Leitfaden

Red Hat OpenShift Service in AWS

Red Hat OpenShift Service in AWS: 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 Supportmodell des Dienstes finden Sie unter Support für ROSA.

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 OpenShift APIs und Produktivitätstools für Entwickler, darunter Service Mesh, CodeReady Workspaces und Serverless.

ROSA Cluster-Bereitstellungsmodelle

ROSA bietet zwei Cluster-Bereitstellungsmodelle: ROSA mit gehosteten Steuerungsebenen (ROSA mit HCP) und ROSA Classic. Bei ROSA mit HCP verfügt jeder Cluster über eine eigene Kontrollebene, die innerhalb der von Red Hat isoliert AWS-Konto und von Red Hat verwaltet wird. Bei ROSA classic wird die Infrastruktur der Cluster-Steuerebene in der des AWS-Konto Kunden gehostet.

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. Weitere Informationen zu ROSA mit HCP und ROSA classic finden Sie unter Bereitstellungsoptionen.

> **Note**
>
> ROSA mit gehosteten Steuerungsebenen bietet derzeit keine Konformitätszertifizierungen oder Federal Information Processing Standards (FIPS) an. Weitere Informationen finden Sie unter Compliance in der Red Hat-Dokumentation.

Zugreifen ROSA

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

AWS

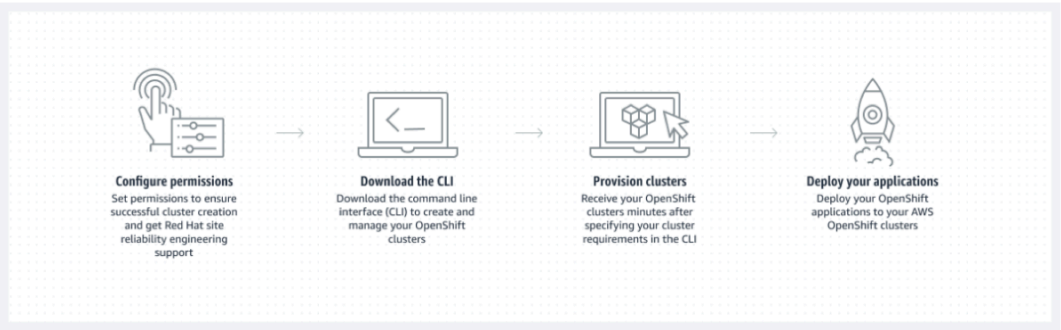
- ROSA Konsole — Stellt eine Weboberfläche zur Verfügung, über die Sie das ROSA Abonnement aktivieren und einen ROSA Softwarevertrag erwerben können.
- AWS Command Line Interface (AWS CLI) — Stellt Befehle für eine Vielzahl von Befehlen bereit AWS-Services und wird unter Windows, MacOS und Linux unterstützt. 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 unter Erste Schritte mit ROSA.

AWS Management Console/AWS CLI

1. Konfigurieren Sie Berechtigungen dafür AWS-Services ROSA , dass die Servicefunktionen bereitgestellt werden. Weitere Informationen finden Sie unter 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 Getting started with the 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 ROSA Verträge.

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.

Übersicht über die Verantwortlichkeiten für Red Hat OpenShift Service in AWS

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

Das -AWS Modell der geteilten Verantwortung definiert die AWS Verantwortung für den Schutz der Infrastruktur, die alle in der angebotenen Services ausführt AWS Cloud, einschließlich ROSAder Hardware, Software, Netzwerke und Einrichtungen, auf denen AWS - AWS Cloud Services ausgeführt werden. Diese AWS Verantwortung wird allgemein als „Sicherheit der Cloud“ bezeichnet. Um ROSA als vollständig verwalteter Service zu arbeiten, 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 kontinuierliche Verwaltung und Sicherheit der ROSA Cluster-Infrastruktur, der zugrunde liegenden Anwendungsplattform und des Betriebssystems verantwortlich. Während ROSA Cluster auf AWS Ressourcen im Kunden- gehostet werden AWS-Konten, wird auf sie remote von ROSA Servicekomponenten und Red Hat Site Reliability Engineers (SREs) über IAM Rollen zugegriffen, die der Kunde erstellt. Red Hat verwendet diesen Zugriff, um die Bereitstellung und Kapazität aller Steuerebenen- und Infrastrukturknoten im Cluster zu verwalten und Versionen für die Steuerebenenknoten, Infrastrukturknoten und Worker-Knoten zu verwalten.

Red Hat und der Kunde haben eine gemeinsame Verantwortung für ROSA Netzwerkmanagement, Clusterprotokollierung, Cluster-Versioning und Kapazitätsmanagement. Während Red Hat den ROSA Service verwaltet, ist der Kunde für die Verwaltung und Sicherung aller Anwendungen, Workloads und Daten verantwortlich, die in bereitgestellt werden ROSA.

Übersicht

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

> **Note**
>
> Wenn die `cluster-admin` Rolle einem Benutzer hinzugefügt wird, lesen Sie die Verantwortlichkeiten und Ausschlusshinweise im Red Hat Enterprise Agreement Anhang 4 (Online-Abonnementservices).

Ressource	Vorfall- und Betriebsmanagement	Änderungsmanagement	Zugriffs- und Identitätsautorisierung	Einhaltung von Sicherheits- und Vorschriften	Notfallwiederherstellung
Kundendaten	Customer	Customer	Customer	Customer	Customer
Kundenanwendungen	Customer	Customer	Customer	Customer	Customer
Entwicklerservices	Customer	Customer	Customer	Customer	Customer

Ressource	Vorfall- und Betriebsmanagement	Änderungsmanagement	Zugriffs- und Identitätsautorisierung	Einhaltung von Sicherheits- und Vorschriften	Notfallwiederherstellung
Plattformüberwachung	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Protokollierung	Red Hat	Red Hat und Kunde	Red Hat und Kunde	Red Hat und Kunde	Red Hat
Anwendungsvernetzung	Red Hat und Kunde	Red Hat und Kunde	Red Hat und Kunde	Red Hat	Red Hat
Cluster-Netzwerke	Red Hat	Red Hat und Kunde	Red Hat und Kunde	Red Hat	Red Hat
Verwaltung virtueller Netzwerke	Red Hat und Kunde	Red Hat und Kunde	Red Hat und Kunde	Red Hat und Kunde	Red Hat und Kunde
Virtuelle Datenverarbeitungsverwaltung (Steuerebene, Infrastruktur und Worker-Knoten)	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Cluster-Version	Red Hat	Red Hat und Kunde	Red Hat	Red Hat	Red Hat
Kapazitätsmanagement	Red Hat	Red Hat und Kunde	Red Hat	Red Hat	Red Hat

Ressource	Vorfall- und Betriebsmanagement	Änderungsmanagement	Zugriffs- und Identitätsautorisierung	Einhaltung von Sicherheits- und Vorschriften	Notfallwiederherstellung
Virtuelle Speicherverwaltung	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS - Software (öffentlich AWS-Services)	AWS	AWS	AWS	AWS	AWS
Hardware/ AWS globale Infrastruktur	AWS	AWS	AWS	AWS	AWS

Aufgaben für gemeinsame Verantwortlichkeiten nach Bereichen

AWS, Red Hat und Kunden haben eine gemeinsame Verantwortung für die Überwachung und Wartung von ROSA Komponenten. Diese Dokumentation definiert ROSA die Service-Verantwortlichkeiten nach Bereich und Aufgabe.

Vorfall- und Betriebsmanagement

AWS ist für den Schutz der Hardwareinfrastruktur verantwortlich, die alle in der angebotenen Services ausführt AWS Cloud. Red Hat ist für die Verwaltung der Servicekomponenten verantwortlich, die für das standardmäßige Plattformnetzwerk erforderlich sind. Der Kunde ist für die Vorfall- und Betriebsverwaltung von Kundenanwendungsdaten und für alle benutzerdefinierten Netzwerke verantwortlich, die der Kunde möglicherweise konfiguriert hat.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Anwendungsvernetzung	Red Hat	Kunde

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
	• Überwachen Sie den nativen OpenShift Router-Service und reagieren Sie auf Warnungen.	• Überwachen Sie den Zustand von Anwendung srouten und den Endpunkte n, die ihnen zugrunde liegen. • Melden Sie Ausfälle an AWS und Red Hat.
Verwaltung virtueller Netzwerke	Red Hat • Überwachen Sie AWS Load Balancer, Amazon VPC Subnetze und AWS-Service Komponenten, die für das standardmäßige Plattformnetzwerk erforderl ich sind. Reagieren Sie auf Warnungen.	Kunde • Überwachen Sie den Zustand von AWS Load Balancer-Endpunkten. • Überwachen Sie den Netzwerkverkehr, der optional über eine Amazon VPC-zu-VPC-Verbindung, eine - AWS VPN Verbindun g oder AWS Direct Connect auf potenzielle Probleme oder Sicherheitsbedrohu ngen konfiguriert ist.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Virtuelle Speicherverwaltung	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 Warnungen.	Kunde • Überwachen Sie den Zustand von Anwendung sdaten. • Wenn vom Kunden verwaltete verwendet AWS KMS keys werden, erstellen und steuern Sie den Schlüssellebenszyklus und die Schlüsselrichtlini en für die Amazon EBS Verschlüsselung.
AWS -Software (öffentlich AWS-Services)	AWS • Weitere Informationen zu AWS Vorfall- und Betriebsm anagement finden Sie unter So AWS gewährleistet die betriebliche Ausfallsicherheit und Kontinuität des Services im - AWS Whitepaper.	Kunde • Überwachen Sie den Zustand von AWS Ressourcen im Kundenkon to. • Verwenden Sie IAM Tools, um die entsprechenden Berechtigungen auf AWS Ressourcen im Kundenkon to anzuwenden.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Hardware/AWS globale Infrastruktur	AWS • Weitere Informationen zu AWS Vorfall- und Betriebsmanagement finden Sie unter So AWS gewährleistet die betriebliche Ausfallsicherheit und Kontinuität des Services im - AWS Whitepaper.	Kunde • Konfigurieren, verwalten und überwachen Sie Kundenanwendungen und -daten, um sicherzustellen, dass Anwendungs- und Datensicherheitskontrollen ordnungsgemäß durchgesetzt werden.

Änderungsmanagement

AWS ist für den Schutz der Hardwareinfrastruktur verantwortlich, die alle in der angebotenen Services ausführt AWS Cloud. Red Hat ist dafür verantwortlich, Änderungen an der Cluster-Infrastruktur und den Services zu ermöglichen, die der Kunde kontrollieren wird, sowie Versionen für die Knoten der Steuerebene, Infrastrukturknoten und Worker-Knoten zu verwalten. Der Kunde ist für die Initiierung von Infrastrukturänderungen verantwortlich. Der Kunde ist auch für die Installation und Pflege optionaler Services, Netzwerkkonfigurationen auf dem Cluster sowie für Änderungen an Kundendaten und Anwendungen verantwortlich.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Protokollierung	Red Hat • Zentrales Aggregieren und Überwachen von Plattform überwachungsprotokollen. • Stellen Sie einen Protokollierungsoperator bereit und verwalten Sie ihn, damit der Kunde einen Protokollierungs-Stack für die Standard-Anwendung	Kunde • Installieren Sie den optionalen Standard-Operator für die Anwendungsprotokollierung auf dem Cluster. • Installieren, konfigurieren und verwalten Sie alle optionalen Lösungen für die App-Protokollierung, z. B. Sidecar-Container

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
	sprotokollierung bereitstellen kann. • Stellen Sie Prüfungsprotokolle auf Kundenanfrage bereit.	oder Protokollierungsanwendungen von Drittanbietern. • Passen Sie Größe und Häufigkeit der von Kundenanwendungen erstellten Anwendungsprotokolle an, wenn sie die Stabilität des Protokollierungs-Stacks oder des Clusters beeinträchtigen. • Fordern Sie Plattform-Auditprotokolle über einen Supportfall für die Untersuchung bestimmter Vorfälle an.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Anwendungsvernetzung	Red Hat • Richten Sie öffentliche Load Balancer ein. Ermöglichen Sie bei Bedarf die Einrichtung privater Load Balancer und bis zu einem zusätzlichen Load Balancer. • Richten Sie den nativen OpenShift Router-Service ein. Geben 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-Datenverkehr. • Geben Sie dem Kunden die Möglichkeit, - `NetworkPolicy` und `EgressNetworkPolicy` (Firewall)-Objekte zu verwalten.	Kunde • Konfigurieren Sie nicht standardmäßige Pod-Netzwerkberechtigungen für Projekt- und Pod-Netzwerke, Pod-Eingang und Pod-Ausgang mithilfe von -`NetworkPolicy` Objekten. • Verwenden Sie OpenShift Cluster Manager, um einen privaten Load Balancer für Standard-Anwendungsrouten 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 Services an und konfigurieren Sie sie. • Konfigurieren Sie alle erforderlichen DNS-Weiterleitungsregeln.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Cluster-Netzwerke	Red Hat • Richten Sie Cluster-V erwaltungskomponenten wie öffentliche oder private Service-Endpunkte und die erforderliche Integration mit - Amazon VPCKompon enten ein. • Richten Sie interne Netzwerkkomponenten ein, die für die interne Cluster-Kommunikation zwischen Worker-, Infrastruktur- und Steuerebenenknoten erforderlich sind.	Kunde • Geben Sie bei Bedarf optionale nicht standardm äßige IP-Adressbereiche für Computer-CIDR, Service-CIDR und Pod-CIDR über OpenShift Cluster Manager an, wenn der Cluster bereitgestellt wird. • Fordern Sie an, dass der API-Service-Endpunkt bei der Clustererstellung oder nach der Clustererstellung über OpenShift Cluster Manager öffentlich oder privat gemacht wird.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Verwaltung virtueller Netzwerke	Red Hat • Richten Sie Amazon VPC Komponenten ein und konfigurieren Sie sie, die für die Bereitstellung des Clusters erforderlich sind, z. B. Subnetze, Load Balancer, Internet-Gateways und NAT-Gateways. • Geben Sie dem Kunden die Möglichkeit, die AWS VPN Konnektivität mit On-Premises-Ressourcen, Amazon VPCmit VPC-Konnektivität und AWS Direct Connect bei Bedarf über OpenShift Cluster Manager zu verwalten. • Kunden ermöglichen, AWS Load Balancer für die Verwendung mit Service Load Balancern zu erstellen und bereitzustellen.	Kunde • Richten Sie optionale Amazon VPC Komponent en wie Amazon VPC-zu-VPC-Verbindung, - AWS VPN Verbindung oder ein und verwalten Sie sie AWS Direct Connect. • Fordern Sie zusätzlic he Load Balancer für bestimmte Services an und konfigurieren Sie sie.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Virtuelle Datenverarbeitungsverwaltung	Red Hat • Richten Sie die ROSA Steuerebene und die Datenebene so ein und konfigurieren Sie sie, dass Amazon EC2 Instances für die Cluster-Datenverarbeitung verwendet werden. • Überwachen und verwalten Sie die Bereitstellung von Amazon EC2 Steuerebene und Infrastrukturknoten auf dem Cluster.	Kunde • Überwachen und verwalten Sie Amazon EC2 Worker-Knoten, indem Sie einen Maschinenpool mit dem OpenShift Cluster Manager oder der ROSA CLI erstellen. • Verwalten Sie Änderungen an vom Kunden bereitgestellten Anwendungen und Anwendungsdaten.
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 Neben- und Wartungsupgrades.	Kunde • Planen Sie Wartungsversions-Upgrades entweder sofort, für die Zukunft oder mit automatischen Upgrades. • Bestätigen und planen Sie Nebenversions-Upgrades. • Stellen Sie sicher, dass die Clusterversion auf einer unterstützten Nebenversion bleibt. • Testen Sie Kundenanwendungen auf Neben- und Wartungsversionen, um die Kompatibilität sicherzustellen.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Kapazitätsmanagement	Red Hat • Überwachen Sie die Verwendung der Steuerebene. Zu den Steuerebenen gehören Knoten der Steuerebene und Infrastrukturknoten. • Skalieren und ändern Sie die Größe der Knoten der Steuerebene, um die Servicequalität aufrechtzuerhalten.	Kunde • Überwachen Sie die Auslastung der Worker-Knoten und aktivieren Sie gegebenenfalls die Auto-Scaling-Funktion. • Bestimmen Sie die Skalierungsstrategie des Clusters. Weitere Informationen zu Maschinenpools finden Sie in den zusätzlichen Ressourcen. • Verwenden Sie die bereitgestellten OpenShift Cluster Manager-Steuerelemente, um bei Bedarf zusätzliche Worker-Knoten hinzuzufügen oder zu entfernen. • Reagieren Sie auf Red-Hat-Benachrichtigungen zu Cluster-Ressourcenanforderungen.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Verwaltung des virtuellen Speichers	Red Hat • Richten Sie ein und konfigurieren Sie Amazon EBS , um lokalen Knotenspeicher und persistenten Volume-Speicher für den Cluster bereitzustellen. • Richten Sie die integrierte Image-Registrierung ein und konfigurieren Sie sie für die Verwendung von Amazon S3 Bucket-Speicher. • Bereinigen Sie regelmäßig Image-Registry-Ressourcen in Amazon S3 , um Amazon S3 Nutzung und Cluster-Leistung zu optimieren.	Kunde • Konfigurieren Sie optional den Amazon EBS CSI-Treiber oder den Amazon EFS CSI-Treiber, um persistente Volumes auf dem Cluster bereitzustellen.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden

