

```
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. Löschen Sie den Stack.

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

2. Initialisieren Sie Ihr Konto erneut.

   ```
   rosa init
   ```

Nächste Schritte

- Besuchen Sie die DokumentationOpenShift .
- Öffnen Sie einen Support Fall oder eine Red Hat Support-Anfrage.
- Hier finden Sie Antworten auf häufig gestellte Fragen zu Red Hat OpenShift Service in AWS.
- Weitere Informationen zum Support-Modell von ROSA finden Sie unterthe section called “Supportanfragen”.

ROSA Unterstützung erhalten

Mit ROSA können Sie Support von Support und den RedHat Support-Teams erhalten. Supportanfragen können bei beiden Organisationen eröffnet werden und werden an das richtige Team weitergeleitet, um Ihr Problem zu lösen.

Öffnen Sie einen Fall Support

Für die Eröffnung ROSA technischer Fälle ist ein AWS Developer Support Plan erforderlich. Für den kontinuierlichen Zugriff auf ROSA technischen Support und Architekturberatung wird jedoch ein AWS Business-, Enterprise- oder Enterprise On-Ramp-Support-Plan empfohlen. Red Hat verwendet die Support API, um bei Bedarf Anfragen für Kunden zu öffnen. AWS On-Ramp-Supportpläne für Unternehmen, Unternehmen und Unternehmen ermöglichen einen kontinuierlichen Telefon-, Internet- und Chat-Zugang zu Support-Technikern. Weitere Informationen zu Support Plänen finden Sie unter Support.

Schritte zur Aktivierung eines Support Plans finden Sie unter Wie melde ich mich für einen Support Plan an?

Informationen zum Erstellen eines Support Kundenfalls finden Sie unter Supportanfragen erstellen und Kundenvorgangsverwaltung.

Öffnen Sie eine Red Hat Support-Anfrage

ROSA beinhaltet Red Hat Premium Support. Um Red Hat Premium Support zu erhalten, navigieren Sie zum Red Hat Customer Portal und verwenden Sie das Support Case Tool, um ein Support-Ticket zu erstellen. Weitere Informationen finden Sie unter So nehmen Sie Kontakt mit dem Red Hat Support auf.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen an der -Dokumentation beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Aktualisiert ROSAKubeControllerPolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSAKubeControllerPolicy , um die Elastic Load Balancing Balancing-Berechtigungen für die Registrierung und Deregistrierung von Zielen bei Zielgruppen zu verdeutlichen. Weitere Informationen finden Sie unter ROSA Aktualisierungen der AWS verwalteten Richtlinien.	5. März 2026
Aktualisiert ROSANodePoolManagementPolicy	ROSA hat die verwaltete Richtlinie aktualisiertROSANodePoolManagementPolicy , um den Ressourcenzugriff für Kapazitätsreservierungen hinzuzufügen, um die Funktion „Kapazitätsreservierungen“ zu unterstützen. Weitere Informationen finden Sie unter ROSA Aktualisierungen der AWS verwalteten Richtlinien.	3. September 2025
Aktualisierte ROSAInstaller Richtlinie	Die Richtlinie für AWS verwaltete ROSAInstaller Richtlinien wurde aktualisi	7. August 2025

	ert, um die neue Funktion für Kapazitätsreservierungen in ROSA zu unterstützen und das Kubernetes-Cluster-Tag-Management zu verbessern. Weitere Informationen finden Sie unter ROSA Aktualisierungen der AWS verwalteten Richtlinien.	
Neue ROSASharedVPCRoute53 Richtlinie	ROSA hat eine neue verwaltete Richtlinie veröffentlicht `ROSASharedVPCRoute53Policy` , die es dem ROSA-Installationsprogramm ermöglicht, Route 53 53-Datensätze in gemeinsam genutzten VPC-Umgebungen zu konfigurieren. Weitere Informationen finden Sie unter ROSA Updates für AWS verwaltete Richtlinien.	7. August 2025

Neue ROSAShared VPCEndpoint Richtlinie	ROSA hat eine neue verwaltete Richtlinie veröffentlicht `ROSASharedVPCEndpointPolicy`, die es dem ROSA-Installationsprogramm ermöglicht, VPC-Endpunkte und Sicherheitsgruppen in gemeinsam genutzten VPC-Umgebungen zu konfigurieren. Diese Richtlinie bietet eine Teilmenge von EC2-Berechtigungen, die auf gemeinsame VPC-Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter ROSA Aktualisierungen der verwalteten Richtlinien. AWS	7. August 2025
Aktualisiert ROSAImageRegistryOperatorPolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSAImageRegistryOperatorPolicy.	19. Mai 2025
Aktualisiert ROSANodePoolManagementPolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSANodePoolManagementPolicy .	5. Mai 2025
Aktualisiert ROSAImageRegistryOperatorPolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSAImageRegistryOperatorPolicy.	16. April 2025
Aktualisiert ROSAWorkerInstancePolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSAWorkerInstancePolicy.	03. März 2025

Aktualisiert ROSANodePoolManagementPolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSANodePoolManagementPolicy.	24. Februar 2025
Aktualisiert ROSAAmazonEBSCSIDriverOperatorPolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSAAmazon EBSCSIDriverOperatorPolicy.	17. Januar 2025
