Guide de l’utilisateur

Red Hat OpenShift Service on AWS

Red Hat OpenShift Service on AWS: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est Red Hat OpenShift Service on AWS ?

Red Hat OpenShift Service on AWS (ROSA) est un service géré que vous pouvez utiliser pour créer, dimensionner et déployer des applications conteneurisées avec la plateforme Red Hat OpenShift Enterprise Kubernetes. AWS ROSA rationalise le transfert des OpenShift charges de travail Red Hat sur site vers AWS les autres et offre une intégration étroite avec les autres. Services AWS

Caractéristiques

ROSA est soutenu et exploité conjointement par Red Hat AWS et Red Hat. Chaque ROSA cluster bénéficie de l'assistance d'un ingénieur en fiabilité des sites (SRE) Red Hat 24 heures sur 24 pour la gestion du cluster, conformément au contrat de niveau de service (SLA) de disponibilité de 99,95 % de Red Hat. Pour plus d'informations sur le modèle de support du service, consultezthe section called "Obtention de support".

ROSA fournit également les fonctionnalités suivantes :

- Installation de clusters, maintenance de clusters et mises à niveau de clusters prises en charge par Red Hat SRE.
- Service AWS les intégrations incluent le AWS calcul, les bases de données, l'analyse, l'apprentissage automatique, la mise en réseau et le mobile.
- Exécutez et dimensionnez le plan de contrôle Kubernetes sur plusieurs zones de AWS disponibilité pour garantir une haute disponibilité.
- Gérez des clusters à OpenShift APIs l'aide d'outils de productivité destinés aux développeurs, notamment Service Mesh, CodeReady Workspaces et Serverless.

Accès ROSA

Vous pouvez définir et configurer vos déploiements ROSA de services à l'aide des interfaces suivantes.

AWS

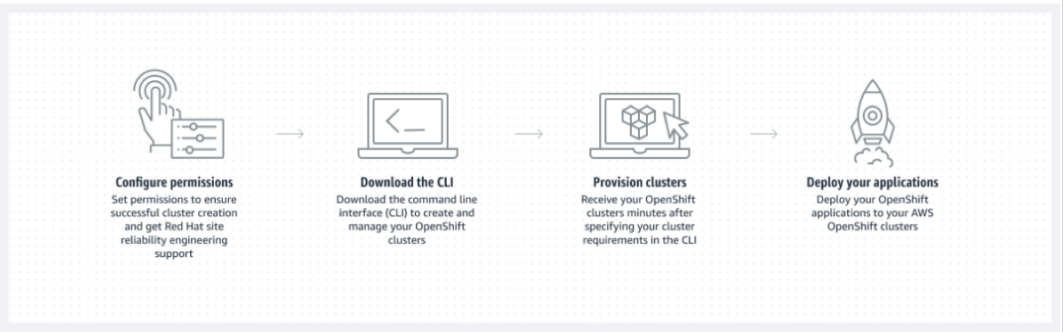
- ROSA console — Fournit une interface Web pour activer l' ROSA abonnement et acheter un contrat ROSA logiciel.

- AWS Command Line Interface (AWS CLI) — Fournit des commandes pour un large éventail de systèmes Services AWS et est compatible avec Windows, macOS et Linux. Pour de plus amples informations, veuillez consulter AWS Command Line Interface.

Chapeau rouge OpenShift

- Red Hat Hybrid Cloud Console : fournit une interface Web permettant de créer, de mettre à jour et de gérer des ROSA clusters, d'installer des modules complémentaires, ainsi que de créer et de déployer des applications sur un ROSA cluster.
- ROSA CLI (rosa) — Fournit des commandes pour créer, mettre à jour et gérer ROSA des clusters.
- OpenShift CLI (oc) — Fournit des commandes pour créer des applications et gérer des projets OpenShift Container Platform.
- CLI Knative (kn) - Fournit des commandes qui peuvent être utilisées pour interagir avec des composants OpenShift sans serveur, tels que Knative Serving et Eventing.
- CLI Pipelines (tkn) - Fournit des commandes pour interagir avec les OpenShift pipelines à l'aide du terminal.
- opm CLI - Fournit des commandes qui aident les développeurs d'opérateurs et les administrateurs de clusters à créer et à gérer des catalogues d' OpenShift opérateurs à partir du terminal.
- CLI du SDK opérateur : fournit des commandes qu'un développeur d'opérateurs peut utiliser pour créer, tester et déployer un OpenShift opérateur.

Comment démarrer avec ROSA



Voici un résumé du processus de démarrage pour ROSA. Pour obtenir des instructions de mise en route détaillées, voirCommencez avec ROSA .

AWS Management Console/AWS CLI

1. Configurer les autorisations pour Services AWS cela ROSA repose sur la fourniture des fonctionnalités du service. Pour de plus amples informations, veuillez consulter the section called "Conditions préalables".
2. Installez et configurez l' AWS CLI outil le plus récent. Pour plus d'informations, voir Installation ou mise à jour de la dernière version du AWS CLI dans le guide de AWS CLI l'utilisateur.
3. Activez ROSA dans la ROSA console.

ROSA Console/CLI pour le cloud hybride Red Hat

1. Téléchargez la dernière version de la ROSA CLI et de la OpenShift CLI depuis la Red Hat Hybrid Cloud Console. Pour plus d'informations, consultez Getting started with the ROSA CLI dans la documentation Red Hat.
2. Créez des ROSA clusters dans la console Red Hat Hybrid Cloud ou à l'aide de la ROSA CLI.
3. Lorsque votre cluster est prêt, configurez un fournisseur d'identité pour accorder aux utilisateurs l'accès au cluster.
4. Déployez et gérez les charges de travail sur votre ROSA cluster de la même manière que vous le feriez avec n'importe quel autre OpenShift environnement.

Tarification

Le coût total de ROSA comprend deux éléments : les frais de ROSA service et les frais AWS d'infrastructure. Pour plus d'informations sur la tarification, consultez Tarification d'Red Hat OpenShift Service on AWS.

ROSA frais de service

Par défaut, les frais de ROSA service s'accumulent sur demande à un taux horaire pour 4 vCPU utilisés par les nœuds de travail. Les frais de service sont uniformes dans toutes les régions AWS standard prises en charge. Outre les frais de service du nœud de travail, les clusters ROSA dotés de plans de contrôle hébergés (HCP) sont soumis à des frais de cluster horaires.

ROSA propose des contrats de frais de service d'un an et de 3 ans que vous pouvez acheter pour économiser sur les frais de service à la demande pour les nœuds de travail. Pour de plus amples informations, veuillez consulter the section called "Acheter un ROSA contrat".

AWS frais d'infrastructure

AWS les frais d'infrastructure s'appliquent aux nœuds de travail, aux nœuds d'infrastructure, aux nœuds du plan de contrôle, au stockage et aux ressources réseau sous-jacents hébergés sur l'infrastructure AWS mondiale. AWS les frais d'infrastructure varient selon Région AWS.

Vue d'ensemble des responsabilités pour ROSA

Cette documentation décrit les responsabilités de Amazon Web Services (AWS), de Red Hat et des clients en ce qui concerne le service géré Red Hat OpenShift Service on AWS (ROSA). Pour plus d'informations sur ROSA et ses composants, consultez la section Politiques et définition du service dans la documentation Red Hat.

Le modèle de responsabilitéAWS partagée définit la AWS responsabilité de protéger l'infrastructure qui gère tous les services proposés dans le AWS Cloud, y compris ROSA. AWS l'infrastructure inclut le matériel, les logiciels, les réseaux et les installations qui exécutent AWS Cloud les services. Cette AWS responsabilité est communément appelée « sécurité du cloud ». Pour fonctionner ROSA comme un service entièrement géré, Red Hat et le client sont responsables des éléments du service que le modèle de AWS responsabilité définit comme « la sécurité dans le cloud ».

Red Hat est responsable de la gestion et de la sécurité continues de l'infrastructure du ROSA cluster, de la plate-forme d'application sous-jacente et du système d'exploitation. Bien que les ROSA clusters soient hébergés sur les AWS ressources du client Comptes AWS, les composants du ROSA service et les ingénieurs de fiabilité des sites Red Hat (SREs) y accèdent à distance via IAM des rôles créés par le client. Red Hat utilise cet accès pour gérer le déploiement et la capacité de tous les nœuds du plan de contrôle et de l'infrastructure du cluster, et pour gérer les versions des nœuds du plan de contrôle, des nœuds d'infrastructure et des nœuds de travail.

Red Hat et le client partagent la responsabilité de la gestion du ROSA réseau, de la journalisation des clusters, du versionnement des clusters et de la gestion des capacités. Pendant que Red Hat gère le ROSA service, le client est entièrement responsable de la gestion et de la sécurisation des applications, des charges de travail et des données sur lesquelles il est déployé. ROSA

Présentation de

Le tableau suivant fournit une vue d'ensemble des AWS responsabilités de Red Hat et des clients en matière de Red Hat OpenShift Service on AWS.

> **Note**
>
> Si le `cluster-admin` rôle est ajouté à un utilisateur, consultez les responsabilités et les notes d'exclusion dans l'annexe 4 du contrat Red Hat Enterprise (Services d'abonnement en ligne).