AWS -Software (öffentliche AWS Services)	AWS
	
	Datenverarbeitung
	
	• Stellen Sie den Amazon EC2 Service bereit, der für ROSA Steuerebene, Infrastruktur und Worker-Kn oten verwendet wird.
	
	Speicherung
	
	• Geben Sie Amazon EBS an, damit der ROSA Service lokalen Knotenspeicher und persistenten Volume-Speicher für den Cluster bereitstellen kann.
	
	Netzwerkfunktionen
	
	• Stellen Sie die folgenden AWS Cloud Services bereit, um die Anforderungen der ROSA virtuellen Netzwerki nfrastruktur zu erfüllen:
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• Stellen Sie die folgenden optionalen AWS-Service Integrationen für bereit ROSA:
	  • AWS VPN
		Kunde
		
		• Signieren Sie Anforderu ngen mit einer Zugriffss chlüssel-ID und einem geheimen Zugriffsschlüssel, die einem - IAM Prinzipal oder AWS STS temporären Sicherheitsanmeldeinformati onen zugeordnet sind.
		• 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	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
	• AWS Direct Connect • AWS PrivateLink • AWS Transit Gateway	
Hardware/AWS globale Infrastruktur	AWS • Informationen zu Verwaltungskontrollen für AWS Rechenzentren finden Sie unter Unsere Kontrollen auf der Seite AWS Cloud Sicherheit. • Informationen zu bewährten Methoden für das Änderungsmanagement finden Sie unter Guidance for Change Management in AWS in der - AWS Lösungsbibliothek.	Kunde • Implementieren Sie bewährte Methoden für das Änderungsmanagement für Kundenanwendungen und Daten, die auf der gehostet werden AWS Cloud.

Zugriffs- und Identitätsautorisierung

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

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Protokollierung	Red Hat • Halten Sie sich an einen auf Branchenstandards basierenden mehrstufigen	Kunde • Konfigurieren Sie OpenShift RBAC, um den Zugriff auf Projekte und damit auch

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
	internen Zugriffsprozess für Plattformprüfungsprotokolle. • Stellen Sie native OpenShift RBAC-Funktionen bereit.	die Anwendungsprotokolle eines Projekts zu steuern. • Bei Protokollierungslösungen von Drittanbietern oder benutzerdefinierten Anwendungen ist der Kunde für die Zugriffsverwaltung verantwortlich.
Anwendungsvernetzung	Red Hat • Stellen Sie native OpenShift RBAC- und -`dedicated-admin`Funktionen bereit.	Kunde • Konfigurieren Sie OpenShift `dedicated-admin` und RBAC, um den Zugriff auf die Routing-Konfiguration nach Bedarf zu steuern. • Verwalten Sie Red-Hat-Organisationsadministratoren für Red Hat, um Zugriff auf OpenShift Cluster Manager zu gewähren. Der Cluster-Manager wird verwendet , um Router-Optionen zu konfigurieren und ein Service-Load-Balancer-Kontingent bereitzustellen.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Cluster-Netzwerke	Red Hat • Stellen Sie Kundenzug riffskontrollen über OpenShift Cluster Manager bereit. Stellen Sie native OpenShift RBAC- und -`dedicated-admin`Funktionen bereit.	Kunde • Konfigurieren Sie OpenShift `dedicated-admin` und RBAC, um den Zugriff auf die Routing-Konfiguration nach Bedarf zu steuern. • Verwalten Sie die Mitglieds chaft der Red-Hat-O rganisation in Red-Hat-K onten. • Verwalten Sie Organisat ionsadministratoren für Red Hat, um Zugriff auf OpenShift Cluster Manager zu gewähren.
Verwaltung virtueller Netzwerke	Red Hat • Stellen Sie Kundenzug riffskontrollen über OpenShift Cluster Manager bereit.	Kunde • Verwalten Sie den optionale n Benutzerzugriff auf AWS Komponenten über OpenShift Cluster Manager.
Virtuelle Datenverarbeitungs verwaltung	Red Hat • Stellen Sie Kundenzug riffskontrollen über OpenShift Cluster Manager bereit.	Kunde • Verwalten Sie den optionale n Benutzerzugriff auf AWS Komponenten über OpenShift Cluster Manager. • Erstellen Sie IAM Rollen und angehängte Richtlini en, die zum Aktivieren des ROSA Servicezugriffs erforderlich sind.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Virtuelle Speicherverwaltung	Red Hat • Stellen Sie Kundenzug riffskontrollen über OpenShift Cluster Manager bereit.	Kunde • Verwalten Sie den optionale n Benutzerzugriff auf AWS Komponenten über OpenShift Cluster Manager. • Erstellen Sie IAM Rollen und angehängte Richtlini en, die zum Aktivieren des ROSA Servicezugriffs erforderlich sind.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
AWS -Software (öffentliche AWS Services)	AWS Datenverarbeitung • Stellen Sie den Amazon EC2 Service bereit, der für ROSA Steuerebene, Infrastruktur und Worker-Knoten verwendet wird. Speicherung • Geben Sie an Amazon EBS, das verwendet wird, um zu ermöglichen ROSA , lokalen Knotenspeicher und persistenten Volume-Speicher für den Cluster bereitzustellen. • Geben Sie an Amazon S3, das für die integrierte Image-Registrierung des Services verwendet wird. Netzwerkfunktionen • Stellen Sie AWS Identity and Access Management (IAM) bereit, das von Kunden verwendet wird, um den Zugriff auf ROSA Ressourcen zu steuern, die auf Kundenkonten ausgeführt werden.	Kunde • Erstellen Sie IAM Rollen und angehängte Richtlinien, die zum Aktivieren des ROSA Servicezugriffs erforderlich sind. • Verwenden Sie IAM Tools, um die entsprechenden Berechtigungen auf AWS Ressourcen im Kundenkonto anzuwenden. • Um in Ihrer ROSA gesamten AWS Organisation zu aktivieren, ist der Kunde für die Verwaltung von AWS Organizations Administratoren verantwortlich. • Um in Ihrer ROSA gesamten AWS Organisation zu aktivieren, ist der Kunde für die Verteilung der ROSA Berechtigungsgewährung mithilfe von verantwortlich AWS License Manager.

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

Einhaltung von Sicherheits- und Vorschriften

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

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Protokollierung	Red Hat • Senden Sie Cluster-Audit-Protokolle an einen Red Hat SIEM, um nach Sicherhei tsereignissen zu analysier en. Aufbewahrung von Prüfungsprotokollen für einen bestimmten Zeitraum zur Unterstützung forensisc her Analysen.	Kunde • Analysieren Sie Anwendung sprotokolle auf Sicherhei tsereignisse. • Senden Sie Anwendung sprotokolle an einen externen Endpunkt über Protokollierungs-Sidecar-Container oder Protokoll ierungsanwendungen von Drittanbietern, wenn eine längere Aufbewahrung erforderlich ist als vom Standardprotokollierungs-St ack angeboten wird.
Verwaltung virtueller Netzwerke	Red Hat	Kunde

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
	• Überwachen Sie virtuelle Netzwerkkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Verwenden Sie öffentliche AWS Tools für zusätzliche Überwachung und Schutz.	• Überwachen Sie optional konfigurierte virtuelle Netzwerkkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Konfigurieren Sie bei Bedarf alle erforderlichen Firewall-Regeln oder den Schutz des Kundenrechenzentrums.
Virtuelle Datenverarbeitungsverwaltung	Red Hat • Überwachen Sie virtuelle Datenverarbeitungskomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Verwenden Sie öffentliche AWS Tools für zusätzliche Überwachung und Schutz.	Kunde • Überwachen Sie optional konfigurierte virtuelle Netzwerkkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Konfigurieren Sie bei Bedarf alle erforderlichen Firewall-Regeln oder den Schutz des Kundenrechenzentrums.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Virtuelle Speicherverwaltung	Red Hat • Überwachen Sie virtuelle Speicherkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Verwenden Sie öffentliche AWS Tools für zusätzliche Überwachung und Schutz. • Konfigurieren Sie den ROSA Service so, dass Volume-Daten auf Steuerebene, Infrastru ktur und Worker-Knoten standardmäßig mit dem von Amazon EBS bereitges tellten AWS verwalteten KMS-Schlüssel verschlüs selt werden. • Konfigurieren Sie den ROSA Service so, dass persistente Kunden-Vo lumes, die die Standards peicherklasse verwenden , mit dem von Amazon EBS bereitgestellten AWS verwalteten KMS-Schlüssel verschlüsselt werden. • Geben Sie dem Kunden die Möglichkeit, einen vom Kunden verwalteten zum Verschlüsseln persisten ter Volumes KMS key zu verwenden.	Kunde • Stellen Sie Amazon EBS Volumes bereit. • Verwalten Sie Amazon EBS Volume-Speicher, um sicherzustellen, dass genügend Speicher für das Mounten als Volume in verfügbar ist ROSA. • Erstellen Sie den persisten ten Volume-Anspruch und generieren Sie ein persisten tes Volume über OpenShift Cluster Manager.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
	• Konfigurieren Sie die Container-Image-Registry, um Image-Registry-Dat en im Ruhezustand mit serverseitiger Verschlüs selung mit - Amazon S3 verwalteten Schlüsseln (SSE-3) zu verschlüsseln. • Geben Sie dem Kunden die Möglichkeit, eine öffentlic he oder private Amazon S3 Image-Registrierun g zu erstellen, um seine Container-Images vor unbefugtem Benutzerzugriff zu schützen.	

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
AWS -Software (öffentliche AWS Services)	AWS Datenverarbeitung • Geben Sie an Amazon EC2, das für ROSA Steuerebene, Infrastruktur und Worker-Knoten verwendet wird. Weitere Informationen finden Sie unter Infrastruktursicherheit in Amazon EC2 im Amazon EC2 -Benutzerhandbuch. Speicherung • Stellen Sie Amazon EBS, das für Volumes der ROSA Steuerebene, Infrastruktur und Worker-Knoten verwendet wird, sowie persistente Kubernetes-Volumes bereit. Weitere Informationen finden Sie unter Datenschutz in Amazon EC2 im Amazon EC2 -Benutzerhandbuch. • Stellen Sie bereit AWS KMS, das ROSA verwendet, um Volumes der Steuerebene, Infrastruktur und Worker-Knoten sowie persistente Volumes zu verschlüsseln. Weitere Informationen finden	Kunde • Stellen Sie sicher, dass bewährte Sicherheitsmethoden und das Prinzip der geringsten Berechtigung befolgt werden, um Daten auf der Amazon EC2 Instance zu schützen. Weitere Informationen finden Sie unter Infrastruktursicherheit in Amazon EC2 und Datenschutz in Amazon EC2. • Überwachen Sie optional konfigurierte virtuelle Netzwerkkomponenten auf potenzielle Probleme und Sicherheitsbedrohungen. • Konfigurieren Sie bei Bedarf alle erforderlichen Firewall-Regeln oder den Schutz des Kundenrechenzentrums. • Erstellen Sie einen optionalen kundenverwalteten KMS-Schlüssel und verschlüsseln Sie das Amazon EBS persistente Volume mit dem KMS-Schlüssel. • Überwachen Sie die Kundendaten im virtuellen Speicher auf potenzielle Probleme und Sicherheitsbedrohungen. Weitere

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
	Sie unter Amazon EBS Verschlüsselung im Amazon EC2 -Benutzerhandbuch. • Geben Sie an Amazon S3, das für die integrierte Container-Image-Registry des ROSA-Service verwendet wird. Weitere Informationen finden Sie unter Amazon S3 Sicherheit im Amazon S3 -Benutzerhandbuch. Netzwerkfunktionen • Stellen Sie Sicherheitsfunktionen und -services bereit, um den Datenschutz zu erhöhen und den Netzwerkzugriff auf die AWS globale -Infrastruktur zu kontrollieren, einschließlich in integrierte Netzwerk-Firewalls Amazon VPC, private oder dedizierte Netzwerkverbindungen und automatische Verschlüsselung des gesamten Datenverkehrs in den AWS globalen und regionalen Netzwerken zwischen AWS gesicherten Einrichtungen. Weitere Informationen finden Sie im Whitepaper Einführung in die - AWS	Informationen finden Sie unter AWS -Modell der geteilten Verantwortung.

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

Notfallwiederherstellung

Die Notfallwiederherstellung umfasst Daten- und Konfigurationssicherung, Datenreplikation und Konfiguration der Notfallwiederherstellungsumgebung sowie Failover bei Notfallereignissen.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
Verwaltung virtueller Netzwerke	Red Hat • Stellen Sie die betroffen en virtuellen Netzwerkk omponenten wieder her oder erstellen Sie sie neu, die für die Funktion 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.
Virtuelle Datenverarbeitungs verwaltung	Red Hat • Überwachen Sie den Cluster und ersetzen Sie ausgefallene Amazon EC2 Steuerebene- oder Infrastru kturknoten. • Geben Sie dem Kunden die Möglichkeit, ausgefall ene Worker-Knoten manuell oder automatisch zu ersetzen.	Kunde • Ersetzen Sie ausgefall ene Amazon EC2 Worker-Knoten, indem Sie die Konfiguration des Maschinenpools über OpenShift Cluster Manager oder die ROSA CLI bearbeiten.
Verwaltung virtueller Speicher	Red Hat • Sichern Sie für ROSA Cluster, die mit AWS IAM Benutzeranmeldeinf ormationen erstellt wurden, alle Kubernetes-Objekte im Cluster über stündliche,	Kunde • Sichern Sie Kundenanw endungen und Anwendung sdaten.