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt im Mittleren Osten (VAE) erhältlich. AWS-Region	13. Mai 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt in Europa (Paris) erhältlich. AWS-Region	6. Mai 2024
Aktualisiert ROSANodePoolManagementPolicy	Die AWS verwaltete Richtlinie ROSANode PoolManagementPolicy wurde aktualisiert.	2. Mai 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt in Europa (Spanien) AWS-Region erhältlich.	29. April 2024
Aktualisierte ROSAInstaller Richtlinie	Die Richtlinie für AWS verwaltete ROSAInstaller Richtlinien wurde aktualisiert.	24. April 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt in Europa (Zürich) erhältlich. AWS-Region	19. April 2024

ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt im asiatisch-pazifischen Raum (Osaka) erhältlich. AWS-Regio n	17. April 2024
Aktualisierte ROSAInstaller Richtlinie und ROSASRESu pport Richtlinie	Die ROSAInstaller Richtlinie und ROSASRESupport die Richtlinie für AWS verwaltete Richtlinien wurden aktualisiert.	10. April 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt im asiatisch-pazifischen Raum (Hongkong) AWS-Region erhältlich.	8. April 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt in Südamerika (São Paulo) erhältlich. AWS-Region	1. April 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt im Nahen Osten (Bahrain) AWS-Region erhältlich.	25. März 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt im asiatisch-pazifischen Raum (Seoul) erhältlich. AWS-Regio n	14. März 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt in Afrika (Kapstadt) erhältlich. AWS-Region	5. März 2024

Aktualisierte Richtlinie ROSAInstaller	Die Richtlinie für AWS verwaltete ROSAInstaller Richtlinien wurde aktualisiert.	26. Januar 2024
Die ROSASRESupport Richtlinie wurde aktualisiert	Die Richtlinie für AWS verwaltete ROSASRESupport Richtlinien wurde aktualisiert.	22. Januar 2024
Aktualisiert ROSAImage RegistryOperatorPolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSAImage RegistryOperatorPolicy.	12. Dezember 2023
Aktualisiert ROSAKubeC ontrollerPolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSAKubeControllerPolicy.	16. Oktober 2023
Das ROSAManage Abonnement wurde aktualisiert	Das ROSAManage Abonnement für AWS verwaltete Richtlinien wurde aktualisiert.	1. August 2023
Aktualisiert ROSAKubeC ontrollerPolicy	Die AWS verwaltete Richtlinie wurde aktualisiert ROSAKubeControllerPolicy.	13. Juli 2023
ROSA-Sicherheitsseiten wurden hinzugefügt	Die Seiten Resilienz in ROSA, Infrastruktursicherheit in ROSA und Datenschutz in ROSA wurden hinzugefügt.	30. Juni 2023
Die Seite mit den Bereitste llungsoptionen wurde hinzugefügt	Die Seite mit den Bereitste llungsoptionen wurde hinzugefügt.	9. Juni 2023
Neue AWS verwaltete Richtlini e hinzugefügt ROSANode PoolManagementPolicy	Eine neue AWS verwaltet e Richtlinie ROSANode PoolManagementPolicy wurde hinzugefügt.	08. Juni 2023

Neue Richtlinie für AWS verwaltete ROSAInstaller Richtlinien hinzugefügt	Eine neue Richtlinie für AWS verwaltete ROSAInstaller Richtlinien wurde hinzugefügt.	6. Juni 2023
Neue Richtlinie für AWS verwaltete ROSASRESupport Richtlinien hinzugefügt	Eine neue Richtlinie für AWS verwaltete ROSASRESupport Richtlinien wurde hinzugefügt.	01. Juni 2023
Ein Überblick über die Zuständigkeiten von ROSA wurde hinzugefügt	Die Seite „Überblick über die Zuständigkeiten für ROSA“ wurde hinzugefügt.	26. Mai 2023
Aktualisiert Was ist Red Hat OpenShift Service in AWS?	Die Red Hat OpenShift Service in AWS Seite Was ist aktualisiert.	24. Mai 2023
Neue AWS verwaltete Richtlinien für ROSA-Operatorrollen hinzugefügt	Neue AWS verwaltete Richtlinien ROSAImage RegistryOperatorPolicy ROSAKubeControllerPolicy, und ROSAKMSProvider Richtlinien wurden hinzugefügt.	27. April 2023
Neue AWS verwaltete Richtlinie hinzugefügt ROSAControl PlaneOperatorPolicy	Eine neue AWS verwaltete Richtlinie ROSAControl PlaneOperatorPolicy wurde hinzugefügt.	24. April 2023
Neue AWS verwaltete Richtlinien für ROSA-Kontorollen hinzugefügt	Neue Seiten mit AWS verwalteten Richtlinien für das ROSA-Konto und die Seite mit Operatorrollen wurden hinzugefügt.	20. April 2023
Die Seite mit den ROSA-Dienstkontingenten wurde hinzugefügt	Die Seite mit den ROSA-Dienstkontingenten wurde hinzugefügt.	22. Dezember 2022

Es wurden Seiten zur Problembehandlung hinzugefügt	Seiten zur Fehlerbehebung wurden hinzugefügt.	1. November 2022
Seiten mit den ersten Schritten wurden hinzugefügt	Seiten mit den ersten Schritten wurden hinzugefügt.	12. August 2022
Neues ROSAManage Abonnement für AWS verwaltete Richtlinien hinzugefügt	Ein neues ROSAManag e Abonnement für AWS verwaltete Richtlinien wurde hinzugefügt.	11. April 2022
Erstversion	Die erste Version des Red Hat OpenShift Service in AWS Benutzerhandbuchs.	24. März 2021

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.