Ressource	Gestion des incidents et des opérations	Gestion du changement	Autorisation d'accès et d'identité	Conformité à la sécurité et aux réglementations	Reprise après sinistre
Données du client	Client	Client	Client	Client	Client
Applications destinées aux clients	Client	Client	Client	Client	Client
Services aux développeurs	Client	Client	Client	Client	Client
Surveillance de la plateforme	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Journalisation	Red Hat	Red Hat et ses clients	Red Hat et ses clients	Red Hat et ses clients	Red Hat
Mise en réseau d'applications	Red Hat et ses clients	Red Hat et ses clients	Red Hat et ses clients	Red Hat	Red Hat
Mise en réseau de clusters	Red Hat	Red Hat et ses clients	Red Hat et ses clients	Red Hat	Red Hat

Ressource	Gestion des incidents et des opérations	Gestion du changement	Autorisation d'accès et d'identité	Conformité à la sécurité et aux réglementations	Reprise après sinistre
Gestion des réseaux virtuels	Red Hat et ses clients	Red Hat et ses clients	Red Hat et ses clients	Red Hat et ses clients	Red Hat et ses clients
Gestion informatique virtuelle (plan de contrôle, infrastructure et nœuds de travail)	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Version du cluster	Red Hat	Red Hat et ses clients	Red Hat	Red Hat	Red Hat
Gestion des capacités	Red Hat	Red Hat et ses clients	Red Hat	Red Hat	Red Hat
Gestion du stockage virtuel	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS logiciel (public Services AWS)	AWS	AWS	AWS	AWS	AWS
Matériel/ infrastructure mondiale AWS	AWS	AWS	AWS	AWS	AWS

Tâches à responsabilités partagées par domaine

AWS, Red Hat et les clients partagent la responsabilité de la surveillance et de la maintenance des ROSA composants. Cette documentation définit les responsabilités ROSA de service par domaine et par tâche.

Gestion des incidents et des opérations

AWS est chargé de protéger l'infrastructure matérielle qui exécute tous les services proposés dans le AWS Cloud. Red Hat est chargé de gérer les composants de service nécessaires à la mise en réseau de la plate-forme par défaut. Le client est responsable de la gestion des incidents et des opérations relatives aux données des applications client et de tout réseau personnalisé qu'il a pu configurer.

Ressource	Responsabilités liées au service	Responsabilités du client
Mise en réseau d'applications	Chapeau rouge • Surveillez OpenShift le service natif du routeur et répondez aux alertes.	Client • Surveillez l'état des routes applicatives et des points de terminaison qui les sous-tendent. • Signalez les pannes à Red Hat AWS et à Red Hat.
Gestion des réseaux virtuels	Chapeau rouge • Surveillez les équilibre urs de AWS charge, les Amazon VPC sous-rése aux et les Service AWS composants nécessaires à la mise en réseau de la plate-forme par défaut. Répondez aux alertes.	Client • Surveillez l'état des points de terminaison de l' AWS équilibreur de charge. • Surveillez le trafic réseau éventuellement configuré via une connexion au Amazon VPC VPC, Site-to-Site VPN une connexion ou Direct Connect pour détecter d'éventuels

Ressource	Responsabilités liées au service	Responsabilités du client
		problèmes ou menaces de sécurité.
Gestion du stockage virtuel	Chapeau rouge • Surveillez les Amazon EBS volumes utilisés pour les nœuds de cluster et les Amazon S3 compartim ents utilisés pour le registre d'images de conteneurs intégré au ROSA service. Répondez aux alertes.	Client • Surveillez l'état des données des applications. • Si des solutions gérées par le client AWS KMS keys sont utilisées, créez et contrôlez le cycle de vie des clés et les politiques clés pour Amazon EBS le chiffrement.
AWS logiciel (public Services AWS)	AWS • Pour plus d'informations sur la gestion des AWS incidents et des opération s, consultez la section Comment AWS maintenir la résilience opérationnelle et la continuité du service dans le AWS livre blanc.	Client • Surveillez l'état AWS des ressources du compte client. • Utilisez IAM les outils pour appliquer les autorisat ions appropriées aux AWS ressources du compte client.

Ressource	Responsabilités liées au service	Responsabilités du client
Matériel/infrastructure mondiale AWS	AWS • Pour plus d'informations sur la gestion des AWS incidents et des opération s, consultez la section Comment AWS maintenir la résilience opérationnelle et la continuité du service dans le AWS livre blanc.	Client • Configurez, gérez et surveillez les applications et les données des clients afin de garantir que les contrôles de sécurité des applicati ons et des données sont correctement appliqués.

Gestion des modifications

AWS est chargé de protéger l'infrastructure matérielle qui exécute tous les services proposés dans le AWS Cloud. Red Hat est chargé de permettre les modifications de l'infrastructure du cluster et des services que le client contrôlera, ainsi que de gérer les versions des nœuds du plan de contrôle, des nœuds d'infrastructure et des nœuds de travail. Le client est responsable de la mise en œuvre des modifications de l'infrastructure. Le client est également responsable de l'installation et de la maintenance des services optionnels, des configurations réseau sur le cluster et des modifications apportées aux données et aux applications du client.

Ressource	Responsabilités liées au service	Responsabilités du client
Journalisation	Chapeau rouge • Agrégez et surveillez de manière centralisée les journaux d'audit de la plateforme. • Fournir et gérer un opérateur de journalis ation pour permettre au client de déployer une pile	Client • Installez l'opérateur optionnel de journalisation des applications par défaut sur le cluster. • Installez, configurez et gérez toutes les solutions de journalisation d'applications facultatives, telles que la

Ressource	Responsabilités liées au service	Responsabilités du client
	de journalisation pour la journalisation des applications par défaut. • Fournissez des journaux d'audit à la demande du client.	journalisation de conteneurs annexes ou d'applications de journalisation tierces. • Ajustez la taille et la fréquence des journaux d'applications produits par les applications clientes s'ils affectent la stabilité de la pile de journalisation ou du cluster. • Demandez les journaux d'audit de la plateforme via un dossier d'assistance pour rechercher des incidents spécifiques.

Ressource	Responsabilités liées au service	Responsabilités du client
Mise en réseau d'applications	Chapeau rouge • Configurez des équilibreurs de charge publics. Offrez la possibilité de configurer des équilibreurs de charge privés et jusqu'à un équilibreur de charge supplémentaire en cas de besoin. • Configurez le service de OpenShift routeur natif. Offrez la possibilité de définir le routeur comme privé et d'ajouter jusqu'à une partition de routeur supplémentaire. • Installez, configurez et gérez les composants OpenShift SDN pour le trafic interne par défaut des pods. • Donnez au client la possibilité de gérer `NetworkPolicy` et `EgressNetworkPolicy` (de protéger) des objets.	Client • Configurez des autorisations réseau de pods autres que celles par défaut pour les réseaux de projets et de pods, l'entrée et la sortie de pods à l'aide d'objets. `NetworkPolicy` • Utilisez OpenShift Cluster Manager pour demander un équilibreur de charge privé pour les itinéraires d'application par défaut. • Utilisez OpenShift Cluster Manager pour configurer jusqu'à une partition de routeur publique ou privée supplémentaire et l'équilibreur de charge correspondant. • Demandez et configurez tout équilibreur de charge de service supplémentaire pour des services spécifiques. • Configurez les règles de transfert DNS nécessaires.

Ressource	Responsabilités liées au service	Responsabilités du client
Mise en réseau de clusters	Chapeau rouge • Configurez les composant s de gestion du cluster, tels que les points de terminais on de service publics ou privés et l'intégration nécessaire avec Amazon VPC les composants. • Configurez les composants réseau internes nécessaires à la communication interne du cluster entre les nœuds de travail, d'infrastructure et de plan de contrôle.	Client • Fournissez des plages d'adresses IP facultatives autres que celles par défaut pour le CIDR de la machine, le CIDR de service et le CIDR du pod si nécessair e via OpenShift Cluster Manager lors du provision nement du cluster. • Demandez que le point de terminaison du service API soit rendu public ou privé lors de la création du cluster ou après la création du OpenShift cluster via Cluster Manager.

Ressource	Responsabilités liées au service	Responsabilités du client
Gestion des réseaux virtuels	Chapeau rouge • Configurez et configure z Amazon VPC les composants nécessaires au provisionnement du cluster, tels que les sous-réseaux, les équilibreurs de charge, les passerelles Internet et les passerelles NAT. • Donnez au client la possibili té de gérer la Site-to-S ite VPN connectivité avec des ressources sur site, une connectivité vers un Amazon VPC VPC et, selon les besoins, via Direct Connect OpenShift Cluster Manager. • Permettez aux clients de créer et de déployer des équilibreurs de AWS charge à utiliser avec les équilibre urs de charge de service.	Client • Configurez et gérez Amazon VPC les composants optionnels, tels que la Amazon VPC connexion au VPC, la Site-to-Site VPN connexion ou. Direct Connect • Demandez et configurez des équilibreurs de charge supplémentaires pour des services spécifiques.

Ressource	Responsabilités liées au service	Responsabilités du client
Gestion du calcul virtuel	Chapeau rouge • Configurez et configurez le plan ROSA de contrôle et le plan de données pour utiliser Amazon EC2 des instances pour le calcul en cluster. • Surveillez et gérez le déploiement du plan de Amazon EC2 contrôle et des nœuds d'infrastructure sur le cluster.	Client • Surveillez et gérez les Amazon EC2 nœuds de travail en créant un pool de machines à l'aide du gestionnaire de OpenShift clusters ou de la ROSA CLI. • Gérez les modifications apportées aux applications déployées par les clients et aux données des applicati ons.
Version du cluster	Chapeau rouge • Activez le processus de planification des mises à niveau. • Surveillez la progression de la mise à niveau et corrigez les éventuels problèmes rencontrés. • Publiez des journaux des modifications et des notes de version pour les mises à niveau mineures et de maintenance.	Client • Planifiez les mises à niveau des versions de maintenan ce immédiatement, pour le futur, ou optez pour des mises à niveau automatiq ues. • Reconnaissez et planifiez les mises à niveau des versions mineures. • Assurez-vous que la version du cluster reste une version secondaire prise en charge. • Testez les applications des clients sur les versions mineures et de maintenan ce pour garantir la compatibi lité.