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
	tägliche und wöchentliche Volume-Snapshots.	

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

Ressource	Service-Verantwortlichkeiten	Zuständigkeiten des Kunden
	• Informationen zu Amazon VPC Funktionen, die Datenausfallsicherheit unterstützen, finden Sie unter Ausfallsicherheit in Amazon Virtual Private Cloud im Amazon VPC - Benutzerhandbuch.	
Hardware/AWS globale Infrastruktur	AWS • Stellen Sie eine AWS globale Infrastruktur bereit, mit ROSA der Steuerebene, Infrastruktur und Worker-Knoten über Availability Zones hinweg skaliert werden können. Diese Funktion ermöglicht es ROSA , das automatische Failover zwischen Zonen ohne Unterbrechung zu orchestrieren. • Weitere Informationen zu bewährten Methoden für die Notfallwiederherstellung finden Sie unter Optionen für die Notfallwiederherstellung in der Cloud im AWS Well-Architected Framework .	Kunde • Konfigurieren Sie ROSA Multi-AZ-Cluster, um die Fehlertoleranz und die Clusterverfügbarkeit zu verbessern.

Zuständigkeiten des Kunden für Daten und Anwendungen

Der Kunde ist für die Anwendungen, Workloads und Daten verantwortlich, die er in bereitstellt Red Hat OpenShift Service in AWS. AWS und Red Hat bieten jedoch verschiedene Tools, mit denen Kunden Daten und Anwendungen auf der Plattform verwalten können.

Ressource	Wie AWS und Red Hat helfen	Zuständigkeiten des Kunden
Kundendaten	Red Hat • Halten Sie die Standards auf Plattformebene für die Datenverschlüsselung gemäß den Sicherheits- und Compliance-Standards der Branche ein. • Stellen Sie OpenShift Komponenten bereit, um die Verwaltung von Anwendungsdaten zu unterstützen, z. B. Secrets. • Aktivieren Sie die Integration mit Datenservices wie Amazon RDS zum Speichern und Verwalten von Daten außerhalb des Clusters und/oder AWS. AWS • Stellen Sie bereit Amazon RDS , damit Kunden Daten außerhalb des Clusters speichern und verwalten können.	Kunde • Behalten Sie die Verantwortung für alle auf der Plattform gespeicherten Kundendaten bei und legen Sie fest, wie Kundenanwendungen diese Daten verbrauchen und preisgeben.
Kundenanwendungen	Red Hat	Kunde

Ressource	Wie AWS und Red Hat helfen	Zuständigkeiten des Kunden
	• Bereitstellen von -Clustern mit installierten OpenShift Komponenten, damit Kunden auf die OpenShift und Kubernetes-APIs zugreifen können, um containerisierte Anwendung en bereitzustellen und zu verwalten • Erstellen Sie Cluster mit Image-Pull-Secrets, damit Kundenbereitstellungen Images aus der Red Hat Container Catalog-Registrier ung abrufen können. • Gewähren Sie Zugriff auf OpenShift APIs, mit denen ein Kunde Operatoren einrichten kann, um dem Cluster Community- AWS, Drittanbieter- und Red-Hat-Services hinzuzufügen. • Stellen Sie Speicherk lassen und Plugins bereit, um persistente Volumes für die Verwendung mit Kundenanwendungen zu unterstützen. • Stellen Sie eine Container-Image-Registrierung bereit, damit Kunden Anwendung s-Container-Images sicher auf dem Cluster speichern können, um Anwendung	• Behalten Sie die Verantwor tung für Kunden- und Drittanbieteranwendungen, Daten und den gesamten Anwendungslebenszyklus bei. • Wenn ein Kunde Red Hat, eine Community, einen Drittanbieter, seinen eigenen oder andere -Services 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) zur Behebung von Problemen verantwortlich. • Verwenden Sie die bereitgestellten Tools und Funktionen, um zu konfigurieren und bereitzus tellen; bleiben Sie auf dem Laufenden; richten Sie Ressourcenanfragen und -limits ein; skalieren Sie den Cluster so, dass er über genügend Ressourcen verfügt, um Apps auszuführ en; richten Sie Berechtig ungen ein; integrieren Sie in andere -Services; verwalten

Ressource	Wie AWS und Red Hat helfen	Zuständigkeiten des Kunden
	en bereitzustellen und zu verwalten. AWS • Stellen Sie bereit Amazon EBS , um persistente Volumes für die Verwendung mit Kundenanwendungen zu unterstützen. • Stellen Sie bereit Amazon S3 , um die Bereitstellung der Container-Image-Registry durch Red Hat zu unterstützen.	Sie alle Image-Streams oder -Vorlagen, die der Kunde bereitstellt; extern bereitstellen; speichern, sichern und wiederherstellen; und verwalten Sie auf andere Weise ihre hochverfügbaren und belastbaren Workloads. • Behalten Sie die Verantwortung für die Überwachung der auf ausgeführten Anwendungen bei Red Hat OpenShift Service in AWS, einschließlich der Installation und des Betriebs von Software, um Metriken zu erfassen, Warnungen zu erstellen und Geheimnisse in der Anwendung zu schützen.

Optionen für die Bereitstellung

ROSA bietet zwei Cluster-Bereitstellungsmodelle: ROSA mit gehosteten Steuerungsebenen (ROSA mit HCP) und ROSA Classic. Bei ROSA with HCP verfügt jeder Cluster über eine eigene Kontrollebene, die innerhalb der von Red Hat isoliert AWS-Konto und von Red Hat verwaltet wird. Bei ROSA classic wird die Infrastruktur der Cluster-Steuerebene in der des AWS-Konto Kunden gehostet.

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. Beide Cluster-Bereitstellungsmodelle können in der AWS ROSA Konsole aktiviert werden. Sie haben die Wahl, welches Bereitstellungsmodell Sie verwenden möchten, wenn Sie ROSA Cluster mithilfe der ROSA CLI bereitstellen.

> **Note**
>
> ROSA mit Hosted Control Planes bietet derzeit keine Compliance-Zertifizierungen oder Federal Information Processing Standards (FIPS) an. Weitere Informationen finden Sie unter Compliance in der Red Hat-Dokumentation.

Unterschiede zwischen ROSA with HCP und ROSA Classic

Es gibt mehrere technische Unterschiede zwischen ROSA with HCP und ROSA classic.

	ROSA mit HCP	ROSA-Klassiker
Hosting der Cluster-Infrastruktur	• Komponenten der Steuerungsebene wie etcd, API-Server und OAuth werden von Red Hat gehostet und verwaltet . AWS-Konten Die Worker-Node-Infrastruktur wird auf der des Kunden gehostet. AWS-Konto Verwendet keine dedizierten Infrastrukturknoten; Plattformkomponenten werden auf Worker-Knoten bereitgestellt.	• Die Komponenten der Steuerungsebene werden zusammen mit den Infrastruktur- und Worker-Knoten auf den Komponenten des Kunden gehostet. AWS-Konto
Bereitstellungszeit	• Ungefähr 10 Minuten.	• Ungefähr 40 Minuten.
Architektur	• Die Infrastruktur der Kontrollebene wird vollständig von Red Hat verwaltet . Die Infrastruktur der Kontrollebene steht Endkunden nicht direkt zur Verfügung, außer über	• Die Infrastruktur der Steuerungsebene wird auf der des Kunden gehostet AWS-Konto. • Die Worker-Knoten werden auf den Knoten des Kunden gehostet AWS-Konto.

	ROSA mit HCP	ROSA-Klassiker
	dedizierte und explizit exponierte Endpunkte. • Die Worker-Knoten werden auf den Knoten des AWS-Konto Kunden gehostet.	
AWS Identity and Access Management	• Verwendet AWS verwaltete Richtlinien.	• Verwendet vom Kunden verwaltete Richtlinien, die vom Service definiert werden.
Minimaler Amazon EC2 Platzbedarf	• Ein Cluster erfordert mindestens zwei Knoten, die auf dem des Kunden gehostet AWS-Konto werden.	• Ein Cluster erfordert mindestens sieben Knoten, die auf dem des Kunden gehostet AWS-Konto werden.
Cluster-Bereitstellung	• Stellen Sie Cluster mithilfe der ROSA-CLI CLI. • Kunden stellen Cluster bereit, die die Komponenten der Steuerungsebene in den Systemen von Red Hat bereitstellen AWS-Konto. • Kunden stellen Maschinenpools bereit, die Worker-Knoten auf Kundenebene bereitstellen AWS-Konto.	• Stellen Sie Cluster mithilfe der ROSA-CLI oder der Weboberfläche bereit. • Die Cluster-Steuerungsebene, die Worker-Knoten und die Infrastrukturknoten werden auf AWS-Konto Kundenebene bereitgestellt.
Upgrades	• Aktualisieren Sie die Steuerungsebene und die Maschinenpools separat.	• Der gesamte Cluster muss gleichzeitig aktualisiert werden.

	ROSA mit HCP	ROSA-Klassiker
AWS-Regionen	• Informationen zur AWS-Region Verfügbarkeit finden Sie unter Red Hat OpenShift Service in AWS Endpunkte und Kontingente im AWS Allgemeinen Referenzhandbuch.	• Informationen zur AWS-Region Verfügbarkeit finden Sie unter Red Hat OpenShift Service in AWS Endpunkte und Kontingente im AWS Allgemeinen Referenzhandbuch.
-Compliance	• Informationen zur Einhaltung von Vorschriften finden Sie unter Compliance in der Red Hat-Dokumentation.	• Informationen zur Einhaltung von Vorschriften finden Sie unter Compliance in der Red Hat-Dokumentation.

Erste Schritte 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

ROSA Cluster-Bereitstellungsmodelle

ROSA unterstützt zwei Cluster-Bereitstellungsmodelle: ROSA mit gehosteten Steuerungsebenen (ROSA mit HCP) und ROSA Classic. ROSA mit HCP bietet eine effizientere Architektur der Steuerungsebene, die die AWS Infrastrukturkosten senkt ROSA und schnellere Clustererstellungszeiten ermöglicht. Weitere Informationen zu ROSA mit HCP und ROSA classic finden Sie unter Bereitstellungsoptionen.

> **Note**
>
> ROSA mit gehosteten Steuerungsebenen bietet derzeit kein FIPS an.

Anleitungen für die ersten Schritte

Für die Bereitstellung einer Anwendung in einem neu erstellten ROSA Cluster stehen vier Anleitungen für die ersten Schritte zur Verfügung. Jedes Tutorial behandelt Folgendes:

- Den ROSA Dienst aktivieren und die AWS Voraussetzungen konfigurieren
- Erstellung der erforderlichen IAM Rollen und Richtlinien
- Den ROSA Cluster erstellen
- Einen Clusteradministrator für schnellen Clusterzugriff erstellen
- Konfiguration eines Identitätsanbieters
- Benutzerzugriff auf den Cluster gewähren
- Stellen Sie eine Anwendung im Cluster bereit
- Löschen des Clusters und der Clusterressourcen

Erste Schritte mit ROSA mit HCP

Mit ROSA with HCP können Sie AWS STS und die ROSA CLI verwenden, um einen Cluster mit den erforderlichen IAM Rollen und Richtlinien zu erstellen. Weitere Informationen zu IAM Richtlinien für ROSA mit HCP finden Sie unter AWS Verwaltete IAM Richtlinien für. ROSA

Sobald der Cluster erstellt ist, können Sie mithilfe der Red Hat Hybrid Cloud Console oder der OpenShift CLI Workloads für öffentliche Anwendungen auf dem Cluster bereitstellen. Schritte zum Bereitstellen einer Anwendung auf einem neu erstellten ROSA mit HCP-Cluster finden Sie unter Erste Schritte mit ROSA mit HCP mithilfe der ROSA CLI im auto Modus.

Erste Schritte mit ROSA classic

Mit ROSA classic können Sie AWS STS und die ROSA CLI verwenden, um einen Cluster mit den erforderlichen IAM Rollen und Richtlinien zu erstellen. Sobald der Cluster erstellt ist, können Sie mithilfe der Red Hat Hybrid Cloud Console oder der OpenShift CLI Workloads für öffentliche Anwendungen auf dem Cluster bereitstellen. Schritte zu den ersten Schritten mit dem automatischen Clustererstellungsmodus (`auto`) der ROSA-CLI finden Sie unter Erste Schritte mit ROSA classic unter Verwendung der ROSA CLI im auto Modus. Schritte zu den ersten Schritten mit dem manuellen Clustererstellungsmodus (`manual`) der ROSA-CLI finden Sie unter Erste Schritte mit ROSA classic unter Verwendung der ROSA CLI im manuellen Modus.

Wenn Sie möchten, dass der ROSA Classic-Cluster und die Anwendungs-Workloads privat sind, finden Sie weitere Informationen unter Erste Schritte mit der Verwendung von AWS PrivateLink ROSA classic.

Erste Schritte mit ROSA mit HCP mithilfe der ROSA CLI im auto Modus

In den folgenden Abschnitten werden die ersten Schritte mit ROSA mit gehosteten Steuerungsebenen (ROSA mit HCP) AWS STS und der ROSA CLI beschrieben. Weitere Informationen zu ROSA mit HCP finden Sie unter Bereitstellungsoptionen.

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 Erste Schritte mit. ROSA

Themen

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Aktionen abgeschlossen haben:

- Installieren und konfigurieren Sie die neueste VersionAWS 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.
- Service Quotasmuss über die erforderlichen Dienstkontingente fürAmazon EC2,, Amazon VPCAmazon EBS, verfügen, Elastic Load Balancing die für die Erstellung und Ausführung eines ROSA Clusters erforderlich sind. AWSoder Red Hat kann in Ihrem Namen eine Erhöhung der Servicekontingenten beantragen, sofern dies zur Problemlösung erforderlich ist. Die erforderlichen Kontingente finden Sie unter Red Hat OpenShift Service in AWSEndpunkte und Kontingente in der AWSAllgemeinen Referenz.

- Um AWS Support für zu erhaltenROSA, 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 Support für ROSA. Informationen zur Aktivierung AWS Support finden Sie AWS Supportauf 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 finden Sie in der ROSASCP-Dokumentation zur Fehlerbehebung. Weitere Informationen zu SCPs finden Sie unter Service Control Policies (SCPs).
- Wenn Sie ein ROSA Cluster With-Token AWS STS in einem aktivierten System 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 Verwaltung AWS-Regionen in der allgemeinen AWS-Referenz.

Schritt 1: Voraussetzungen aktivieren ROSA und konfigurieren

Um einen zu erstellen ROSACluster, müssen Sie zuerst 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 Get started (Erste Schritte) aus.
3. Wählen Sie auf der Seite ROSAVoraussetzungen 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.

Schritt 2: Erstellen Sie eine Amazon VPC Architektur für ROSA mit HCP-Clustern

Um eine ROSA mit HCP zu erstellenCluster, müssen Sie zunächst Ihre eigene Amazon VPC Architektur für die Implementierung Ihrer Lösung konfigurieren. 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 Single-AZ-Cluster wird nur Availability Zone verwendet. Für Multi-AZ-Cluster sind drei Availability Zones erforderlich.

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

Im folgenden Verfahren werden sowohl ein öffentliches als auch ein privates Subnetz AWS CLI zu einer einzigen Availability Zone für einen Single-AZ-Cluster erstellt. Alle Cluster Ressourcen befinden sich im privaten Subnetz. Das öffentliche Subnetz leitet ausgehenden Datenverkehr mithilfe eines NAT-Gateways ins Internet weiter.