Ressource	Responsabilités liées au service	Responsabilités du client
Gestion des capacités	Chapeau rouge • Surveillez l'utilisation du plan de contrôle. Les plans de contrôle incluent les nœuds du plan de contrôle et les nœuds d'infrast ructure. • Faites évoluer et redimensi onnez les nœuds du plan de contrôle pour maintenir la qualité de service.	Client • Surveillez l'utilisation des nœuds de travail et, le cas échéant, activez la fonction de dimension nement automatique. • Déterminez la stratégie de mise à l'échelle du cluster. • Utilisez les commandes du gestionnaire de OpenShift clusters fournies pour ajouter ou supprimer des nœuds de travail supplémen taires selon les besoins. • Répondez aux notifications Red Hat concernant les besoins en ressources du cluster.

Ressource	Responsabilités liées au service	Responsabilités du client
Gestion du stockage virtuel	Chapeau rouge • Configurez et configure z Amazon EBS pour provisionner le stockage sur les nœuds locaux et le stockage en volume persistant pour le cluster. • Configurez et configurez le registre d'images intégré pour utiliser le stockage par Amazon S3 compartiments. • Régulièrement, optimisez les ressources du registre d'images Amazon S3 afin Amazon S3 d'optimiser l'utilisation et les performan ces du cluster.	Client • Configurez éventuellement le pilote Amazon EBS CSI ou le pilote Amazon EFS CSI pour provisionner des volumes persistants sur le cluster.

Ressource	Responsabilités liées au service	Responsabilités du client

AWS logiciels (AWS services publics)	AWS
	
	Calcul
	
	• Fournissez le Amazon EC2 service, utilisé pour le plan ROSA de contrôle, l'infrast ructure et les nœuds de travail.
	
	Stockage
	
	• Fournir Amazon EBS pour permettre au ROSA service de fournir un stockage sur nœud local et un stockage de volume persistant pour le cluster.
	
	Réseaux
	
	• Fournissez les AWS Cloud services suivants pour répondre aux besoins en infrastructure de réseau ROSA virtuel :
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• Fournissez les Service AWS intégrations facultatives suivantes pour ROSA :
	  • Site-to-Site VPN
		Client
		
		• Signez les demandes à l'aide d'un identifiant de clé d'accès et d'une clé d'accès secrète associés à un identifiant de sécurité IAM principal ou AWS STS temporaire.
		• Spécifiez les sous-rése aux VPC que le cluster doit utiliser lors de la création du cluster.
		• Configurez éventuellement un VPC géré par le client pour une utilisation avec des clusters. ROSA

Ressource	Responsabilités liées au service	Responsabilités du client
	• Direct Connect • AWS PrivateLink • AWS Transit Gateway	
Matériel/infrastructure mondiale AWS	AWS • Pour plus d'informations sur les contrôles de gestion AWS des centres de données, consultez Nos contrôles sur la page AWS Cloud Sécurité. • Pour plus d'informations sur les meilleures pratiques en matière de gestion des modifications, consultez les instructions relatives à la gestion des modifications AWS dans la bibliothèque de AWS solutions.	Client • Mettez en œuvre les meilleures pratiques de gestion du changement pour les applications clients et les données hébergées sur le AWS Cloud.

Autorisation d'accès et d'identité

L'autorisation d'accès et d'identité inclut les responsabilités relatives à la gestion de l'accès autorisé aux clusters, aux applications et aux ressources d'infrastructure. Cela inclut des tâches telles que la fourniture de mécanismes de contrôle d'accès, l'authentification, l'autorisation et la gestion de l'accès aux ressources.

Ressource	Responsabilités liées au service	Responsabilités du client
Journalisation	Chapeau rouge	Client

Ressource	Responsabilités liées au service	Responsabilités du client
	• Adhérez à un processus d'accès interne hiérarchisé basé sur les normes du secteur pour les journaux d'audit de la plateforme. • Fournissez des fonctionnalités OpenShift RBAC natives.	• Configurez le OpenShift RBAC pour contrôler l'accès aux projets et, par extension, aux journaux des applications d'un projet. • Pour les solutions de journalisation d'applications tierces ou personnalisées, le client est responsable de la gestion des accès.
Mise en réseau d'applications	Chapeau rouge • Fournissez un OpenShift RBAC et des `dedicated-admin` fonctionnalités natives.	Client • Configurez OpenShift `dedicated-admin` et RBAC pour contrôler l'accès à la configuration du routage selon les besoins. • Gérez les administrateurs de l'organisation Red Hat pour que Red Hat accorde l'accès à OpenShift Cluster Manager. Le gestionnaire de cluster est utilisé pour configurer les options du routeur et fournir un quota d'équilibreur de charge de service.

Ressource	Responsabilités liées au service	Responsabilités du client
Mise en réseau de clusters	Chapeau rouge • Fournissez des contrôles d'accès aux clients via OpenShift Cluster Manager. Fournissez un OpenShift RBAC et des `dedicated-admin` fonctionnalités natives.	Client • Configurez OpenShift `dedicated-admin` et RBAC pour contrôler l'accès à la configuration du routage selon les besoins. • Gérez l'adhésion des organisations Red Hat aux comptes Red Hat. • Gérez les administrateurs de l'organisation pour que Red Hat accorde l'accès à OpenShift Cluster Manager.
Gestion des réseaux virtuels	Chapeau rouge • Fournissez des contrôles d'accès aux clients via OpenShift Cluster Manager.	Client • Gérez l'accès utilisate ur facultatif aux AWS composants via OpenShift Cluster Manager.
Gestion du calcul virtuel	Chapeau rouge • Fournissez des contrôles d'accès aux clients via OpenShift Cluster Manager.	Client • Gérez l'accès utilisate ur facultatif aux AWS composants via OpenShift Cluster Manager. • Créez IAM les rôles et les politiques associées nécessaires pour permettre l'accès aux ROSA services.

Ressource	Responsabilités liées au service	Responsabilités du client
Gestion du stockage virtuel	Chapeau rouge • Fournissez des contrôles d'accès aux clients via OpenShift Cluster Manager.	Client • Gérez l'accès utilisate ur facultatif aux AWS composants via OpenShift Cluster Manager. • Créez IAM les rôles et les politiques associées nécessaires pour permettre l'accès aux ROSA services.

Ressource	Responsabilités liées au service	Responsabilités du client
AWS logiciels (AWS services publics)	AWS Calcul • Fournissez le Amazon EC2 service, utilisé pour le plan ROSA de contrôle, l'infrast ructure et les nœuds de travail. Stockage • Fournir Amazon EBS, utilisé pour permettre de ROSA provisionner le stockage sur les nœuds locaux et le stockage en volume persistant pour le cluster. • Amazon S3 Provide, utilisé pour le registre d'images intégré au service. Réseaux • Gestion des identités et des accès AWS Provide (IAM), utilisé par les clients pour contrôler l'accès aux ROSA ressources exécutées sur les comptes clients.	Client • Créez IAM les rôles et les politiques associées nécessaires pour permettre l'accès aux ROSA services. • Utilisez IAM les outils pour appliquer les autorisat ions appropriées aux AWS ressources du compte client. • Pour l'activer ROSA dans l'ensemble de votre AWS organisation, le client est responsable de la gestion des AWS Organizations administrateurs. • Pour l'activer ROSA dans l'ensemble de votre AWS organisation, le client est responsable de distribuer les ROSA droits accordés à l'aide AWS License Manager de.

Ressource	Responsabilités liées au service	Responsabilités du client
Matériel/infrastructure mondiale AWS	AWS • Pour plus d'informations sur les contrôles d'accès physiques pour les centres de AWS données, consultez Nos contrôles sur la page AWS Cloud Sécurité.	Client • Le client n'est pas responsable de l'infrast ructure AWS mondiale.

Conformité à la sécurité et aux réglementations

Les responsabilités et les contrôles liés à la conformité sont les suivants :

Ressource	Responsabilités liées au service	Responsabilités du client
Journalisation	Chapeau rouge • Envoyez les journaux d'audit du cluster à un système SIEM Red Hat pour qu'il analyse les événements de sécurité. Conservez les journaux d'audit pendant une période définie pour faciliter l'analyse médico-lé gale.	Client • Analysez les journaux des applications pour détecter les événements de sécurité. • Envoyez les journaux des applications à un point de terminaison externe via des conteneurs annexes ou des applications de journalis ation tierces si une durée de conservation plus longue que celle proposée par la pile de journalisation par défaut est requise.
Gestion des réseaux virtuels	Chapeau rouge	Client

Ressource	Responsabilités liées au service	Responsabilités du client
	• Surveillez les composant s du réseau virtuel pour détecter les problèmes potentiels et les menaces de sécurité. • Utilisez des AWS outils publics pour une surveilla nce et une protection supplémentaires.	• Surveillez les composants réseau virtuels configurés en option pour détecter les problèmes potentiels et les menaces de sécurité. • Configurez les règles de pare-feu ou les protectio ns du centre de données client nécessaires selon les besoins.
Gestion du calcul virtuel	Chapeau rouge • Surveillez les composant s informatiques virtuels pour détecter les problèmes potentiels et les menaces de sécurité. • Utilisez des AWS outils publics pour une surveilla nce et une protection supplémentaires.	Client • Surveillez les composants réseau virtuels configurés en option pour détecter les problèmes potentiels et les menaces de sécurité. • Configurez les règles de pare-feu ou les protectio ns du centre de données client nécessaires selon les besoins.

Ressource	Responsabilités liées au service	Responsabilités du client
Gestion du stockage virtuel	Chapeau rouge • Surveillez les composant s de stockage virtuel pour détecter les problèmes potentiels et les menaces de sécurité. • Utilisez des AWS outils publics pour une surveilla nce et une protection supplémentaires. • Configurez le ROSA service pour chiffrer les données du plan de contrôle, de l'infrast ructure et du volume des nœuds de travail par défaut à l'aide de la clé KMS AWS gérée qui Amazon EBS fournit. • Configurez le ROSA service pour chiffrer les volumes persistants des clients qui utilisent la classe de stockage par défaut à l'aide de la clé KMS AWS gérée qui Amazon EBS fournit. • Donnez au client la possibili té d'utiliser un client géré KMS key pour chiffrer les volumes persistants. • Configurez le registre d'images de conteneur pour chiffrer les données	Client • Amazon EBS Volumes de provision. • Gérez Amazon EBS le stockage en volume pour vous assurer que suffisamm ent de stockage est disponible pour le montage en tant que volume ROSA. • Créez la réclamation de volume persistant et générez un volume persistant via OpenShift Cluster Manager.

Ressource	Responsabilités liées au service	Responsabilités du client
	du registre d'images au repos à l'aide du chiffrement côté serveur avec des clés Amazon S3 gérées (SSE-3). • Donnez au client la possibilité de créer un registre d'images public ou privé Amazon S3 pour protéger ses images de conteneur contre tout accès non autorisé par des utilisateurs.	

Ressource	Responsabilités liées au service	Responsabilités du client
AWS logiciels (AWS services publics)	AWS Calcul • Fournir Amazon EC2, utilisé pour le plan ROSA de contrôle, l'infrastructure et les nœuds de travail. Pour plus d'informations, consultez la section Sécurité de l'infrastructure Amazon EC2 dans le Guide de Amazon EC2 l'utilisateur. Stockage • Provide Amazon EBS, utilisé pour les volumes du plan de ROSA contrôle, de l'infrastructure et des nœuds de travail, ainsi que pour les volumes persistan ts Kubernetes. Pour plus d'informations, consultez la section Protection des données Amazon EC2 dans le guide de Amazon EC2 l'utilisateur. • Provide AWS KMS, qui permet ROSA de chiffrer les volumes du plan de contrôle, de l'infrastructure, des nœuds de travail et des volumes persistants.	Client • Assurez-vous que les meilleures pratiques de sécurité et le principe du moindre privilège sont respectés pour protéger les données de l' Amazon EC2 instance. Pour plus d'informations, voir Sécurité de l'infrastructure dans Amazon EC2 et Protection des données dans Amazon EC2. • Surveillez les composants réseau virtuels configurés en option pour détecter les problèmes potentiels et les menaces de sécurité. • Configurez les règles de pare-feu ou les protectio ns du centre de données client nécessaires selon les besoins. • Créez une clé KMS optionnelle gérée par le client et chiffrez le volume Amazon EBS persistant à l'aide de la clé KMS. • Surveillez les données des clients dans le stockage virtuel pour détecter les problèmes potentiels et

Ressource	Responsabilités liées au service	Responsabilités du client
	Pour plus d'informations, consultez la section sur le Amazon EBS chiffrement dans le guide de Amazon EC2 l'utilisateur. • Amazon S3 Provide, utilisé pour le registre d'images de conteneurs intégré au service ROSA. Pour plus d'informations, consultez Amazon S3 la section sécurité dans le guide de Amazon S3 l'utilisateur. Réseaux • Fournissez des fonctionn alités et des services de sécurité pour améliorer la confidentialité et contrôler l'accès au réseau sur l'infrastructure AWS mondiale, notamment des pare-feux intégrés Amazon VPC, des connexions réseau privées ou dédiées, et le chiffrement automatiq ue de tout le trafic sur les réseaux AWS mondiaux et régionaux entre les installat ions AWS sécurisées. Pour plus d'informations, consultez le modèle de responsabilitéAWS partagée	les menaces de sécurité. Pour plus d'informations, consultez le Modèle de responsabilité partagée AWS.

Ressource	Responsabilités liées au service	Responsabilités du client
	et la sécurité de l'infrastructure dans le livre blanc Introduction à AWS la sécurité.	
Matériel/infrastructure mondiale AWS	AWS • Fournissez l'infrastructure AWS globale ROSA utilisée pour fournir des fonctionnalités de service. Pour plus d'informations sur les contrôles AWS de sécurité, consultez la section Sécurité de l' AWS infrastructure dans le AWS livre blanc. • Fournissez de la documentation au client pour qu'il puisse gérer ses besoins en matière de conformité et vérifier son état de sécurité à AWS l'aide d'outils tels que AWS Artifact AWS Security Hub.	Client • Configurez, gérez et surveillez les applications et les données des clients afin de garantir que les contrôles de sécurité des applications et des données sont correctement appliqués. • Utilisez IAM les outils pour appliquer les autorisations appropriées aux AWS ressources du compte client.

Reprise après sinistre

La reprise après sinistre inclut la sauvegarde des données et de la configuration, la réplication des données et la configuration de l'environnement de reprise après sinistre, ainsi que le basculement en cas de sinistre.

Ressource	Responsabilités liées au service	Responsabilités du client
Gestion des réseaux virtuels	Chapeau rouge • Restaurez ou recréez les composants réseau virtuels concernés qui sont nécessaires au fonctionn ement de la plate-forme.	Client • Configurez des connexion s réseau virtuelles avec plusieurs tunnels dans la mesure du possible pour vous protéger contre les pannes. • Conservez le DNS de basculement et l'équilibrage de charge si vous utilisez un équilibreur de charge global avec plusieurs clusters.
Gestion du calcul virtuel	Chapeau rouge • Surveillez le cluster et remplacez le plan Amazon EC2 de contrôle ou les nœuds d'infrastructure défaillants. • Donnez au client la possibili té de remplacer manuellem ent ou automatiquement les nœuds de travail défaillants.	Client • Remplacez les Amazon EC2 nœuds de travail défaillants en modifiant la configuration du pool de machines via OpenShift Cluster Manager ou la ROSA CLI.
Gestion du stockage virtuel	Chapeau rouge • Pour les ROSA clusters créés avec des informati ons d'identification AWS IAM utilisateur, sauvegardez tous les objets Kubernetes du cluster via des instantan	Client • Sauvegardez les applicati ons clients et les données des applications.

Ressource	Responsabilités liées au service	Responsabilités du client
	és de volume horaires, quotidiens et hebdomada ires.	

Ressource	Responsabilités liées au service	Responsabilités du client
AWS logiciels (AWS services publics)	AWS Calcul • Fournissez des Amazon EC2 fonctionnalités qui soutiennent la résilience des données, telles que les Amazon EBS instantan és et. Amazon EC2 Auto Scaling Pour plus d'informa tions, voir Resilience Amazon EC2 dans le guide de Amazon EC2 l'utilisateur. Stockage • Donnez au ROSA service et aux clients la possibilité de sauvegarder le Amazon EBS volume du cluster via des instantanés de Amazon EBS volume. • Pour plus d'informa tions sur les Amazon S3 fonctionnalités qui prennent en charge la résilience des données, consultez Resilience in Amazon S3. Réseaux • Pour plus d'informations sur les Amazon VPC fonctionn	Client • Configurez des clusters ROSA multi-AZ pour améliorer la tolérance aux pannes et la disponibilité des clusters. • Provisionnez des volumes persistants à l'aide du pilote Amazon EBS CSI pour activer les instantanés de volumes. • Créez des instantanés de volumes CSI de volumes Amazon EBS persistants.

Ressource	Responsabilités liées au service	Responsabilités du client
	alités qui prennent en charge la résilience des données, voir Résilience Amazon Virtual Private Cloud dans le guide de l' Amazon VPC utilisateur.	
Matériel/infrastructure mondiale AWS	AWS • Fournissez une infrastructure AWS globale qui permet ROSA de faire évoluer le plan de contrôle, l'infrastructure et les nœuds de travail entre les zones de disponibilité. Cette fonctionnalité permet d' ROSA orchestrer le basculement automatique entre les zones sans interruption. • Pour plus d'informations sur les meilleures pratiques de reprise après sinistre, consultez la section Options de reprise après sinistre dans le cloud dans le AWS Well-Architected Framework .	Client • Configurez des clusters ROSA multi-AZ pour améliorer la tolérance aux pannes et la disponibilité des clusters.

Responsabilités du client à l'égard des données et des applications

Le client est responsable des applications, des charges de travail et des données sur lesquelles il est déployé. Red Hat OpenShift Service on AWS Cependant, AWS Red Hat fournit divers outils pour aider le client à gérer les données et les applications sur la plate-forme.