In diesem Beispiel wird der CIDR-Block `10.0.0.0/16` für die verwendet. Amazon VPC Sie können jedoch einen anderen CIDR-Block wählen. Weitere Informationen finden Sie unter Dimensionierung der VPC.

1. Legen Sie eine Umgebungsvariable für den Cluster Namen fest, indem Sie den folgenden Befehl ausführen.

   ```
   ROSA_CLUSTER_NAME=rosa-hcp
   ```

2. 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 ID der neuen VPC zurück. Im Folgenden finden Sie eine Beispielausgabe.

   ```
   vpc-0410832ee325aafea
   ```

3. Verwenden Sie die VPC-ID aus dem vorherigen Schritt und kennzeichnen Sie die VPC mit der `ROSA_CLUSTER_NAME` Variablen.

```
aws ec2 create-tags --resources <VPC_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

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

```
aws ec2 modify-vpc-attribute --vpc-id <VPC_ID_VALUE> --enable-dns-hostnames
```

5. Erstellen Sie ein öffentliches Subnetz in der VPC mit einem `10.0.1.0/24` CIDR-Block und geben Sie die Availability Zone an, in der die Ressource erstellt werden soll.

> **Important**
>
> Achten Sie beim Erstellen von Subnetzen darauf, dass Subnetze für eine Availability Zone erstellt werden, in der Instanztypen verfügbar sind. ROSA Wenn Sie keine bestimmte Availability Zone auswählen, wird das Subnetz in einer der Availability Zones in der von Ihnen angegebenen Availability Zone erstellt. AWS-Region
> Verwenden Sie das `--availability zone` Argument im `create-subnet` Befehl, um eine bestimmte Availability Zone anzugeben. Sie können den `rosa list instance-types` Befehl verwenden, um alle verfügbaren ROSA Instance-Typen aufzulisten. Verwenden Sie den folgenden 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>"
> ```

> **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 Single-AZ-Cluster ist nur eine Availability Zone erforderlich. Für Multi-AZ-Cluster sind drei Availability Zones erforderlich. Wenn diese Anforderungen nicht erfüllt sind, schlägt die Clustererstellung fehl.

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.1.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

Der vorherige Befehl gibt die ID des neuen Subnetzes zurück. Im Folgenden finden Sie eine Beispielausgabe.

```
subnet-0b6a7e8cbc8b75920
```

6. Verwenden Sie die Subnetz-ID aus dem vorherigen Schritt und kennzeichnen Sie das Subnetz mithilfe der Variablen. `ROSA_CLUSTER_NAME-public`

```
aws ec2 create-tags --resources <PUBLIC_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-public
```

7. Erstellen Sie ein privates Subnetz in der VPC mit einem `10.0.0.0/24` CIDR-Block und geben Sie dabei dieselbe Availability Zone an, in der das öffentliche Subnetz bereitgestellt wurde.

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.0.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

Der vorherige Befehl gibt die ID des neuen Subnetzes zurück. Im Folgenden finden Sie eine Beispielausgabe.

```
subnet-0b6a7e8cbc8b75920
```

8. Verwenden Sie die Subnetz-ID aus dem vorherigen Schritt und kennzeichnen Sie das Subnetz mithilfe der Variablen. `ROSA_CLUSTER_NAME-private`

```
aws ec2 create-tags --resources <PRIVATE_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

9. Erstellen Sie ein Internet-Gateway für ausgehenden Datenverkehr und hängen Sie es an die VPC an.

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output
 text
```

```
aws ec2 attach-internet-gateway --vpc-id <VPC_ID_VALUE> --internet-gateway-id
 <IG_ID_VALUE>
```

10. Kennzeichnen Sie das Internet-Gateway mit der ROSA_CLUSTER_NAME Variablen.

```
aws ec2 create-tags --resources <IG_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

11. Erstellen Sie eine Routing-Tabelle für ausgehenden Verkehr, ordnen Sie sie dem öffentlichen Subnetz zu und konfigurieren Sie den Verkehr so, dass er zum Internet-Gateway weitergeleitet wird.

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PUBLIC_SUBNET_ID> --route-table-id
 <PUBLIC_RT_ID>

aws ec2 create-route --route-table-id <PUBLIC_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <IG_ID_VALUE>
```

12. Kennzeichnen Sie die öffentliche Routing-Tabelle mit der ROSA_CLUSTER_NAME Variablen und stellen Sie sicher, dass die Routing-Tabelle ordnungsgemäß konfiguriert wurde.

```
aws ec2 create-tags --resources <PUBLIC_RT_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME

aws ec2 describe-route-tables --route-table-id <PUBLIC_RT_ID>
```

13. Erstellen Sie ein NAT-Gateway im öffentlichen Subnetz mit einer elastischen IP-Adresse, um den Verkehr zum privaten Subnetz zu ermöglichen.

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text

aws ec2 create-nat-gateway --subnet-id <PUBLIC_SUBNET_ID> --allocation-id
 <EIP_ADDRESS>  --query NatGateway.NatGatewayId --output text
```

14. Kennzeichnen Sie das NAT-Gateway und die elastische IP-Adresse mit der $ROSA_CLUSTER_NAME Variablen.

```
aws ec2 create-tags --resources <EIP_ADDRESS>  --resources <NAT_GATEWAY_ID> --tags
 Key=Name,Value=$ROSA_CLUSTER_NAME
```

15 Erstellen Sie eine Routing-Tabelle für privaten Subnetzverkehr, ordnen Sie sie dem privaten Subnetz zu und konfigurieren Sie den Datenverkehr so, dass er zum NAT-Gateway weitergeleitet wird.

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PRIVATE_SUBNET_ID> --route-table-id
 <PRIVATE_RT_ID>

aws ec2 create-route --route-table-id <PRIVATE_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <NAT_GATEWAY_ID>
```

16 Kennzeichnen Sie die private Routentabelle und die elastische IP-Adresse mit der `$ROSA_CLUSTER_NAME-private` Variablen.

```
aws ec2 create-tags --resources <PRIVATE_RT_ID> <EIP_ADDRESS> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

Schritt 3: 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 Verwaltete Richtlinien für. AWSIAMROSA

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.

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

   Der force-policy-creation Parameter -- aktualisiert alle vorhandenen Rollen und Richtlinien. Wenn keine Rollen und Richtlinien vorhanden sind, erstellt der Befehl stattdessen diese Ressourcen.

> **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 unter Problembehandlung 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
```

Schritt 4: Erstellen Sie eine ROSA mit HCP-Cluster mit AWS STS und dem ROSA CLI-Modus **`auto`**

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 erstellenCluster, geben Sie `multi-az` im Befehl und die privaten 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 die öffentlichen und privaten Subnetz-IDs an.

     ```
     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 die privaten Subnetz-IDs an.

     ```
     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 unter Problembehandlung bei der ROSA Clustererstellung.
> Wenn Sie sich an den Red Hat Support wenden AWS Support möchten, um Unterstützung zu erhalten, siehe Support für ROSA.

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

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

Schritt 5: Konfigurieren Sie einen Identitätsanbieter und gewähren Cluster Sie Zugriff

ROSAbeinhaltet einen integrierten OAuth-Server. Nach der Erstellung müssen Sie OAuth für die Verwendung eines Identitätsanbieters konfigurieren. Cluster 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 ROSACluster. 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 Identitätsbereitstellung verwenden könnenCluster, 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 <GITHUB_ORG_NAME> 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 auf der GitHub OAuth-Seite, um die verbleibenden `rosa create idp` interaktiven Eingabeaufforderungen zu füllen, indem Sie den folgenden Befehl ausführen. Ersetzen Sie <GITHUB_CLIENT_ID> und <GITHUB_CLIENT_SECRET> durch die Anmeldeinformationen aus Ihrer OAuth-Anwendung. GitHub

```
...
? 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 Identitätsanbieter-Konfiguration aktiv wird. Wenn Sie einen `cluster-admin` Benutzer konfiguriert haben, können Sie das Programm 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>
```

Schritt 6: 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.

Schritt 7: Erteilen Sie einem Benutzer Administratorrechte

Nachdem Sie Ihrem konfigurierten Identitätsanbieter einen Benutzer hinzugefügt haben, können Sie dem Benutzer `cluster-admin` oder `dedicated-admin` Berechtigungen für Ihren gewährenCluster.

`cluster-admin`Berechtigungen konfigurieren

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>
```

`dedicated-admin`Berechtigungen konfigurieren

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>
```

Schritt 8: 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 mit dem folgenden Cluster Befehl die Konsolen-URL für Sie ab. Ersetzen Sie `<CLUSTER_NAME>` 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.

Schritt 9: 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-Image-Anwendung 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.

Schritt 10: Löschen Sie einen Cluster und AWS STS Ressourcen

Sie können die ROSA CLI verwenden, um eine zu löschenCluster, 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 löschenROSA, können Sie die IAM Konsole verwenden.

> **Important**
>
> IAMRollen 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 IhresCluster.

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

> **Important**
>
> Sie müssen wartenCluster, 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

Erste Schritte mit ROSA classic mithilfe der ROSA CLI im auto Modus

In den folgenden Abschnitten wird beschrieben, wie Sie mit der Verwendung von ROSA classic AWS STS und der ROSA CLI beginnen. Weitere Informationen zu ROSA classic finden Sie unter Bereitstellungsoptionen.

Die ROSA CLI verwendet `auto` Modus oder `manual` Modus, um die IAM Ressourcen zu erstellen, die für die Bereitstellung von a erforderlich sind ROSACluster. `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.

Die Verfahren in diesem Dokument verwenden den `auto` Modus der ROSA CLI, um die erforderlichen IAM Ressourcen für ROSA classic zu erstellen. Weitere Optionen für den Einstieg finden Sie unter Erste Schritte mit ROSA.

Themen

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Aktionen abgeschlossen haben:

- Installieren und konfigurieren Sie die neueste VersionAWS 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.
- Service Quotasmuss über die erforderlichen Dienstkontingente fürAmazon EC2,, Amazon VPCAmazon EBS, verfügen, Elastic Load Balancing die für die Erstellung und Ausführung eines ROSA Clusters erforderlich sind. AWSoder Red Hat kann in Ihrem Namen eine Erhöhung der Servicekontingenten beantragen, sofern dies zur Problemlösung erforderlich ist. Die erforderlichen

Kontingente finden Sie unter Red Hat OpenShift Service in AWSEndpunkte und Kontingente in der AWSAllgemeinen Referenz.

- Um AWS Support für zu erhaltenROSA, 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 Support für ROSA. Informationen zur Aktivierung AWS Support finden Sie AWS Supportauf 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 finden Sie in der ROSASCP-Dokumentation zur Fehlerbehebung. Weitere Informationen zu SCPs finden Sie unter Service Control Policies (SCPs).
- Wenn Sie ein ROSA Cluster With-Token AWS STS in einem aktivierten System 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 Verwaltung AWS-Regionen in der allgemeinen AWS-Referenz.

Schritt 1: Voraussetzungen aktivieren ROSA und konfigurieren

Um einen zu erstellen ROSACluster, müssen Sie zuerst den ROSA Dienst in der AWS ROSA Konsole aktivieren und überprüfen, ob die AWS Voraussetzungen erfüllt sind. Die AWS ROSA Konsole überprüft, ob Sie AWS-Konto über die erforderlichen AWS Marketplace Berechtigungen und Dienstkontingente verfügen und ob Sie über die angegebene Elastic Load Balancing (ELB-) dienstbezogene 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 Get started (Erste Schritte) aus.
3. Wählen Sie auf der Seite ROSAVoraussetzungen überprüfen die Option Ich stimme zu, meine Kontaktinformationen an Red Hat weiterzugeben.
4. Wählen Sie Aktivieren ROSA.

5. Sobald auf der Seite bestätigt wurde, dass Ihre Servicekontingenten die ROSA Voraussetzungen erfüllen, und die mit dem ELB Service verknüpfte Rolle erstellt wurde, öffnen Sie eine neue Terminalsitzung, um Ihre erste ROSA Classic Cluster mithilfe der ROSA CLI zu erstellen.

Schritt 2: Erstellen Sie einen klassischen ROSA-Cluster mit AWS STS und dem ROSA`auto` CLI-Modus

Sie können einen ROSA-Klassiker Cluster mit AWS Security Token Service (AWS STS) und dem in der ROSA CLI bereitgestellten `auto` Modus erstellen.

1. Erstellen Sie die erforderlichen IAM Kontorollen und Richtlinien.

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

> **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 unter Problembehandlung bei abgelaufenen Offline-Zugriffstoken für ROSA CLI.

2. Erstellen Sie eine Cluster AWS STS mit den Standardeinstellungen im ROSA `auto` CLI-Modus. Wenn Sie die Standardeinstellungen verwenden, wird die neueste stabile OpenShift Version installiert.

```
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.

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 unter Problembehandlung bei der ROSA Cluster-Bereitstellung.
> Wenn Sie sich an den Red Hat Support wenden AWS Support möchten, um Unterstützung zu erhalten, siehe Support für ROSA.

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

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

Schritt 3: Konfigurieren Sie einen Identitätsanbieter und gewähren Cluster Sie Zugriff

ROSAbeinhaltet einen integrierten OAuth-Server. Nach der Erstellung müssen Sie OAuth für die Verwendung eines Identitätsanbieters konfigurieren. Cluster 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 ROSACluster. 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 könnenCluster, 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 `<GITHUB_ORG_NAME>` 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 auf der GitHub OAuth-Seite, um die verbleibenden `rosa create idp` interaktiven Eingabeaufforderungen zu füllen, indem Sie den folgenden Befehl ausführen. Ersetzen Sie `<GITHUB_CLIENT_ID>` und `<GITHUB_CLIENT_SECRET>` durch die Anmeldeinformationen aus Ihrer OAuth-Anwendung. GitHub

```
...
? 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 Identitätsanbieter-Konfiguration aktiv wird. Wenn Sie einen `cluster-admin` Benutzer konfiguriert haben, können Sie das Programm 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>
```

Schritt 4: 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.

Schritt 5: Erteilen Sie einem Benutzer Administratorrechte

Nachdem Sie Ihrem konfigurierten Identitätsanbieter einen Benutzer hinzugefügt haben, können Sie dem Benutzer `cluster-admin` oder `dedicated-admin` Berechtigungen für Ihren Benutzer gewährenCluster.