Ressource	Comment AWS et Red Hat peut vous aider	Responsabilités du client
Données du client	Chapeau rouge • Respectez les normes de chiffrement des données au niveau de la plate-forme, telles que définies par les normes de sécurité et de conformité du secteur. • Fournissez OpenShift des composants pour aider à gérer les données des applications, telles que les secrets. • Activez l'intégration avec des services de données tels que Amazon RDS le stockage et la gestion des données en dehors du cluster et/ou AWS. AWS • Fournir Amazon RDS pour permettre aux clients de stocker et de gérer des données en dehors du cluster.	Client • Assumez la responsab ilité de toutes les données clients stockées sur la plateforme et de la manière dont les applications clients consomment et exposent ces données.
Applications destinées aux clients	Chapeau rouge • Provisionnez des clusters avec OpenShift des composants installés afin que les clients puissent	Client • Assumez la responsabilité des applications et des données des clients et des tiers, ainsi que du cycle de

Ressource	Comment AWS et Red Hat peut vous aider	Responsabilités du client
	accéder à Kubernetes OpenShift et APIs pour déployer et gérer des applications conteneurisées. • Créez des clusters avec des secrets d'extraction d'images afin que les déploiements des clients puissent extraire des images du registre Red Hat Container Catalog. • Fournissez un accès OpenShift APIs qu'un client peut utiliser pour configurer les opérateurs afin d'ajouter des services communaut aires AWS, tiers et Red Hat au cluster. • Fournissez des classes de stockage et des plug-ins pour prendre en charge les volumes persistants à utiliser avec les applications des clients. • Fournissez un registre d'images de conteneur afin que les clients puissent stocker en toute sécurité des images de conteneurs d'applications sur le cluster afin de déployer et de gérer des applications.	vie complet des applicati ons. • Si un client ajoute des services Red Hat, communautaires, tiers, ses propres services ou d'autres services au cluster à l'aide d'opérateurs ou d'images externes, il est responsable de ces services et de la collaboration avec le fournisseur approprié (y compris Red Hat) pour résoudre les problèmes éventuels. • Utilisez les outils et fonctionnalités fournis pour configurer et déployer, rester à jour, configurer les demandes et les limites de ressources, dimensionner le cluster afin de disposer de suffisamment de ressources pour exécuter des applicati ons, configurer les autorisat ions, intégrer d'autres services, gérer les flux d'images ou les modèles déployés par le client, servir en externe, enregistrer, sauvegarder et restaurer les données, et gérer autrement leurs charges de travail

Ressource	Comment AWS et Red Hat peut vous aider	Responsabilités du client
	AWS • Fournir Amazon EBS pour prendre en charge les volumes persistants à utiliser avec les applications des clients. • Fournir Amazon S3 pour prendre en charge le provisionnement par Red Hat du registre d'images de conteneurs.	hautement disponibles et résilientes. • Assumez la responsab ilité de la surveillance des applications exécutées Red Hat OpenShift Service on AWS, y compris de l'install ation et de l'exploitation de logiciels permettant de recueillir des métriques , de créer des alertes et de protéger les secrets de l'application.

ROSA architecture

Red Hat OpenShift Service on AWS (ROSA) possède les topologies de cluster suivantes :

- Plan de contrôle hébergé (HCP) : le plan de contrôle est hébergé par Red Hat Compte AWS et géré par Red Hat. Les nœuds de travail sont déployés chez le client Compte AWS.
- Classique — Le plan de contrôle et les nœuds de travail sont déployés chez le client Compte AWS.

ROSA avec HCP offre une architecture de plan de contrôle plus efficace qui permet de réduire les frais AWS d'infrastructure liés à l'exécution ROSA et d'accélérer les temps de création de clusters. ROSA avec HCP et ROSA classic peuvent être activés dans la AWS ROSA console. Vous avez le choix de sélectionner l'architecture que vous souhaitez utiliser lorsque vous provisionnez des ROSA clusters à l'aide de la ROSA CLI.

> **Note**
>
> ROSA avec plans de contrôle hébergés (HCP) propose les certifications de conformité FedRAMP High et HIPAA Qualified. Pour plus d'informations, consultez la section Conformité dans la documentation Red Hat.

Comparaison entre ROSA, HCP et ROSA classic

Le tableau suivant compare les modèles d'architecture ROSA aux modèles d'architecture classique HCP et ROSA.

	ROSA avec HCP	ROSA classique
Hébergement d'infrastructures de clusters	Les composants du plan de contrôle, tels que etcd, le serveur API et oauth, sont hébergés dans un environne ment appartenant à Red Hat. Compte AWS	Les composants du plan de contrôle, tels que etcd, le serveur d'API et oauth, sont hébergés dans un établisse ment appartenant au client. Compte AWS
Amazon VPC	Les nœuds de travail communiquent avec le plan de contrôle AWS PrivateLink.	Les nœuds de travail et les nœuds du plan de contrôle sont déployés dans le VPC du client.
Gestion des identités et des accès AWS	Utilise des politiques AWS gérées.	Utilise les politiques gérées par le client définies par le service.
Déploiement multizone	Le plan de contrôle est déployé sur plusieurs zones de disponibilité (AZs).	Le plan de contrôle peut être déployé au sein d'une seule zone d'exploitation ou sur plusieurs zones AZs.
Nœuds d'infrastructure	N'utilise pas de nœuds d'infrastructure dédiés. Les composants de la plate-forme	Utilise deux nœuds dédiés mono-AZ ou trois nœuds dédiés multi-AZ pour héberger

	ROSA avec HCP	ROSA classique
	sont déployés sur les nœuds de travail.	les composants de la plate-forme.
OpenShift capacités	La surveillance de la plate-forme, le registre d'images et le contrôleur d'entrée sont déployés dans les nœuds de travail.	La surveillance de la plate-forme, le registre d'images et le contrôleur d'entrée sont déployés dans des nœuds d'infrastructure dédiés.
Améliorations de clusters	Le plan de commande et chaque parc de machines peuvent être mis à niveau séparément.	L'ensemble du cluster doit être mis à niveau en même temps.
Amazon EC2 Encombrement minimal	Deux Amazon EC2 instances sont nécessaires pour créer un cluster.	Sept instances mono-AZ ou neuf Amazon EC2 instances multi-AZ sont nécessaires pour créer un cluster.
Régions AWS	Pour en Région AWS savoir plus sur la disponibilité, consultez la section Red Hat OpenShift Service on AWS Points de terminaison et quotas dans le Guide de référence AWS général.	Pour en Région AWS savoir plus sur la disponibilité, consultez la section Red Hat OpenShift Service on AWS Points de terminaison et quotas dans le Guide de référence AWS général.

Commencez avec ROSA

Red Hat OpenShift Service on AWS (ROSA) est un service géré que vous pouvez utiliser pour créer, dimensionner et déployer des applications conteneurisées avec la plateforme Red Hat OpenShift Enterprise Kubernetes. AWS

Vous pouvez utiliser les guides suivants pour créer votre premier ROSA cluster, accorder l'accès aux utilisateurs, déployer votre première application et apprendre à révoquer l'accès des utilisateurs et à supprimer votre cluster.

- the section called “Création d'un cluster ROSA HCP - CLI”- Créez votre premier cluster ROSA avec HCP à l'aide de AWS STS la ROSA CLI.
- the section called “Créez un cluster ROSA classic - AWS PrivateLink ”- Créez votre premier cluster ROSA Classic en utilisant AWS PrivateLink.
- the section called “Création d'un cluster classique ROSA - CLI”- Créez votre premier cluster ROSA Classic à l'aide AWS STS de la ROSA CLI.

Configurer pour utiliser ROSA

Pour préparer votre environnement à la création d'un ROSA cluster, vous devez effectuer les actions suivantes.

Conditions préalables

Les conditions préalables suivantes doivent être remplies pour permettre la création de ROSA clusters.

- Installez et configurez la dernière version AWS CLI. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI.
- Installez et configurez les dernières ROSA CLI et OpenShift Container Platform CLI. Pour plus d'informations, consultez Getting started with the ROSA CLI.
- Les quotas de service requis doivent être définis pour Amazon EC2 Amazon VPC, Amazon EBS, et Elastic Load Balancing. AWS ou Red Hat peut demander des augmentations de quota de service en votre nom, selon les besoins de résolution du problème. Pour consulter les quotas de service requis ROSA, consultez les Red Hat OpenShift Service on AWS points de terminaison et les quotas dans la référence AWS générale.

- Pour bénéficier de l' AWS assistance ROSA, vous devez activer les plans de support AWS Business, Enterprise On-Ramp ou Enterprise. Red Hat peut demander une AWS assistance en votre nom pour résoudre le problème. Pour de plus amples informations, veuillez consulter the section called “Obtention de support”. Pour l'activer Support, consultez la Support page.
- Si vous utilisez AWS Organizations pour gérer le service Comptes AWS qui héberge le ROSA service, la politique de contrôle des services (SCP) de l'organisation doit être configurée pour permettre à Red Hat d'exécuter les actions politiques répertoriées dans le SCP sans restriction. Pour de plus amples informations, veuillez consulter the section called “AWS Organizations la politique de contrôle des services refuse AWS Marketplace les autorisations requises”. Pour plus d'informations SCPs, voir Politiques de contrôle des services (SCPs).
- Si vous déployez un ROSA cluster jeton de sécurité AWS STS dans une région activée Région AWS désactivée par défaut, vous devez mettre à jour le jeton de sécurité vers la version 2 pour toutes les régions du à l' Compte AWS aide de la commande suivante.

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

  Pour plus d'informations sur l'activation des régions, consultez le lien : accounts/latest/reference/manage

Activer ROSA et configurer les AWS prérequis

Pour créer un ROSA cluster, vous devez activer le ROSA service dans la AWS ROSA console. La AWS ROSA console vérifie si vous disposez Compte AWS des AWS Marketplace autorisations nécessaires, des quotas de service et du nom du rôle lié au service Elastic Load Balancing (ELB). `AWSServiceRoleForElasticLoadBalancing` Si l'un de ces prérequis est absent, la console fournit des instructions sur la façon de configurer votre compte afin de répondre à ces prérequis.

1. Accédez à la console ROSA.
2. Choisissez Démarrer.
3. Sur la page Vérifier ROSA les conditions requises, sélectionnez J'accepte de partager mes informations de contact avec Red Hat.
4. Choisissez Activer ROSA .
5. Une fois que la page a vérifié que vos quotas de service répondent aux ROSA prérequis et que le rôle lié au service ELB est créé, ouvrez une nouvelle session de terminal pour créer votre première session à l'aide ROSA cluster de la CLI. ROSA

Créez un cluster ROSA avec HCP à l'aide de la ROSA CLI

Les sections suivantes décrivent comment démarrer avec ROSA avec des plans de contrôle hébergés (ROSA avec HCP) à l'aide AWS STS de la ROSA CLI. Pour savoir comment créer un cluster ROSA avec HCP à l'aide de Terraform, consultez la documentation Red Hat. Pour en savoir plus sur le fournisseur Terraform pour la création de ROSA clusters, consultez la documentation Terraform.

La ROSA CLI utilise le `auto` mode ou le `manual` mode pour créer les IAM ressources et la configuration OpenID Connect (OIDC) requises pour créer un. ROSA cluster`auto`le mode crée automatiquement les IAM rôles et politiques requis et le fournisseur OIDC. `manual`le mode affiche les AWS CLI commandes nécessaires pour créer les IAM ressources manuellement. En utilisant `manual` le mode, vous pouvez consulter les AWS CLI commandes générées avant de les exécuter manuellement. Avec `manual` le mode, vous pouvez également transmettre les commandes à un autre administrateur ou à un autre groupe de votre organisation afin qu'il puisse créer les ressources.

Les procédures décrites dans ce document utilisent le `auto` mode de la ROSA CLI pour créer les IAM ressources requises et la configuration OIDC pour ROSA avec HCP. Pour plus d'options de démarrage, consultezCommencez avec ROSA .

Rubriques

Conditions préalables

Effectuez les actions préalables répertoriées dansthe section called "Configuration".

Création d'une Amazon VPC architecture

La procédure suivante crée une Amazon VPC architecture qui peut être utilisée pour héberger un cluster. Toutes les cluster ressources sont hébergées dans le sous-réseau privé. Le sous-réseau public achemine le trafic sortant du sous-réseau privé via une passerelle NAT vers l'Internet public. Cet exemple utilise le bloc CIDR `10.0.0.0/16` pour le Amazon VPC. Vous pouvez toutefois choisir un autre bloc CIDR. Pour de plus amples informations, veuillez consulter Dimensionnement d'un VPC.

> **Important**
>
> Si Amazon VPC les exigences ne sont pas satisfaites, la création du cluster échoue.

Example

Terraform

1. Installez la CLI Terraform. Pour plus d'informations, consultez les instructions d'installation dans la documentation Terraform.
2. Ouvrez une session de terminal et clonez le référentiel VPC Terraform.

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

3. Accédez au répertoire créé.

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

4. Initiez le fichier Terraform.

   ```
   terraform init
   ```

   Une fois terminé, la CLI renvoie un message indiquant que Terraform a été initialisé avec succès.

5. Pour créer un plan Terraform basé sur le modèle existant, exécutez la commande suivante. Le Région AWS doit être spécifié. Vous pouvez éventuellement choisir de spécifier un nom de cluster.

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

   Une fois la commande exécutée, un `rosa.tfplan` fichier est ajouté au `hypershift-tf` répertoire. Pour des options plus détaillées, consultez le fichier README du référentiel Terraform VPC.

6. Appliquez le fichier de plan pour créer le VPC.

```
terraform apply rosa.tfplan
```

   Une fois l'opération terminée, la CLI a renvoyé un message de réussite qui vérifie les ressources ajoutées.

   a. (Facultatif) Créez des variables d'environnement pour le sous-réseau privé, public et machinepool approvisionné par Terraform à utiliser lors de la création de votre cluster ROSA avec IDs HCP.

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

   b. (Facultatif) Vérifiez que les variables d'environnement ont été correctement définies.

```
echo $SUBNET_IDS
```

Amazon VPC console

1. Ouvrez la Amazon VPC console.
2. Sur le tableau de bord VPC, choisissez Create VPC (Créer un VPC).
3. Sous Ressources à créer, choisissez VPC et plus encore.
4. Maintenez l'option Génération automatique de balise de nom sélectionnée pour créer des balises de nom pour les ressources VPC, ou désactivez-la pour fournir vos propres balises de nom pour les ressources VPC.
5. Pour le bloc IPv4 CIDR, entrez une plage d' IPv4 adresses pour le VPC. Un VPC doit avoir une plage d' IPv4 adresses.

6. (Facultatif) Pour prendre en charge IPv6 le trafic, choisissez le bloc IPv6 CIDR, le bloc CIDR fourni par Amazon IPv6 .
7. Laissez la location telle **`Default`** quelle.
8. Pour Nombre de zones de disponibilité (AZs), choisissez le nombre dont vous avez besoin. Pour les déploiements multi-AZ, ROSA trois zones de disponibilité sont nécessaires. Pour choisir le AZs pour vos sous-réseaux, développez Personnaliser AZs.

> **Note**
>
> Certains types d' ROSA instances ne sont disponibles que dans certaines zones de disponibilité. Vous pouvez utiliser la `rosa list instance-types` commande ROSA CLI pour répertorier tous les types d' ROSA instances disponibles. Pour vérifier si un type d'instance est disponible pour une zone de disponibilité donnée, utilisez la AWS CLI commande`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

9. Pour configurer vos sous-réseaux, choisissez des valeurs pour Nombre de sous-réseaux publics et Nombre de sous-réseaux privés. Pour choisir les plages d'adresses IP pour vos sous-réseaux, développez Personnaliser les blocs CIDR des sous-réseaux.

> **Note**
>
> ROSA avec HCP exige que les clients configurent au moins un sous-réseau public et privé par zone de disponibilité utilisée pour créer des clusters.

10. Pour accorder aux ressources du sous-réseau privé l'accès à l'Internet public via IPv4, pour les passerelles NAT, choisissez le nombre de AZs passerelles NAT à créer. En production, nous vous recommandons de déployer une passerelle NAT dans chaque zone de disponibilité avec des ressources nécessitant un accès à l'Internet public.
11. (Facultatif) Si vous devez accéder Amazon S3 directement depuis votre VPC, choisissez les points de terminaison du VPC, S3 Gateway.
12. Laissez les options DNS par défaut sélectionnées. ROSA nécessite la prise en charge du nom d'hôte DNS sur le VPC.

13. Développez les balises supplémentaires, choisissez Ajouter une nouvelle balise et ajoutez les clés de balise suivantes. ROSA utilise des contrôles automatisés avant le vol qui vérifient que ces balises sont utilisées.
    - Clé : `kubernetes.io/role/elb`
    - Clé : `kubernetes.io/role/internal-elb`
14. Sélectionnez Create VPC (Créer un VPC).

AWS CLI

1. Créez un VPC avec un bloc d'adresse CIDR `10.0.0.0/16`.

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

   La commande précédente renvoie l'ID du VPC. Voici un exemple de sortie.

```
vpc-1234567890abcdef0
```

2. Stockez l'ID du VPC dans une variable d'environnement.

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

3. Créez une `Name` balise pour le VPC à l'aide de la variable d'`VPC_ID`environnement.

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

4. Activez la prise en charge des noms d'hôte DNS sur le VPC.

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

5. Créez un sous-réseau public et privé dans le VPC, en spécifiant les zones de disponibilité dans lesquelles les ressources doivent être créées.

> **Important**
>
> ROSA avec HCP exige que les clients configurent au moins un sous-réseau public et privé par zone de disponibilité utilisée pour créer des clusters. Pour les déploiements multi-AZ, trois zones de disponibilité sont requises. Si ces conditions ne sont pas remplies, la création du cluster échoue.

> **Note**
>
> Certains types d' ROSA instances ne sont disponibles que dans certaines zones de disponibilité. Vous pouvez utiliser la `rosa list instance-types` commande ROSA CLI pour répertorier tous les types d' ROSA instances disponibles. Pour vérifier si un type d'instance est disponible pour une zone de disponibilité donnée, utilisez la AWS CLI commande`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

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

6. Stockez les sous-réseaux public et privé IDs dans des variables d'environnement.

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

7. Créez les balises suivantes pour vos sous-réseaux VPC. ROSA utilise des contrôles automatisés avant le vol qui vérifient que ces balises sont utilisées.

> **Note**
>
> Vous devez baliser au moins un sous-réseau privé et, le cas échéant, un sous-réseau public.

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

8. Créez une passerelle Internet et une table de routage pour le trafic sortant. Créez une table de routage et une adresse IP élastique pour le trafic privé.

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

9. Stockez les IDs dans les variables d'environnement.

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

10. Connectez la passerelle Internet au VPC.

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

11. Associez la table de routage publique au sous-réseau public et configurez le trafic pour qu'il soit acheminé vers la passerelle Internet.

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

12. Créez la passerelle NAT et associez-la à l'adresse IP élastique pour activer le trafic vers le sous-réseau privé.

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

13. Associez la table de routage privée au sous-réseau privé et configurez le trafic pour qu'il soit acheminé vers la passerelle NAT.