`cluster-admin`Berechtigungen konfigurieren

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>
```

`dedicated-admin`Berechtigungen konfigurieren

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. Vergewissern Sie sich, dass der Benutzer als Mitglied der `cluster-admins` Gruppe aufgeführt ist.

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

Schritt 6: Greifen Sie Cluster über die Webkonsole 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. Ersetzen Sie <CLUSTER_NAME> 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 habenCluster, wählen Sie den Namen des Identitätsanbieters im Dialogfeld Anmelden mit... und füllen Sie alle Autorisierungsanfragen Ihres Anbieters aus.

Schritt 7: 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 anschließend „Anwendung erstellen“, um die Seite „Source-to-Image-Anwendung 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.

Schritt 8: Widerrufen Sie Administratorrechte und Benutzerzugriff

Mit der ROSA CLI können Sie einem Benutzer `dedicated-admin` Berechtigungen `cluster-admin` entziehen.

Um einem Benutzer den Zugriff zu entziehen, müssen Sie den Benutzer von Ihrem konfigurierten Identitätsanbieter entfernen.

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 konfigurierenCluster. 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.

Schritt 9: Löschen Sie einen Cluster und AWS STS Ressourcen

Sie können die ROSA CLI verwenden, um eine zu löschenCluster, 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 löschenROSA, können Sie die IAM Konsole verwenden.

> **Important**
>
> IAMRollen 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 IhresCluster.

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

> **Important**
>
> Sie müssen wartenCluster, 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

Erste Schritte mit ROSA classic mithilfe der ROSA CLI im manuellen Modus

In den folgenden Abschnitten wird beschrieben, wie Sie mit der Verwendung von ROSA classic AWS STS und der ROSA CLI beginnen. Weitere Informationen zu ROSA classic finden Sie unter Bereitstellungsoptionen.

Die ROSA CLI verwendet `auto` Modus oder `manual` Modus, um die IAM Ressourcen zu erstellen, die für die Bereitstellung von a erforderlich sind ROSACluster. `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. Sie können die Befehle auch an einen anderen Administrator oder eine andere Gruppe in Ihrer Organisation weiterleiten, sodass diese die Ressourcen erstellen können. `manual`

Die Verfahren in diesem Dokument verwenden den `manual` Modus der ROSA CLI, um die erforderlichen IAM Ressourcen für ROSA classic zu erstellen. Weitere Optionen für den Einstieg finden Sie unter Erste Schritte mit ROSA.

Themen

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Aktionen abgeschlossen haben:

- Installieren und konfigurieren Sie die neueste VersionAWS 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.
- Service Quotasmuss über die erforderlichen Dienstkontingente fürAmazon EC2,, Amazon VPCAmazon EBS, verfügen, Elastic Load Balancing die für die Erstellung und Ausführung eines ROSA Clusters erforderlich sind. AWSoder Red Hat kann in Ihrem Namen eine Erhöhung der Servicekontingenten beantragen, sofern dies zur Problemlösung erforderlich ist. Die erforderlichen Kontingente finden Sie unter Red Hat OpenShift Service in AWSEndpunkte und Kontingente in der AWSAllgemeinen Referenz.
- Um AWS Support für zu erhaltenROSA, 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 Support für ROSA. Informationen zur Aktivierung AWS Support finden Sie AWS Supportauf 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 finden Sie in der ROSASCP-Dokumentation zur Fehlerbehebung. Weitere Informationen zu SCPs finden Sie unter Service Control Policies (SCPs).
- Wenn Sie ein ROSA Cluster With-Token AWS STS in einem aktivierten System 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 Verwaltung AWS-Regionen in der allgemeinen AWS-Referenz.

Schritt 1: Voraussetzungen aktivieren ROSA und konfigurieren

Um einen zu erstellen ROSACluster, müssen Sie zuerst 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 Get started (Erste Schritte) aus.
3. Wählen Sie auf der Seite ROSAVoraussetzungen 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.

Schritt 2: Erstellen Sie einen klassischen ROSA-Cluster mit AWS STS und dem ROSA`manual` CLI-Modus

Sie können einen ROSA-Klassiker Cluster mit AWS Security Token Service (AWS STS) und dem in der ROSA CLI bereitgestellten `manual` Modus erstellen.

Wenn Sie eine erstellenCluster, können Sie ausführen, `rosa create cluster --interactive` um Ihre Bereitstellung mit einer Reihe interaktiver Eingabeaufforderungen anzupassen. Weitere Informationen finden Sie in der Referenz zum interaktiven Clustererstellungsmodus in der Red Hat-Dokumentation.

Nach der Bereitstellung Cluster wird ein einziger Befehl in der Ausgabe bereitgestellt. Führen Sie diesen Befehl aus, um weitere Cluster bereitzustellen, die genau dieselbe benutzerdefinierte Konfiguration verwenden.

> **Note**
>
> AWSGemeinsam genutzte VPCs werden derzeit nicht für ROSA Installationen unterstützt.

1. Erstellen Sie die erforderlichen IAM Kontorollen und Richtlinien.

```
rosa create account-roles --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 unter Problembehandlung bei abgelaufenen Offline-Zugriffstoken für ROSA CLI.

2. Führen Sie die in der Ausgabe generierten AWS CLI Befehle aus, um die Rollen und Richtlinien zu erstellen.
3. Erstellen Sie Cluster einen AWS STS `--interactive` With-In-Modus, um benutzerdefinierte Einstellungen anzugeben.

```
rosa create cluster --interactive --sts
```

> **Important**
>
> Nachdem Sie die etcd-Verschlüsselung für die Schlüsselwerte in etcd aktiviert haben, entsteht ein Leistungsaufwand von etwa 20%. Der Mehraufwand ist darauf zurückzuführen, dass zusätzlich zur Standardverschlüsselung, die die etcd-Volumes verschlüsselt, diese zweite Amazon EBS Verschlüsselungsebene eingeführt wird.

4. Um die clusterspezifischen IAM Operatorrollen zu erstellen, generieren Sie die JSON-Dateien mit den Operatorrichtlinien im aktuellen Arbeitsverzeichnis und geben Sie die Befehle zur AWS CLI Überprüfung aus.

```
rosa create operator-roles --mode manual --cluster <CLUSTER_NAME|CLUSTER_ID>
```

5. Führen Sie die AWS CLI Befehle von der Ausgabe aus.
6. Erstellen Sie den OpenID Connect (OIDC) -Anbieter, den die Cluster Betreiber zur Authentifizierung verwenden.

```
rosa create oidc-provider --mode auto --cluster <CLUSTER_NAME|CLUSTER_ID>
```

7. Überprüfen Sie den Status Ihres. Cluster

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

> **Note**
>
> Wenn der Erstellungsvorgang fehlschlägt oder das `State` Feld nach 40 Minuten nicht den Status „Bereit“ annimmt, finden Sie weitere Informationen unter Problembehandlung bei der ROSA Clustererstellung.
> Wenn Sie sich an den Red Hat Support wenden AWS Support möchten, um Unterstützung zu erhalten, siehe Support für ROSA.

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

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

Schritt 3: Konfigurieren Sie einen Identitätsanbieter und gewähren Cluster Sie Zugriff

ROSAbeinhaltet einen integrierten OAuth-Server. Nach der Erstellung müssen Sie OAuth für die Verwendung eines Identitätsanbieters konfigurieren. Cluster 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 konfigurierenCluster. 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 Identitätsbereitstellung verwenden können ROSACluster, 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 mit dem folgenden Befehl. `<GITHUB_ORG_NAME>`Ersetzen Sie es 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 auf der GitHub OAuth-Seite, um die verbleibenden `rosa create idp` interaktiven Eingabeaufforderungen mit dem folgenden Befehl auszufüllen. Ersetzen

Sie <GITHUB_CLIENT_ID> und <GITHUB_CLIENT_SECRET> durch die Anmeldeinformationen aus Ihrer OAuth-Anwendung. GitHub

```
...
? 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 Identitätsanbieter-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 mithilfe des folgenden Befehls sicher, dass der Identitätsanbieter korrekt konfiguriert wurde.

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

Schritt 4: Gewähren Sie dem Benutzer Zugriff auf eine Cluster

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

Mit dem folgenden Verfahren wird ein Benutzer zu einer GitHub Organisation hinzugefügt, die für die Identitätsbereitstellung konfiguriert ist. Cluster

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 Dokumentation auf Github unter Benutzer einladen, Ihrer Organisation beizutreten.

Schritt 5: Erteilen Sie einem Benutzer Administratorrechte

Nachdem Sie Ihrem konfigurierten Identitätsanbieter einen Benutzer hinzugefügt haben, können Sie dem Benutzer `cluster-admin` oder `dedicated-admin` Berechtigungen für Ihren gewährenCluster.

`cluster-admin`Berechtigungen konfigurieren

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>
```

`dedicated-admin`Berechtigungen konfigurieren

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>
```

Schritt 6: Greifen Sie Cluster über die Webkonsole 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 mit Cluster dem folgenden Befehl ab. Ersetzen Sie <CLUSTER_NAME> 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 erstellen, melden Sie sich mit den angegebenen Anmeldeinformationen an.
   - Wenn Sie einen Identitätsanbieter für Ihren konfigurierenCluster, wählen Sie den Namen des Identitätsanbieters im Dialogfeld Anmelden mit... und füllen Sie alle Autorisierungsanfragen aus, die von Ihrem Anbieter gestellt werden.

Schritt 7: 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 anschließend „Anwendung erstellen“, um die Seite „Source-to-Image-Anwendung 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.

    Eine neue Registerkarte im Browser wird mit einer Meldung ähnlich der folgenden geöffnet.

```
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.

Schritt 8: Widerrufen Sie Administratorrechte und Benutzerzugriff

Mit der ROSA CLI können Sie einem Benutzer `dedicated-admin` Berechtigungen `cluster-admin` entziehen.

Um einem Benutzer den Zugriff zu entziehen, müssen Sie den Benutzer von Ihrem konfigurierten Identitätsanbieter entfernen.

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

1. Widerrufen Sie die `cluster-admin` Erlaubnis 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` Erlaubnis 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 konfigurierenCluster. 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.

Schritt 9: Löschen Sie einen Cluster und AWS STS Ressourcen

Sie können die ROSA CLI verwenden, um eine zu löschenCluster, 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 löschenROSA, können Sie die IAM Konsole verwenden.

> **Important**
>
> IAMRollen 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 IhresCluster.

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

> **Important**
>
> Sie müssen wartenCluster, 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 Namen der Richtlinie ein und wählen Sie Löschen.
   e. Wiederholen Sie diesen Schritt, um alle IAM-Richtlinien für zu löschen. Cluster

Erste Schritte mit ROSA classic mit AWS PrivateLink

Die klassischen ROSA-Cluster können auf verschiedene Arten bereitgestellt werden: öffentlich, privat oder privat mitAWS PrivateLink. Weitere Informationen zu ROSA classic finden Sie unter Bereitstellungsoptionen. 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 PrivateLinkist 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 istAWS PrivateLink.

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

Themen

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Aktionen abgeschlossen haben:

- Installieren und konfigurieren Sie die neueste VersionAWS 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.
- Service Quotasmuss über die erforderlichen Dienstkontingente fürAmazon EC2,, Amazon VPCAmazon EBS, verfügen, Elastic Load Balancing die für die Erstellung und Ausführung eines ROSA Clusters erforderlich sind. AWSoder Red Hat kann in Ihrem Namen eine Erhöhung der Servicekontingenten beantragen, sofern dies zur Problemlösung erforderlich ist. Die erforderlichen Kontingente finden Sie unter Red Hat OpenShift Service in AWSEndpunkte und Kontingente in der AWSAllgemeinen Referenz.
- Um AWS Support für zu erhaltenROSA, 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 Support für ROSA. Informationen zur Aktivierung AWS Support finden Sie AWS Supportauf 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 finden Sie in der ROSASCP-Dokumentation zur Fehlerbehebung. Weitere Informationen zu SCPs finden Sie unter Service Control Policies (SCPs).
- Wenn Sie ein ROSA Cluster With-Token AWS STS in einem aktivierten System 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 Verwaltung AWS-Regionen in der allgemeinen AWS-Referenz.

Schritt 1: Voraussetzungen aktivieren ROSA und konfigurieren

Um einen zu erstellen ROSACluster, müssen Sie zuerst 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 Get started (Erste Schritte) aus.
3. Wählen Sie auf der Seite ROSAVoraussetzungen 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.

Schritt 2: Erstellen Sie die Amazon VPC Architektur für den Cluster

Um eine zu erstellen, ROSA Cluster die verwendetAWS PrivateLink, müssen Sie zunächst Ihre eigene Amazon VPC Architektur konfigurieren, in der Ihre Lösung bereitgestellt werden soll. ROSAerfordert, dass Kunden mindestens ein öffentliches und ein privates Subnetz pro Availability Zone konfigurieren, die zum Erstellen von Clustern verwendet wird. Für Single-AZ-Cluster wird nur Availability Zone verwendet. Für Multi-AZ-Cluster sind drei Availability Zones erforderlich.

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

Das folgende Verfahren verwendet dieAWS CLI, um sowohl ein öffentliches als auch ein privates Subnetz in einer einzigen Availability Zone für einen Single-AZ-Cluster zu erstellen. Alle Cluster Ressourcen befinden sich im privaten Subnetz. Das öffentliche Subnetz leitet ausgehenden Datenverkehr mithilfe eines NAT-Gateways ins Internet weiter.

In diesem Beispiel wird der CIDR-Block `10.0.0.0/16` für die verwendet. Amazon VPC Sie können jedoch einen anderen CIDR-Block wählen. Weitere Informationen finden Sie unter Dimensionierung der VPC.

1. Legen Sie eine Umgebungsvariable für den Cluster Namen fest, indem Sie den folgenden Befehl ausführen.

```
ROSA_CLUSTER_NAME=rosa-privatelink
```

2. 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 ID der neuen VPC zurück. Im Folgenden finden Sie eine Beispielausgabe.

```
vpc-0410832ee325aafea
```

3. Verwenden Sie die VPC-ID aus dem vorherigen Schritt und kennzeichnen Sie die VPC mit der `ROSA_CLUSTER_NAME` Variablen.

```
aws ec2 create-tags --resources <VPC_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

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

```
aws ec2 modify-vpc-attribute --vpc-id <VPC_ID_VALUE> --enable-dns-hostnames
```

5. Erstellen Sie ein öffentliches Subnetz in der VPC mit einem `10.0.1.0/24` CIDR-Block und geben Sie die Availability Zone an, in der die Ressource erstellt werden soll.

> **Important**
>
> Achten Sie beim Erstellen von Subnetzen darauf, dass Subnetze für eine Availability Zone erstellt werden, in der Instanztypen verfügbar sind. ROSA Wenn Sie keine bestimmte Availability Zone auswählen, wird das Subnetz in einer der Availability Zones in der von Ihnen angegebenen Availability Zone erstellt. AWS-Region
> Verwenden Sie das `--availability zone` Argument im `create-subnet` Befehl, um eine bestimmte Availability Zone anzugeben. Sie können den `rosa list instance-types` Befehl verwenden, um alle verfügbaren ROSA Instance-Typen aufzulisten.
> Verwenden Sie den folgenden 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>"
```

> **Important**
>
> ROSAerfordert, dass Kunden mindestens ein öffentliches und ein privates Subnetz pro Availability Zone konfigurieren, die zur Erstellung von Clustern verwendet wird. Für Single-AZ-Cluster ist nur eine Availability Zone erforderlich. Für Multi-AZ-Cluster sind drei Availability Zones erforderlich. Wenn diese Anforderungen nicht erfüllt sind, schlägt die Clustererstellung fehl.

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.1.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

Der vorherige Befehl gibt die ID des neuen Subnetzes zurück. Im Folgenden finden Sie eine Beispielausgabe.

```
subnet-0b6a7e8cbc8b75920
```

6. Verwenden Sie die Subnetz-ID aus dem vorherigen Schritt und kennzeichnen Sie das Subnetz mithilfe der Variablen. `ROSA_CLUSTER_NAME-public`

```
aws ec2 create-tags --resources <PUBLIC_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-public
```

7. Erstellen Sie ein privates Subnetz in der VPC mit einem `10.0.0.0/24` CIDR-Block und geben Sie dabei dieselbe Availability Zone an, in der das öffentliche Subnetz bereitgestellt wurde.