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

14. (Facultatif) Pour les déploiements multi-AZ, répétez les étapes ci-dessus pour configurer deux autres zones de disponibilité avec des sous-réseaux publics et privés.

Créez les IAM rôles requis et la configuration d'OpenID Connect

Avant de créer un cluster ROSA avec HCP, vous devez créer les IAM rôles et politiques nécessaires ainsi que la configuration OpenID Connect (OIDC). Pour plus d'informations sur IAM les rôles et les politiques de ROSA avec HCP, consultezthe section called " AWS politiques gérées".

Cette procédure utilise le `auto` mode de la ROSA CLI pour créer automatiquement la configuration OIDC nécessaire à la création d'un cluster ROSA avec HCP.

1. Créez les rôles et politiques de IAM compte requis. Le `--force-policy-creation` paramètre met à jour tous les rôles et politiques existants. Si aucun rôle ni aucune politique n'est présent, la commande crée ces ressources à la place.

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

> **Note**
>
> Si votre jeton d'accès hors ligne a expiré, la ROSA CLI affiche un message d'erreur indiquant que votre jeton d'autorisation doit être mis à jour. Pour connaître les étapes de résolution des problèmes, voirthe section called "Résoudre les problèmes liés aux jetons d'accès hors ligne expirés de la ROSA CLI".

2. Créez la configuration OpenID Connect (OIDC) qui permet l'authentification des utilisateurs auprès du cluster. Cette configuration est enregistrée pour être utilisée avec OpenShift Cluster Manager (OCM).

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

3. Copiez l'ID de configuration OIDC fourni dans la sortie de la ROSA CLI. L'ID de configuration OIDC doit être fourni ultérieurement pour créer le cluster ROSA avec HCP.
4. Pour vérifier les configurations OIDC disponibles pour les clusters associés à votre organisation d'utilisateurs, exécutez la commande suivante.

```
rosa list oidc-config
```

5. Créez les rôles d' IAM opérateur requis, en les `<OIDC_CONFIG_ID>` remplaçant par l'ID de configuration OIDC copié précédemment.

Example

> **Important**
>
> Vous devez fournir un préfixe <PREFIX_NAME> lors de la création des rôles d'opérateur. Si vous ne le faites pas, une erreur se produit.

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

6. Pour vérifier que les rôles d' IAM opérateur ont été créés, exécutez la commande suivante :

```
rosa list operator-roles
```

Créez un cluster ROSA avec HCP à l'aide de la ROSA CLI et AWS STS

Vous pouvez créer un ROSA avec HCP cluster en utilisant AWS Security Token Service (AWS STS) et le `auto` mode fourni dans la ROSA CLI. Vous avez la possibilité de créer un cluster avec une API publique et Ingress ou une API privée et Ingress.

Vous pouvez créer une cluster avec une seule zone de disponibilité (mono-AZ) ou plusieurs zones de disponibilité (multi-AZ). Dans les deux cas, la valeur CIDR de votre machine doit correspondre à la valeur CIDR de votre VPC.

La procédure suivante utilise la `rosa create cluster --hosted-cp` commande pour créer un ROSA mono-AZ avec HCP cluster. Pour créer un Multi-AZ cluster, spécifiez `multi-az` dans la commande et le sous-réseau privé IDs pour chaque sous-réseau privé sur lequel vous souhaitez effectuer le déploiement.

1. Créez un cluster ROSA avec HCP à l'aide de l'une des commandes suivantes.
   - Créez un cluster ROSA avec HCP avec une API publique et une entrée, en spécifiant le nom du cluster, le préfixe du rôle d'opérateur, l'ID de configuration OIDC et le sous-réseau public et privé. IDs

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

- Créez un cluster ROSA avec HCP avec une API privée et une entrée, en spécifiant le nom du cluster, le préfixe du rôle d'opérateur, l'ID de configuration OIDC et le sous-réseau privé. IDs

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

2. Vérifiez l'état de votre cluster.

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

> **Note**
>
> Si le processus de création échoue ou si le `State` champ ne passe pas à l'état « prêt » au bout de 10 minutes, consultezRésolution des problèmes.
> Pour contacter le support Red Hat Support ou obtenir de l'aide, consultezthe section called "Obtention de support".

3. Suivez la progression de la cluster création en consultant les journaux du OpenShift programme d'installation.

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

Configuration d'un fournisseur d'identité et autorisation cluster d'accès

ROSA inclut un OAuth serveur intégré. Une fois votre cluster identifiant créé, vous devez le configurer OAuth pour utiliser un fournisseur d'identité. Vous pouvez ensuite ajouter des utilisateurs à votre fournisseur d'identité configuré pour leur accorder l'accès à votre cluster. Vous pouvez accorder ces utilisateurs `cluster-admin` ou `dedicated-admin` autorisations selon les besoins.

Vous pouvez configurer différents types de fournisseurs d'identité pour votre ROSA cluster. Les types pris en charge incluent GitHub Enterprise GitHub GitLab, Google, LDAP, OpenID Connect et les fournisseurs HTPasswd d'identité.

> **Important**
>
> Le fournisseur HTPasswd d'identité est inclus uniquement pour permettre la création d'un seul utilisateur administrateur statique. HTPasswd n'est pas pris en charge en tant que fournisseur d'identité à usage général pour. ROSA

La procédure suivante configure un fournisseur d' GitHub identité à titre d'exemple. Pour obtenir des instructions sur la configuration de chacun des types de fournisseurs d'identité pris en charge, consultez la section Configuration des fournisseurs d'identité pour AWS STS.

1. Accédez à github.com et connectez-vous à votre GitHub compte.
2. Si vous n'avez aucune GitHub organisation à utiliser pour vous fournir des identités cluster, créez-en une. Pour plus d'informations, consultez les étapes décrites dans la GitHub documentation.
3. À l'aide du mode interactif de l' ROSA interface de ligne de commande, configurez un fournisseur d'identité pour votre cluster.

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

4. Suivez les instructions de configuration affichées dans le résultat pour restreindre cluster l'accès aux membres de votre GitHub organisation.

```
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. Ouvrez l'URL dans la sortie, en la <GITHUB_ORG_NAME> remplaçant par le nom de votre GitHub organisation.
6. Sur la page GitHub Web, choisissez Enregistrer une application pour enregistrer une nouvelle OAuth application dans votre GitHub organisation.
7. Utilisez les informations de la GitHub OAuth page pour remplir les autres invites `rosa create idp` interactives en exécutant la commande suivante. Remplacez <GITHUB_CLIENT_ID> et <GITHUB_CLIENT_SECRET> par les informations d'identification de votre GitHub OAuth application.

```
...
? 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**
>
> L'activation de la configuration du fournisseur d'identité peut prendre environ deux minutes. Si vous avez configuré un `cluster-admin` utilisateur, vous pouvez courir `oc get pods -n openshift-authentication --watch` pour regarder les OAuth pods se redéployer avec la configuration mise à jour.

8. Vérifiez que le fournisseur d'identité est correctement configuré.

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

Accorder à l'utilisateur l'accès à un cluster

Vous pouvez accorder à un utilisateur l'accès à votre cluster compte en l'ajoutant au fournisseur d'identité configuré.

La procédure suivante ajoute un utilisateur à une GitHub organisation configurée pour l'attribution d'identités au cluster.

1. Accédez à github.com et connectez-vous à votre GitHub compte.
2. Invitez les utilisateurs qui ont besoin cluster d'accéder à votre GitHub organisation. Pour plus d'informations, consultez la section Inviter des utilisateurs à rejoindre votre organisation dans la GitHub documentation.

Configurer les autorisations `cluster-admin`

1. Accordez les `cluster-admin` autorisations en exécutant la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et de cluster.

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

2. Vérifiez que l'utilisateur est répertorié comme membre du `cluster-admins` groupe.

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

Configurer les autorisations `dedicated-admin`

1. Accordez les `dedicated-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et votre cluster nom en exécutant la commande suivante.

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

2. Vérifiez que l'utilisateur est répertorié comme membre du `cluster-admins` groupe.

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

Accédez à un cluster via la console Red Hat Hybrid Cloud

Connectez-vous à votre compte cluster via la console Red Hat Hybrid Cloud.

1. Obtenez l'URL de la console correspondante cluster à l'aide de la commande suivante. Remplacez <CLUSTER_NAME> par le nom de votre cluster.

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

2. Accédez à l'URL de la console dans la sortie et connectez-vous.

   Dans la boîte de dialogue Se connecter avec..., choisissez le nom du fournisseur d'identité et complétez toutes les demandes d'autorisation présentées par votre fournisseur.

Déployer une application depuis le catalogue des développeurs

À partir de la console Red Hat Hybrid Cloud, vous pouvez déployer une application de test Developer Catalog et l'exposer à l'aide d'un itinéraire.

1. Accédez à Red Hat Hybrid Cloud Console et choisissez le cluster dans lequel vous souhaitez déployer l'application.
2. Sur la page du cluster, choisissez Ouvrir la console.
3. Du point de vue de l'administrateur, choisissez Accueil > Projets > Créer un projet.
4. Entrez un nom pour votre projet et ajoutez éventuellement un nom d'affichage et une description.
5. Choisissez Create pour créer le projet.
6. Passez au point de vue Développeur et choisissez +Ajouter. Assurez-vous que le projet sélectionné est bien celui qui vient d'être créé.
7. Dans la boîte de dialogue Developer Catalog, sélectionnez Tous les services.
8. Sur la page du catalogue pour développeurs, choisissez Langues > dans le JavaScriptmenu.
9. Choisissez Node.js, puis sélectionnez Créer une application pour ouvrir la page Créer Source-to-Image une application.