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.0.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

Der vorherige Befehl gibt die ID des neuen Subnetzes zurück. Im Folgenden finden Sie eine Beispielausgabe.

```
subnet-0b6a7e8cbc8b75920
```

8. Verwenden Sie die Subnetz-ID aus dem vorherigen Schritt und kennzeichnen Sie das Subnetz mithilfe der Variablen. `ROSA_CLUSTER_NAME-private`

```
aws ec2 create-tags --resources <PRIVATE_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

9. Erstellen Sie ein Internet-Gateway für ausgehenden Datenverkehr und hängen Sie es an die VPC an.

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output
 text

aws ec2 attach-internet-gateway --vpc-id <VPC_ID_VALUE> --internet-gateway-id
 <IG_ID_VALUE>
```

10. Kennzeichnen Sie das Internet-Gateway mit der `ROSA_CLUSTER_NAME` Variablen.

```
aws ec2 create-tags --resources <IG_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

11. Erstellen Sie eine Routing-Tabelle für ausgehenden Verkehr, ordnen Sie sie dem öffentlichen Subnetz zu und konfigurieren Sie den Verkehr so, dass er zum Internet-Gateway weitergeleitet wird.

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PUBLIC_SUBNET_ID> --route-table-id
 <PUBLIC_RT_ID>

aws ec2 create-route --route-table-id <PUBLIC_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <IG_ID_VALUE>
```

12. Kennzeichnen Sie die öffentliche Routing-Tabelle mit der `ROSA_CLUSTER_NAME` Variablen und stellen Sie sicher, dass die Routing-Tabelle ordnungsgemäß konfiguriert wurde.

```
aws ec2 create-tags --resources <PUBLIC_RT_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

```
aws ec2 describe-route-tables --route-table-id <PUBLIC_RT_ID>
```

13 Erstellen Sie ein NAT-Gateway im öffentlichen Subnetz mit einer elastischen IP-Adresse, um den Verkehr zum privaten Subnetz zu ermöglichen.

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text

aws ec2 create-nat-gateway --subnet-id <PUBLIC_SUBNET_ID> --allocation-id
 <EIP_ADDRESS>  --query NatGateway.NatGatewayId --output text
```

14 Kennzeichnen Sie das NAT-Gateway und die elastische IP-Adresse mit der `$ROSA_CLUSTER_NAME` Variablen.

```
aws ec2 create-tags --resources <EIP_ADDRESS>  --resources <NAT_GATEWAY_ID> --tags
 Key=Name,Value=$ROSA_CLUSTER_NAME
```

15 Erstellen Sie eine Routing-Tabelle für privaten Subnetzverkehr, ordnen Sie sie dem privaten Subnetz zu und konfigurieren Sie den Datenverkehr so, dass er zum NAT-Gateway weitergeleitet wird.

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PRIVATE_SUBNET_ID> --route-table-id
 <PRIVATE_RT_ID>

aws ec2 create-route --route-table-id <PRIVATE_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <NAT_GATEWAY_ID>
```

16 Kennzeichnen Sie die private Routentabelle und die elastische IP-Adresse mit der `$ROSA_CLUSTER_NAME-private` Variablen.

```
aws ec2 create-tags --resources <PRIVATE_RT_ID> <EIP_ADDRESS> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

Schritt 3: Erstellen Sie einen Cluster mit AWS PrivateLink

Sie können AWS PrivateLink und die ROSA CLI verwenden, um eine Cluster mit einer einzigen Availability Zone (Single-AZ) oder mehreren Availability Zones (Multi-AZ) zu 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 eine Single-AZ zu erstellen. ROSA Cluster Um eine Multi-AZ zu erstellenCluster, geben Sie `multi-az` im Befehl und die privaten Subnetz-IDs für jedes private Subnetz an, in dem Sie die Bereitstellung durchführen möchten.

> **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 AWSFirewall-Voraussetzungen in der Red OpenShift Hat-Dokumentation.

1. Erstellen Sie eine Single-AZ, Cluster indem Sie den folgenden Befehl ausführen.

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

> **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 Befehls an. `rosa create cluster`

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

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

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

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

4. Überprüfen Sie den Status Ihres. Cluster

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

Example

> **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 unter Problembehandlung bei der ROSA Cluster-Bereitstellung.

Wenn Sie sich an den Red Hat Support wenden AWS Support möchten, um Unterstützung zu erhalten, siehe Support für ROSA.

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

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

Schritt 4: Konfigurieren Sie die AWS PrivateLink DNS-Weiterleitung

Cluster, die verwenden, AWS PrivateLink erstellen eine öffentliche gehostete Zone und eine private gehostete Zone inRoute 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 normalerweise 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

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

1. Öffnen Sie die Route 53-Konsole.
2. Wählen Sie im Navigationsbereich unter Resolver die Option Inbound Endpoints aus.
3. Wählen Sie Endpunkte konfigurieren aus.
4. Wählen Sie mit dem AWS-Region Selektor oben rechts die ausAWS-Region, die die für den Cluster verwendete VPC enthält.
5. Wählen Sie unter Grundkonfiguration die Option Nur eingehend und dann Weiter aus.
6. Füllen Sie auf der Seite „Eingehenden Endpunkt konfigurieren“ den Abschnitt Allgemeine Einstellungen für eingehenden Endpunkt aus. Wählen Sie unter Sicherheitsgruppe für diesen Endpunkt eine Sicherheitsgruppe aus, die eingehenden UDP- und TCP-Verkehr vom Remote-Netzwerk am Zielport 53 zulässt.
7. Wählen Sie im Abschnitt IP-Adresse die Availability Zones und privaten Subnetze aus, die bei der Erstellung des Clusters verwendet wurden, und klicken Sie auf Weiter.
8. (Optional) Füllen Sie den Abschnitt „Tags“ aus.
9. Wählen Sie Submit (Absenden) aus.

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.

Schritt 5: Konfigurieren Sie einen Identitätsanbieter und gewähren Cluster Sie Zugriff

ROSAbeinhaltet einen integrierten OAuth-Server. Nach der Erstellung müssen Sie OAuth für die Verwendung eines Identitätsanbieters konfigurieren. ROSA Cluster 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 konfigurierenCluster. 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 Identitätsbereitstellung verwenden können ROSACluster, 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 auf der GitHub OAuth-Seite, um die verbleibenden `rosa create idp` interaktiven Eingabeaufforderungen zu füllen, <GITHUB_CLIENT_ID> und <GITHUB_CLIENT_SECRET> ersetzen Sie dabei die Anmeldeinformationen Ihrer OAuth-Anwendung. GitHub

```
...
? 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 Identitätsanbieter-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>
```

Schritt 6: 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.

Schritt 7: Erteilen Sie einem Benutzer Administratorrechte

Nachdem Sie Ihrem konfigurierten Identitätsanbieter einen Benutzer hinzugefügt haben, können Sie dem Benutzer `cluster-admin` oder `dedicated-admin` Berechtigungen für Ihren gewährenCluster.

`cluster-admin`Berechtigungen konfigurieren

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>
```

`dedicated-admin`Berechtigungen konfigurieren

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>
```

Schritt 8: Greifen Sie Cluster über die Webkonsole 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. Ersetzen Sie `<CLUSTER_NAME>` 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 habenCluster, wählen Sie den Namen des Identitätsanbieters im Dialogfeld Anmelden mit... und füllen Sie alle Autorisierungsanfragen Ihres Anbieters aus.

Schritt 9: 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 anschließend „Anwendung erstellen“, um die Seite „Source-to-Image-Anwendung 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.

Schritt 10: Widerrufen Sie Administratorrechte und Benutzerzugriff

Mit der ROSA CLI können Sie einem Benutzer `dedicated-admin` Berechtigungen `cluster-admin` entziehen.

Um einem Benutzer den Zugriff zu entziehen, müssen Sie den Benutzer von Ihrem konfigurierten Identitätsanbieter entfernen.

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 konfigurierenCluster. 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.

Schritt 11: Löschen Sie einen Cluster und AWS STS Ressourcen

Sie können die ROSA CLI verwenden, um eine zu löschenCluster, 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 löschenROSA, können Sie die IAM Konsole verwenden.

> **Important**
>
> IAMRollen 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 IhresCluster.

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

> **Important**
>
> Sie müssen wartenCluster, 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

Der Überblick über die Verantwortlichkeiten für die ROSA Dokumentation und das Modell der AWS gemeinsamen Verantwortung definieren den Datenschutz in ROSA. AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen 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 sollten Sie die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie 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 API ROSA oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Dienste ROSA oder andere Dienste eingeben, werden möglicherweise für die 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 durch 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 sekundäre Gruppen-IDs des Access Points Amazon EFS berücksichtigt werden. Amazon EFS ersetzt die Benutzer- und Gruppen-IDs in Dateien durch die Benutzer- und Gruppen-IDs auf dem Access Point und ignoriert NFS-Client-IDs. Ignoriert daher Amazon EFS stillschweigend Einstellungen. `fsGroup` ROSA ist nicht in der Lage, die GIDs von Dateien mithilfe von zu ersetzen. `fsGroup` Jeder Pod, der auf einen bereitgestellten Access Point Amazon EFS 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 Ihren eigenen, vom Kunden verwalteten Schlüssel anzugeben. Weitere Informationen finden Sie unter Datenverschlüsselung mit KMS.

Datenverschlüsselung für die integrierte Image-Registrierung

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.

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.
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 key Weitere Informationen zum Erstellen von Schlüsseln finden Sie unter KMS-Schlüssel mit symmetrischer Verschlüsselung erstellen im AWS KMS Developer Guide.

Sie können auch persistente Volumes 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.

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 Infrastruktursicherheit in ROSA.

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
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- ROSA Beispiele für identitätsbasierte Richtlinien
- AWS verwaltete IAM Richtlinien für ROSA
- Fehlerbehebung bei ROSA Identität und Zugriff

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 Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in nicht auf eine Funktion zugreifen können ROSA, finden Sie weitere Informationen unter Problembehandlung bei ROSA Identität und Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die 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 IAM verwenden können, finden Sie unter Beispiele für ROSA identitätsbasierte Richtlinien.

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 Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung bei 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 unter Signaturprozess für Signature Version 4 in der Allgemeinen AWS-Referenz.

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.

Root-Benutzer des AWS-Kontos

Wenn Sie eine erstellen AWS-Konto, beginnen Sie mit einer Single-Sign-In-Identität, die vollständigen Zugriff auf alle Ressourcen im Konto hat. AWS-Services 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 Referenzhandbuch zur Kontoverwaltung unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind.

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 AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) -Benutzerhandbuch.

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 vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe mit dem Namen IAMAdmins einrichten und dieser Gruppe Berechtigungen zur Verwaltung von Ressourcen erteilen. IAM

Benutzer unterscheiden sich von 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 unter Wann sollte eine Rolle IAM-Benutzer (statt einer Rolle) erstellt werden? im IAM-Benutzerhandbuch.

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 Management Console 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 (Nachfolger von AWS Single Sign-On) -Benutzerhandbuch.

- Temporäre IAM-Benutzer Berechtigungen — Ein 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-Anfragen 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 sollte eine IAM Rolle (anstelle eines Benutzers) erstellt werden?.

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. Berechtigungen in den Richtlinien bestimmen, ob die 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 Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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 Management Console 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. Inline-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.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 AWS WAF, und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen zu ACLs finden Sie unter Zugriffssteuerungsliste (ACL) – Übersicht im Entwicklerhandbuch zu Amazon Simple Storage Service.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- 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.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP beschränkt die Berechtigungen für Entitäten in Mitgliedskonten, einschließlich der einzelnen AWS-Konto Root-Benutzer. Weitere Informationen zu Organisationen und SCPs finden Sie unter Funktionsweise von 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 mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

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 Management Console 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. Weitere Informationen zu finden Sie `ROSAManageSubscription` unter AWS Verwaltete Richtlinie: ROSA ManageSubscription.

AWS verwaltete Richtlinien für ROSA mit HCP

ROSA mit Hosted Control Planes (HCP) verwendet AWS verwaltete Richtlinien mit Berechtigungen, die für den Betrieb und Support des Dienstes 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 AWS -verwaltete Richtlinien für ROSA.

Vom Kunden verwaltete Richtlinien für ROSA classic

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 einem eingeschränkteren Satz von Berechtigungen. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für ROSA.

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 finden Sie unter ROSA Classic-Kontorichtlinien und ROSA Classic-Betreiberrichtlinien.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es ermöglicht, die internen und verwalteten Richtlinien IAM-Benutzer einzusehen, 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": [
```

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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 durch Ausführen `rosa list account-roles` sicherstellen, dass die Richtlinienversion und die Clusterversion identisch sind. Wenn die

Richtlinienversion niedriger als die Clusterversion ist, führen Sie die Ausführung aus, `rosa upgrade account-roles` um die Rollen und die zugehörigen 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

In diesem Richtliniendokument definierte 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:PassRole",
                "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:GetBucketReplication",
```

```
                "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:PassRole",
                "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 wie Zugriffsschlüssel-IDs, angehängten Inline-Richtliniendokumenten, Erstellungsdatum, Pfad, Benutzer-ID und Amazon-Ressourcenname (ARN) des Benutzers. 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, einschließlich. 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 IAM Richtlinien für ROSA

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, 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 kundenverwaltete 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: ROSA ManageSubscription

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 Konsolenrolle 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 ROSA ManageSubscription im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinien für ROSA mit HCP-Kontorollen

Sie können diese AWS verwalteten Richtlinien den Kontorollen zuordnen, die für die Verwendung von ROSA mit Hosted Control Planes (HCP) erforderlich sind. Die Berechtigungen sind für die Unterstützung von Red Hat Site Reliability Engineering (SRE) auf dem Cluster, die Clustererstellung und die Rechenfunktionen erforderlich.

Die folgenden verwalteten Richtlinien sind erforderlich:

- ROSA WorkerInstancePolicy — Ermöglicht dem ROSA Service, Amazon EC2 Instanzlebenszyklen in einem ROSA Cluster zu verwalten.
- ROSASRE SupportPolicy — 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 Clusterknoten zu ändern. ROSA
- ROSA InstallerPolicy — Erteilt dem Installer die erforderlichen Berechtigungen zur Verwaltung von AWS Ressourcen, die die Clusterinstallation unterstützen.

AWS verwaltete Richtlinien für ROSA mit HCP-Operatorrollen

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

Die folgenden verwalteten Richtlinien sind erforderlich:

- Amazon EBS RosaAmazoneBSCSI DriverOperatorPolicy — Erteilt dem CSI-Treiberoperator die erforderlichen Berechtigungen zur Installation und Wartung des CSI-Treibers auf einem Cluster Amazon EBS . ROSA
- ROSA IngressOperatorPolicy — Erteilt dem Ingress Operator die erforderlichen Berechtigungen zur Bereitstellung und Verwaltung von Load Balancers und DNS-Konfigurationen für Cluster. ROSA Die Richtlinie ermöglicht den Lesezugriff auf Tag-Werte. Der Operator filtert dann die Tag-Werte nach Route 53 Ressourcen, um gehostete Zonen zu erkennen.

- ROSA ImageRegistryOperatorPolicy — Erteilt 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.
- ROSA CloudNetworkConfigOperatorPolicy — Erteilt dem Cloud Network Config Controller Operator die erforderlichen Berechtigungen zur Bereitstellung und Verwaltung von Netzwerkressourcen für das ROSA Cluster-Netzwerk-Overlay.
- ROSA KubeControllerPolicy — Erteilt dem Kube-Controller die erforderlichen Berechtigungen zur Verwaltung Amazon EC2 Elastic Load Balancing, und AWS KMS Ressourcen für einen Cluster ROSA mit gehosteten Steuerungsebenen.
- ROSA NodePoolManagementPolicy — Erteilt dem NodePool Controller die erforderlichen Berechtigungen zum Beschreiben, Ausführen und Beenden von Amazon EC2 Instanzen, die als Worker-Knoten verwaltet werden. Diese Richtlinie ermöglicht auch die Festplattenverschlüsselung des Worker-Knoten-Root-Volumes mithilfe von AWS KMS Schlüsseln.
- ROSAKMS ProviderPolicy — Erteilt dem integrierten AWS Encryption Provider die erforderlichen Berechtigungen zur Verwaltung von AWS KMS Schlüsseln, die die etcd-Datenverschlüsselung unterstützen. Diese Richtlinie ermöglicht Amazon EC2 das Verschlüsseln und Entschlüsseln von `etcd` Daten mithilfe der vom Encryption Provider bereitgestellten KMS-Schlüssel. AWS
- ROSA ControlPlaneOperatorPolicy — Erteilt dem Bediener der Kontrollebene die erforderlichen Berechtigungen zur Verwaltung von Amazon EC2 Clustern und Route 53 Ressourcen für ROSA gehostete Kontrollebenen.

Informationen zu verwalteten Richtlinienberechtigungen finden Sie unter AWS Verwaltete Richtlinien im Referenzhandbuch für AWS verwaltete Richtlinien.

ROSA Aktualisierungen AWS verwalteter Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die ROSA seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite mit dem ROSA Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
ROSA NodePoolManagement Policy — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass der ROSA Knotenpool-Manager DHCP-	2. Mai 2024

Änderung	Beschreibung	Datum
	Optionssätze beschreiben kann, um die richtigen privaten DNS-Namen festzulegen. Weitere Informationen finden Sie unter ROSA NodePoolManagementPolicy.	
ROSA InstallerPolicy — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass das ROSA Installationsprogramm mithilfe von Tag-Schlüsseln Tags zu Subnetzen hinzufügen kann. `"kubernetes.io/cluster/*"` Weitere Informationen finden Sie unter ROSA InstallerPolicy.	24. April 2024
ROSSARE SupportPolicy — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass die SRE-Rolle Informationen zu Instanzprofilen abrufen kann, die mit as gekennzeichnet ROSA wurden. `red-hat-managed` Weitere Informationen finden Sie unter ROSASRE SupportPolicy.	10. April 2024

Änderung	Beschreibung	Datum
ROSA InstallerPolicy — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass das ROSA Installationsprogramm überprüfen kann, ob AWS verwaltete Richtlinien für IAM Rollen zugeordnet ROSA sind, die von verwendet werden ROSA. Mit diesem Update kann das Installationsprogr amm auch feststellen, ob vom Kunden verwaltete Richtlinien an ROSA Rollen angehängt wurden. Weitere Informati onen finden Sie unter ROSA InstallerPolicy.	10. April 2024
ROSA InstallerPolicy — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass der Dienst Warnmeldungen für das Installationsprogramm ausgeben kann, wenn die Clusterinstallation aufgrund eines fehlenden kundenspe zifischen Cluster-OIDC-Anbieters fehlschlägt. Dieses Update ermöglicht es dem Dienst auch, vorhandene DNS-Nameserver abzurufen , sodass Cluster-Bereitstel lungsvorgänge idempoten t sind. Weitere Informati onen finden Sie unter ROSA. InstallerPolicy	26. Januar 2024

Änderung	Beschreibung	Datum
ROSSARE SupportPolicy — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass der Dienst mithilfe der API Lesevorgänge für Sicherheitsgruppen durchführen kann. DescribeSecurityGroups Weitere Informationen finden Sie unter ROSASRE SupportPolicy.	22. Januar 2024
ROSA ImageRegistryOperatorPolicy — Richtlinie 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 finden Sie unter ROSA. ImageRegistryOperatorPolicy	12. Dezember 2023
ROSA KubeControllerPolicy — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, sodass Availability Zones, Amazon EC2 Instances, Routing-Tabellen, Sicherheitsgruppen, VPCs und Subnetze beschrieben werden können. kube-controller-manager Weitere Informationen finden Sie unter ROSA. KubeControllerPolicy	16. Oktober 2023

Änderung	Beschreibung	Datum
ROSA ManageSubscription — Richtlinie aktualisiert	ROSA Die Richtlinie wurde aktualisiert, um die ROSA mit gehosteten Kontrollebenen hinzuzufügen ProductId. Weitere Informationen finden Sie unter ROSA ManageSubscription.	1. August 2023
ROSA KubeControllerPolicy — 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 finden Sie unter ROSA. KubeControllerPolicy	13. Juli 2023

Änderung	Beschreibung	Datum
ROSA NodePoolManagement Policy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem NodePool Controller ermöglicht, Amazon EC2 Instanzen, die als Worker-Knoten verwaltet werden, zu beschreiben, auszuführen und zu beenden. Diese Richtlinie ermöglicht auch die Festplattenverschlüsselung des Worker-Knoten-Root-Volumes mithilfe von AWS KMS Schlüsseln. Weitere Informationen finden Sie unter ROSA NodePoolManagement Policy.	08. Juni 2023
ROSA InstallerPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Installer ermöglicht, AWS Ressourcen zu verwalten, die die Clusterinstallation unterstützen. Weitere Informationen finden Sie unter ROSA InstallerPolicy.	6. Juni 2023

Änderung	Beschreibung	Datum
ROSSARE SupportPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es Red Hat SREs ermöglicht, 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. Weitere Informationen finden Sie unter SupportPolicyROSASRE.	01. Juni 2023
ROSAMS — Neue Richtlinie hinzugefügt ProviderPolicy	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 finden Sie unter ProviderPolicyROSAKMS.	27. April 2023

Änderung	Beschreibung	Datum
ROSA KubeControllerPolicy — 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 gehostete n Steuerungsebenen zu verwalten und zu verwalten. Weitere Informationen finden Sie unter ROSA KubeContr ollerPolicy.	27. April 2023
ROSA ImageRegistryOpera torPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Image Registry Operator ermöglicht, Ressourcen für die ROSA Cluster-Image-Regi stry und abhängige Dienste, einschließlich S3, bereitzus tellen und zu verwalten. Weitere Informationen finden Sie unter ROSA ImageRegi stryOperatorPolicy.	27. April 2023

Änderung	Beschreibung	Datum
ROSA ControlPlaneOperatorPolicy — 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 finden Sie unter ROSA ControlPlaneOperatorPolicy.	24. April 2023
ROSA CloudNetworkConfigOperatorPolicy — 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 finden Sie unter ROSA CloudNetworkConfigOperatorPolicy.	20. April 2023
ROSA IngressOperatorPolicy — 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 finden Sie unter ROSA. IngressOperatorPolicy	20. April 2023

Änderung	Beschreibung	Datum
RosaAmazoneBSCSI DriverOperatorPolicy — Neue Richtlinie hinzugefügt	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Amazon EBS CSI Driver Operator ermöglicht, den CSI-Treiber auf einem Cluster zu installieren und zu warten. Amazon EBS ROSA Weitere Informationen finden Sie unter DriverOperatorPolicyRosaAmazonEBSCSI.	20. April 2023
ROSA — Neue Richtlini e hinzugefügt WorkerIns tancePolicy	ROSA Es wurde eine neue Richtlinie hinzugefügt, die es dem Dienst ermöglich t, Clusterressourcen zu verwalten. Weitere Informati onen finden Sie unter ROSA WorkerInstancePolicy.	20. April 2023
ROSA ManageSubscription — 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 finden Sie unter ROSA ManageSub scription.	11. April 2022
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

AWS verwaltete Richtlinien für ROSA mit HCP-Kontorollen

> **Note**
>
> Diese AWS verwalteten 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 ROSA Classic-Kontorichtlinien und ROSA Classic-Betreiberrichtlinien.

Diese AWS verwalteten Richtlinien fügen Berechtigungen hinzu, die von ROSA mit IAM-Rollen für Hosted Control Planes (HCP) 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.

Themen

- AWS verwaltete Richtlinie: ROSA WorkerInstancePolicy
- AWS verwaltete Richtlinie: ROSASRE SupportPolicy
- AWS verwaltete Richtlinie: ROSA InstallerPolicy

AWS verwaltete Richtlinie: ROSA WorkerInstancePolicy

Sie können eine Verbindung `ROSAWorkerInstancePolicy` zu Ihren IAM Entitäten herstellen. Bevor Sie eine ROSA mit einem Cluster für gehostete Steuerungsebenen erstellen, müssen Sie diese Richtlinie zunächst einer Worker-IAM-Rolle zuordnen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, mit denen der ROSA Dienst die folgenden Aufgaben ausführen kann:

- `ec2`— Überprüfung AWS-Region und Amazon EC2 Instanzdetails im Rahmen des Lebenszyklusmanagements von Worker-Knoten in einem ROSA Cluster.

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

AWS verwaltete Richtlinie: ROSASRE SupportPolicy

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

Bevor Sie einen ROSA-Cluster mit gehosteten Steuerungsebenen erstellen, müssen Sie diese Richtlinie zunächst einer Support-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 ROSASRE SupportPolicy im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSA InstallerPolicy

Sie können eine Verbindung `ROSAInstallerPolicy` zu Ihren IAM Entitäten herstellen.

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 aus, die auf AWS-Konten RedHat gehostet werden und von Red Hat verwaltet werden. Beschreiben Sie Amazon EC2 Instanzen, Volumes und Netzwerkressourcen, die mit Amazon EC2 Knoten verknüpft sind. Dies ist erforderlich, damit die Kubernetes-Steuerebene Instanzen zu einem Cluster zusammenfügen kann. Dies ist auch erforderlich, damit der Cluster seine Präsenz innerhalb des Clusters bewerten kann. Amazon VPC Kennzeichnen Sie Subnetze mithilfe von übereinstimmenden `"kubernetes.io/cluster/*"` Tag-Schlüsseln. Dies ist erforderlich, um sicherzustellen, dass der für den Clustereingang verwendete Load Balancer nur in den entsprechenden Subnetzen erstellt wird.
- `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 auf sichere Weise zu ermöglichen.

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

AWS verwaltete Richtlinien für ROSA mit HCP-Operatorrollen

> **Note**
>
> Diese AWS verwalteten 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 ROSA Classic-Kontorichtlinien und ROSA Classic-Betreiberrichtlinien.

Diese AWS verwalteten Richtlinien fügen Berechtigungen hinzu, die von ROSA mit IAM-Rollen für Hosted Control Planes (HCP) verwendet werden. Die Berechtigungen sind für OpenShift Betreiber auf dem ROSA with HCP-Cluster erforderlich, um Clusterknoten zu verwalten.

Themen

- AWS verwaltete Richtlinie: RosaAmazonEBSCSI DriverOperatorPolicy
- AWS verwaltete Richtlinie: ROSA IngressOperatorPolicy
- AWS verwaltete Richtlinie: ROSA ImageRegistryOperatorPolicy
- AWS verwaltete Richtlinie: ROSA CloudNetworkConfigOperatorPolicy
- AWS verwaltete Richtlinie: ROSA KubeControllerPolicy
- AWS verwaltete Richtlinie: ROSA NodePoolManagementPolicy
- AWS verwaltete Richtlinie: ROSAMS ProviderPolicy
- AWS verwaltete Richtlinie: ROSA ControlPlaneOperatorPolicy

AWS verwaltete Richtlinie: RosaAmazonEBSCSI DriverOperatorPolicy

Sie können eine Verbindung zu Ihren Entitäten herstellen. `ROSAAmazonEBSCSIDriverOperatorPolicy` IAM 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 unter RosaAmazonEBSCSI DriverOperatorPolicy im Managed Policy Reference Guide. AWS

AWS verwaltete Richtlinie: ROSA IngressOperatorPolicy

Sie können eine Verbindung `ROSAIngressOperatorPolicy` zu Ihren IAM Entitäten herstellen. 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 unter ROSA IngressOperatorPolicy im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSA ImageRegistryOperatorPolicy

Sie können eine Verbindung `ROSAImageRegistryOperatorPolicy` zu Ihren IAM Entitäten herstellen. 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 unter ROSA ImageRegistryOperatorPolicy im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSA CloudNetworkConfigOperatorPolicy

Sie können eine Verbindung `ROSACloudNetworkConfigOperatorPolicy` zu Ihren IAM Entitäten herstellen. 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 unter ROSA CloudNetworkConfigOperatorPolicy im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSA KubeControllerPolicy

Sie können eine Verbindung `ROSAKubeControllerPolicy` zu Ihren IAM Entitäten herstellen. 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, Sicherheitsgruppen, VPCs und Subnetze.
- `elasticloadbalancing`— Load Balancer und ihre Richtlinien erstellen und verwalten, Load Balancer-Listener erstellen und verwalten, Ziele bei Zielgruppen registrieren und Zielgruppen verwalten, Amazon EC2 Instances bei einem Load Balancer registrieren und deregistrieren und Tags zu Load Balancers hinzufügen.
- `kms`— Rufen Sie 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 unter ROSA KubeControllerPolicy im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSA NodePoolManagementPolicy

Sie können eine Verbindung `ROSANodePoolManagementPolicy` zu Ihren IAM Entitäten herstellen. 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, um die Festplattenverschlüsselung des Worker-Knoten-Root-Volumes mithilfe von AWS KMS Schlüsseln zu ermöglichen. 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 aus, die auf AWS-Konten RedHat gehostet werden und von Red Hat verwaltet werden. 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
- `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 unter ROSA NodePoolManagementPolicy im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSAMS ProviderPolicy

Sie können eine Verbindung `ROSAKMSProviderPolicy` zu Ihren IAM Entitäten herstellen. 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 ROSAKMS ProviderPolicy im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: ROSA ControlPlaneOperatorPolicy

Sie können eine Verbindung `ROSAControlPlaneOperatorPolicy` zu Ihren IAM Entitäten herstellen. 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 unter ROSA ControlPlaneOperatorPolicy im Referenzhandbuch für AWS verwaltete Richtlinien.

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 ROSA ManageSubscription im Referenzhandbuch für AWS verwaltete Richtlinien.
2. Gehen Sie wie in Schritt 1: Aktivieren ROSA und Konfigurieren der Voraussetzungen für die Aktivierung beschrieben vor ROSA.

Wenn Sie nicht berechtigt sind, Ihren Berechtigungssatz 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 `ROSAManageSubscription` anzuhängen, und folgen Sie den Anweisungen in Schritt 1: 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 bei der Aktivierung 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 ROSA ManageSubscription im Referenzhandbuch für AWS verwaltete Richtlinien.
2. Gehen Sie wie in Schritt 1: Aktivieren ROSA und Konfigurieren der Voraussetzungen für die Aktivierung beschrieben vor 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.

Die Site Reliability Engineers (SREs) von Red Hat verwalten die Kontrollebene und die Infrastrukturknoten vollständig. Red Hat SREs überwachen den ROSA Cluster proaktiv und sind dafür verantwortlich, alle ausgefallenen Knoten der Steuerungsebene und Infrastrukturknoten zu ersetzen. Weitere Informationen finden Sie unter Überblick über die Zuständigkeiten für. ROSA

> **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 Amazon EC2 Instances, die sie ROSA verwenden, manuell von der AWS Konsole oder aus 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 (SREs) von Red Hat 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 unter Überblick über die Zuständigkeiten für ROSA.

Wenn Sie einen neuen Cluster erstellen, haben Sie die ROSA Möglichkeit, 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 der 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. Weitere Informationen finden Sie unter Netzwerkrichtlinie in der Red Hat-Dokumentation.

ROSA-Service Quotas

Red Hat OpenShift Service in AWS(ROSA) verwendet Servicekontingente fürAmazon EC2, Amazon Virtual Private Cloud (Amazon VPC), Amazon Elastic Block Store (Amazon EBS) und Elastic Load Balancing (ELB) zur Bereitstellung von Clustern.

Erforderliche Mindestkontingente für ROSA

Für die folgenden Amazon EC2 und Amazon EBS Kontingente ROSA ist ein höheres Kontingent erforderlich, als es der Standardservice bietet. Sie müssen möglicherweise eine Erhöhung einiger dieser Kontingente anfordern. ROSA Weitere Informationen finden Sie unter Anfordern einer Kontingenterhöhung im Service QuotasBenutzerhandbuch.

Important

Für Amazon EC2 On-Demand-Standard-Instances (A, C, D, H, I, M, R, T, Z) reicht der Standardwert von 5 vCPUs nicht aus, um Cluster zu erstellenROSA. ROSAbenötigt 100 vCPUs oder mehr für die Clustererstellung. Um eine Kontingenterhöhung anzufordern, können Sie die Service QuotasKonsole verwenden.

Note

Sie können Ihre Kontingente mithilfe der AWS SDKs überprüfen, aber die SDK-Berechnung berücksichtigt keine vorhandenen ROSA Ressourcen. Die Kontingentprüfung im SDK ist möglicherweise erfolgreich und die ROSA Cluster Erstellung schlägt möglicherweise fehl. Um dieses Problem zu beheben, können Sie die Service QuotasKonsole verwenden.

Name	Code des Dienstes	Standard	Minimum erforderlich	Einstellbar	Beschreibung
On-Demand -Ausführung von Standard-	ec2	5	100	Ja	Maximale Anzahl von vCPUs, die laufenden

Name	Code des Dienstes	Standard	Minimum erforderlich	Einstellbar	Beschreibung
Instances (A, C, D, H, I, M, R, T, Z)					On-Demand -Standard -Instances (A, C, D, H, I, M, R, T, Z) zugewiesen sind. Der Standardwert von 5 vCPUs reicht nicht aus, um Cluster zu erstellen ROSA. ROSAbenötigt 100 vCPUs für die Clusterer stellung.

Name	Code des Dienstes	Standard	Minimum erforderlich	Einstellbar	Beschreibung
Speicher für Universelle-SSD-Volumes (gp3), in TiB	ebs	50	300	Ja	Die maximale aggregierte Speicherm enge in TiB, die über Universelle-HDD-Volumes (gp3) in dieser Region bereitgestellt werden kann. Für eine optimale Leistung sind 300 TiB Speicher erforderlich.

Name	Code des Dienstes	Standard	Minimum erforderlich	Einstellbar	Beschreibung
Speicher für Universelle-SSD-Volumes (gp2), in TiB	ebs	50	300	Ja	Die maximale aggregierte Speicherm enge in TiB, die über Universelle-HDD-Volumes (gp2) in dieser Region bereitgestellt werden kann. Für eine optimale Leistung sind 300 TiB Speicher erforderlich.

Name	Code des Dienstes	Standard	Minimum erforderlich	Einstellbar	Beschreibung
Speicher für Bereitgestellte-IOPS-SSD-Volumes (io1), in TiB	ebs	50	300	Ja	Die maximale aggregierte Speicherm enge in TiB, die über Bereitgestellte-IOPS-SSD-Volumes (io1) in dieser Region bereitgestellt werden kann. Für eine optimale Leistung sind 300 TiB Speicher erforderlich.

> **Note**
>
> Die Standardwerte sind die anfänglichen Kontingente, die von AWS gesetzt werden und die vom tatsächlich angewendeten Kontingentwert und dem maximal möglichen Dienstkontingent getrennt sind. Weitere Informationen finden Sie Service Quotasim Service QuotasBenutzerhandbuch unter Terminologie.

Standardkontingente für ROSA

ROSAverwendet die folgenden Standardkontingente fürAmazon EC2, Amazon VPCAmazon EBS, undElastic Load Balancing. Informationen zur Erhöhung von Kontingenten finden Sie im Service QuotasBenutzerhandbuch unter Anfordern einer Kontingenterhöhung.

Amazon EC2

- EC2-VPC Elastic IPs

Amazon VPC

- VPCs pro Region
- Netzwerkschnittstellen pro Region
- Internet-Gateways pro Region

Amazon EBS

- Snapshots pro Region
- IOPS für bereitgestellte IOPS-SSD-Volumes (io1)

Elastic Load Balancing

- Application Load Balancerspro Region
- Classic Load Balancerspro Region

AWS In ROSA integrierte -Services

ROSA arbeitet mit anderen zusammenAWS-Services, um zusätzliche Lösungen für Ihre geschäftlichen Herausforderungen bereitzustellen. In diesem Thema werden Services aufgeführt, die mithilfe von ROSA ihre Funktionalität erweitern, sowie Services, die ROSA zur Ausführung von Aufgaben nutzt.

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 Management Console.

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 Red Hat Site Reliability Engineers (SREs) anfallen. 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 Red Hat Site Reliability Engineers (SREs) ab. ROSA

Die Servicegebühren sind in allen unterstützten AWS Standardregionen einheitlich. ROSA mit HCP-Servicegebühren fallen standardmäßig bei Bedarf zu einem pauschalen Stundensatz an, der auf der Anzahl der laufenden Cluster und der Worker-Node-vCPUs basiert, die in diesen Clustern ausgeführt werden. Die klassischen Servicegebühren von ROSA fallen bei Bedarf auf der Grundlage der Anzahl der Worker-Node-vCPUs vCPUs. 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. Um zusätzliche Einsparungen bei den AWS Infrastrukturkosten zu erzielen, 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 Billing and Cost Management 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.

ROSA Verträge

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 -Preisgestaltung.

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 Unterschiede zwischen ROSA mit HCP und ROSA classic.
> Um in Regionen ohne ROSA Classic-Verträge mit HCP-Support zu erwerben, rufen Sie die ROSA Konsole auf und wählen Sie „Softwarevertrag kaufen“ und „Bestehende Verträge anzeigen“.

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 aus.
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 AWS 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 die von Ihnen angegebenen Worker-Node-vCPUs und Steuerungsebenen deckt.

Wenn Sie einen 12-Monats-Vertrag mit ROSA mit HCP erwerben, zahlen Sie eine Vorauszahlung für eine jährliche Laufzeit und zahlen für die nächsten 12 Monate keine stündliche Nutzungsgebühr für die betroffenen Worker-Node-vCPUs und Steuerungsebenen. Die Vertragskosten basieren auf der Anzahl der Worker-Node-vCPUs und Steuerungsebenen, die Sie auswählen. Der Vertrag deckt nur die Worker-Node-vCPUs und Steuerungsebenen 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 -Preisgestaltung.

Monatliches Nutzungskontingent

Beim Kauf werden Ihre Prepaid-vCPUs und Control Planes 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-Node-vCPUs: Anzahl der vCPUs 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-Node-vCPUs und 8 Steuerungsebenen würde beispielsweise zu einem monatlichen Kontingent von 2.920.000 Worker-Node-vCPU-Stunden und 5.840 Stunden für die Kontrollebene, die pro Monat verbraucht werden können, 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 unter Unterschiede zwischen 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 Anzahl der zu kaufenden vCPUs ein. 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 AWS 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-vCPUs und Steuerungsebenen 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 die Worker-Node-vCPUs und Steuerungsebenen ab, die Sie bei der Vertragserstellung angeben. Vertrags-Upgrades wirken sich nicht auf die für AWS die Infrastruktur erhobenen Gebühren aus.

Nach dem Upgrade werden die hinzugefügten vCPUs und Steuerungsebenen in ein monatliches Nutzungskontingent umgewandelt, 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 Monatliches Nutzungskontingent.

Um einen 12-Monats-Vertrag 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 Anzahl der hinzuzufügenden vCPUs ein. 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.

Einholung eines privaten Angebots

Sie können ein AWS Marketplace privates Angebot für ROSA bei HCP oder ROSA classic anfordern, um die mit Red Hat ausgehandelten Produktpreise und die 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 mit dem richtigen Konto anmelden, wird der Fehler „Seitennotiz gefunden“ (404) angezeigt.

4. Lesen Sie sich die Allgemeinen Geschäftsbedingungen durch.
5. Wählen Sie Bedingungen akzeptieren aus.

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

6. Um die Angebotsdetails zu überprüfen, wählen Sie in der Produktliste 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

In der folgenden Dokumentation wird beschrieben, wie Sie Probleme beheben können, die bei der Aktivierung ROSA und Bereitstellung von Clustern auftreten können. ROSA

Themen

Support für ROSA

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

AWS Support

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

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

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

RedHat Support

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.

Probleme bei der ROSA Clustererstellung beheben

Dieser Abschnitt enthält Lösungen für Probleme, die beim Erstellen von ROSA Clustern auftreten können.

Mit ROSA können Sie auch Unterstützung bei der Fehlerbehebung von AWS Support und den RedHat Support-Teams erhalten. Weitere Informationen finden Sie unter Support für ROSA.

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

Beschreibung

Für die Nutzung ROSA müssen die Dienstkontingente für Ihr Konto möglicherweise erhöht werden. Weitere Informationen finden Sie unter ROSA -Servicekontingente.

Lösung

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

   ```
   rosa verify quota
   ```

> **Note**
>
> Kontingente unterscheiden sich von Grund auf 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

Beschreibung

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.

Lösung

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>"
```

Beheben Sie Probleme mitROSA Nicht-STS-Clustern

In diesem Abschnitt erfahren Sie, wie Sie Probleme beheben, die bei der Bereitstellung vonROSA Nicht-STS-Clustern auftreten können.

Für einen besseren Sicherheitsschutz empfehlen wir,ROSA Cluster mit kurzlebigen AnmeldeinformationenAWS Security Token Service (STS) bereitzustellen. Weitere Informationen

zur Bereitstellung vonROSA STS-Clustern finden Sie unter Erste Schritte mitAWS STS derROSA Verwendung im auto Modus.

MitROSA können Sie auch Unterstützung bei der Fehlerbehebung vonAWS Support oder den Red Hat-Supportteams erhalten. Weitere Informationen finden Sie unter Support fürROSA.

Fehler beim Erstellen einesCluster mit einem osdCcsAdmin Fehler

> **Note**
>
> Dieser Fehler tritt nur auf, wenn Sie die Nicht-STS-Methode zur Bereitstellung vonROSA Clustern verwenden. Um dieses Problem zu vermeiden, stellen Sie IhreROSA Cluster mithilfe von bereitAWS STS. Weitere Informationen finden Sie unter Erste Schritte mitAWS STS derROSA Verwendung im auto Modus.

Beschreibung

Wenn dieCluster Erstellung nicht möglich ist, 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.
```

Lösung

1. Löschen Sie den Stack.

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

2. Initialisieren Sie Ihr Konto erneut.

   ```
   rosa init
   ```

Dokumentenverlauf für das ROSA Benutzerhandbuch

Die folgende Tabelle enthält alle Aktualisierungen der Dokumentation für ROSA.

Änderung	Beschreibung	Datum
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt im Nahen 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
ROSA aktualisiert NodePoolManagementPolicy	Die von AWS verwaltete Richtlinie ROSA wurde aktualisiertNodePoolManagementPolicy.	2. Mai 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt in Europa (Spanien) erhältlich. AWS-Region	29. April 2024
ROSA aktualisiert Installer Policy	Die von AWS verwaltete Richtlinie ROSA wurde aktualisiertInstallerPolicy.	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	17. April 2024

	(Osaka) erhältlich. AWS-Regio n	
ROSA InstallerPolicy und ROSSARE wurden aktualisiert SupportPolicy	Die von AWS verwalteten Richtlinien ROSA Installer Policy und SupportPolicy ROSSARE wurden aktualisi ert.	10. April 2024
ROSA mit HCP-Erweiterung AWS-Region	ROSA mit Hosted Control Planes (HCP) ist jetzt im asiatisch-pazifischen Raum (Hongkong) erhältlich. AWS-Region	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) erhältlich. AWS-Region	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

ROSA aktualisiert Installer Policy	Die von AWS verwaltete Richtlinie ROSA wurde aktualisiertInstallerPolicy.	26. Januar 2024
ROSSARE aktualisiert SupportPolicy	Die von AWS verwaltete Richtlinie SupportPolicy ROSSARE wurde aktualisiert.	22. Januar 2024
ROSA aktualisiert ImageRegistryOperatorPolicy	Die von AWS verwaltete Richtlinie ROSA wurde aktualisiertImageRegistryOperatorPolicy.	12. Dezember 2023
ROSA wurde aktualisiert KubeControllerPolicy	Die von AWS verwaltete Richtlinie ROSA wurde aktualisiertKubeControllerPolicy.	16. Oktober 2023
ROSA wurde aktualisiert ManageSubscription	Die von AWS verwaltete Richtlinie ROSA wurde aktualisiertManageSubscription.	1. August 2023
ROSA wurde aktualisiert KubeControllerPolicy	Die von AWS verwaltete Richtlinie ROSA wurde aktualisiertKubeControllerPolicy.	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 Bereitstellungsoptionen wurde hinzugefügt	Die Seite mit den Bereitstellungsoptionen wurde hinzugefügt.	9. Juni 2023

Neue AWS-verwaltete Richtlinie ROSA hinzugefügt NodePoolManagementPolicy	Die neue von AWS verwaltete Richtlinie ROSA NodePoolManagementPolicy wurde hinzugefügt.	08. Juni 2023
Neue AWS-verwaltete Richtlinie ROSA hinzugefügt InstallerPolicy	Die neue von AWS verwaltete Richtlinie ROSA InstallerPolicy wurde hinzugefügt.	6. Juni 2023
Neue AWS-verwaltete Richtlinie ROSSARE hinzugefügt SupportPolicy	Die neue AWS-verwaltete Richtlinie ROSSARE SupportPolicy 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 auf AWS?	Die Seite Was ist Red Hat OpenShift Service auf AWS aktualisiert.	24. Mai 2023
Neue von AWS verwaltete Richtlinien für ROSA-Operatorrollen hinzugefügt	Die neuen von AWS verwaltet en Richtlinien ROSA ImageRegistryOperatorPolicy KubeControllerPolicy, ROSA und ROSAKMS ProviderPolicy wurden hinzugefügt.	27. April 2023
Neue AWS-verwaltete Richtlinie ROSA hinzugefügt ControlPlaneOperatorPolicy	Die neue von AWS verwaltete Richtlinie ROSA ControlPlaneOperatorPolicy wurde hinzugefügt.	24. April 2023

Neue von AWS verwaltete Richtlinien für ROSA-Kontorollen hinzugefügt	Neue Seiten mit verwaltet en AWS-Richtlinien für das ROSA-Konto und die Seite mit Operatorrollen wurden hinzugefügt.	20. April 2023
Die Seite mit den ROSA-Servicekontingenten 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
Neue AWS-verwaltete Richtlinie ROSA hinzugefügt ManageSubscription	Die neue von AWS verwaltete Richtlinie ROSA ManageSubscription wurde hinzugefügt.	11. April 2022
Erstversion	Die erste Version des Red Hat OpenShift Service on 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.