> **Note**
>
> Vous devrez peut-être choisir Effacer tous les filtres pour afficher l'option Node.js.

10. Dans la section Git, choisissez Try Sample.
11. Dans le champ Nom, ajoutez un nom unique.
12. Choisissez Créer.

> **Note**
>
> Le déploiement de la nouvelle application prend plusieurs minutes.

13. Lorsque le déploiement est terminé, choisissez l'URL de route pour l'application.

    Un nouvel onglet du navigateur s'ouvre avec un message similaire au suivant.

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

14. (Facultatif) Supprimez l'application et nettoyez les ressources :

    a. Du point de vue de l'administrateur, choisissez Accueil > Projets.

    b. Ouvrez le menu d'actions de votre projet et choisissez Supprimer le projet.

Révoquer **`cluster-admin`** les autorisations d'un utilisateur

1. Révoquez les `cluster-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et votre cluster nom.

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

2. Vérifiez que l'utilisateur n'est pas répertorié comme membre du `cluster-admins` groupe.

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

Révoquer **`dedicated-admin`** les autorisations d'un utilisateur

1. Révoquez les `dedicated-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et votre cluster nom.

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

2. Vérifiez que l'utilisateur n'est pas répertorié comme membre du `dedicated-admins` groupe.

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

Révoquer l'accès d'un utilisateur à un cluster

Vous pouvez révoquer cluster l'accès d'un utilisateur du fournisseur d'identité en le supprimant du fournisseur d'identité configuré.

Vous pouvez configurer différents types de fournisseurs d'identité pour votre cluster. La procédure suivante révoque cluster l'accès d'un membre d'une GitHub organisation.

1. Accédez à github.com et connectez-vous à votre GitHub compte.
2. Supprimez l'utilisateur de votre GitHub organisation. Pour plus d'informations, consultez la section Suppression d'un membre de votre organisation dans la GitHub documentation.

Supprimer un cluster et des AWS STS ressources

Vous pouvez utiliser la ROSA CLI pour supprimer un cluster qui utilise AWS Security Token Service (AWS STS). Vous pouvez également utiliser la ROSA CLI pour supprimer les IAM rôles et le fournisseur OIDC créés par ROSA. Pour supprimer les IAM politiques créées par ROSA, vous pouvez utiliser la IAM console.

> **Note**
>
> IAM les rôles et les politiques créés par ROSA peuvent être utilisés par d'autres ROSA clusters du même compte.

1. cluster Supprimez-les et observez les journaux. Remplacez <CLUSTER_NAME> par le nom ou l'identifiant de votre cluster.

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

> **Important**
>
> Vous devez attendre que la suppression cluster soit complète avant de supprimer les IAM rôles, les politiques et le fournisseur OIDC. Les rôles IAM du compte sont nécessaires pour supprimer les ressources créées par le programme d'installation. Les rôles IAM des opérateurs sont nécessaires pour nettoyer les ressources créées par les OpenShift opérateurs. Les opérateurs utilisent le fournisseur OIDC pour s'authentifier.

2. Supprimez le fournisseur OIDC que les cluster opérateurs utilisent pour s'authentifier en exécutant la commande suivante.

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

3. Supprimez les rôles d'opérateur spécifiques au cluster. IAM

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

4. Supprimez les rôles IAM du compte à l'aide de la commande suivante. `<PREFIX>`Remplacez-le par le préfixe du compte IAM roles à supprimer. Si vous avez spécifié un préfixe personnalisé lors de la création des rôles IAM du compte, spécifiez le préfixe par défaut`ManagedOpenShift`.

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

5. Supprimez les IAM politiques créées par ROSA.
   a. Connectez-vous à la console IAM.
   b. Dans le menu de gauche, sous Gestion des accès, sélectionnez Politiques.
   c. Sélectionnez la politique que vous souhaitez supprimer, puis sélectionnez Actions > Supprimer.
   d. Entrez le nom de la politique et choisissez Supprimer.
   e. Répétez cette étape pour supprimer chacune des politiques IAM pour le cluster.

Créez un cluster ROSA classic à l'aide de la ROSA CLI

Les sections suivantes décrivent comment démarrer avec ROSA Classic en utilisant AWS STS la ROSA CLI. Pour savoir comment créer un cluster ROSA Classic à l'aide de Terraform, consultez la documentation Red Hat. Pour en savoir plus sur le fournisseur Terraform pour la création de ROSA clusters, consultez la documentation Terraform.

La ROSA CLI utilise le `auto` mode ou le `manual` mode pour créer les IAM ressources nécessaires au provisionnement d'un ROSA cluster. `auto`le mode crée immédiatement les IAM rôles et les politiques requis ainsi qu'un fournisseur OpenID Connect (OIDC). `manual`le mode affiche les AWS CLI commandes nécessaires à la création des IAM ressources. En utilisant `manual` le mode, vous pouvez consulter les AWS CLI commandes générées avant de les exécuter manuellement. Avec `manual` le mode, vous pouvez également transmettre les commandes à un autre administrateur ou à un autre groupe de votre organisation afin qu'il puisse créer les ressources.

Pour plus d'options de démarrage, consultezCommencez avec ROSA .

Rubriques

Conditions préalables

Effectuez les actions préalables répertoriées dansthe section called “Configuration”.

Créez un cluster ROSA classic à l'aide de la ROSA CLI et AWS STS

Vous pouvez créer un classique ROSA à cluster l'aide de la ROSA CLI et AWS STS.

1. Créez les rôles et politiques de IAM compte requis à l'aide de `--mode auto` ou`--mode manual`.

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

     > **Note**
     >
     > Si votre jeton d'accès hors ligne a expiré, la ROSA CLI affiche un message d'erreur indiquant que votre jeton d'autorisation doit être mis à jour. Pour connaître les étapes de

résolution des problèmes, voirthe section called “Résoudre les problèmes liés aux jetons d'accès hors ligne expirés de la ROSA CLI”.

2. Créez un cluster en utilisant `--mode auto` ou`--mode manual`. `auto`le mode permet de créer un cluster plus rapidement. `manual`le mode vous invite à définir des paramètres personnalisés pour votre cluster.

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

  Note

  Lorsque vous le spécifiez`--mode auto`, la `rosa create cluster` commande crée automatiquement les IAM rôles d'opérateur spécifiques au cluster et le fournisseur OIDC. Les opérateurs utilisent le fournisseur OIDC pour s'authentifier.

  Note

  Lorsque vous utilisez les `--mode auto` valeurs par défaut, la dernière OpenShift version stable est installée.

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

  Important

  Si vous activez le chiffrement etcd en `manual` mode, vous encourez une surcharge de performance d'environ 20 %. La surcharge est due à l'introduction de cette deuxième couche de chiffrement, en plus du chiffrement Amazon EBS par défaut qui chiffre les volumes etcd.

> **Note**
>
> Après avoir exécuté le `manual` mode pour créer le cluster, vous devez créer manuellement les rôles IAM des opérateurs spécifiques au cluster et le fournisseur OpenID Connect que les opérateurs du cluster utilisent pour s'authentifier.

3. Vérifiez l'état de votre cluster.

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

> **Note**
>
> Si le processus de provisionnement échoue ou si le `State` champ ne passe pas à l'état « prêt » après 40 minutes, consultezRésolution des problèmes. Pour contacter le support Red Hat Support ou obtenir de l'aide, consultezthe section called "Obtention de support".

4. Suivez la progression de la cluster création en consultant les journaux du OpenShift programme d'installation.

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

Configuration d'un fournisseur d'identité et autorisation cluster d'accès

ROSA inclut un OAuth serveur intégré. Une fois votre cluster identifiant créé, vous devez le configurer OAuth pour utiliser un fournisseur d'identité. Vous pouvez ensuite ajouter des utilisateurs à votre fournisseur d'identité configuré pour leur accorder l'accès à votre cluster. Vous pouvez accorder ces utilisateurs `cluster-admin` ou `dedicated-admin` autorisations selon les besoins.

Vous pouvez configurer différents types de fournisseurs d'identité pour votre ROSA cluster. Les types pris en charge incluent GitHub Enterprise GitHub GitLab, Google, LDAP, OpenID Connect et les fournisseurs HTPasswd d'identité.

> **Important**
>
> Le fournisseur HTPasswd d'identité est inclus uniquement pour permettre la création d'un seul utilisateur administrateur statique. HTPasswd n'est pas pris en charge en tant que fournisseur d'identité à usage général pour. ROSA

La procédure suivante configure un fournisseur d' GitHub identité à titre d'exemple. Pour obtenir des instructions sur la configuration de chacun des types de fournisseurs d'identité pris en charge, consultez la section Configuration des fournisseurs d'identité pour AWS STS.

1. Accédez à github.com et connectez-vous à votre GitHub compte.
2. Si vous n'avez aucune GitHub organisation à utiliser pour vous fournir des identités cluster, créez-en une. Pour plus d'informations, consultez les étapes décrites dans la GitHub documentation.
3. À l'aide du mode interactif de l' ROSA interface de ligne de commande, configurez un fournisseur d'identité pour votre cluster.

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

4. Suivez les instructions de configuration affichées dans le résultat pour restreindre cluster l'accès aux membres de votre GitHub organisation.

```
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. Ouvrez l'URL dans la sortie, en la <GITHUB_ORG_NAME> remplaçant par le nom de votre GitHub organisation.
6. Sur la page GitHub Web, choisissez Enregistrer une application pour enregistrer une nouvelle OAuth application dans votre GitHub organisation.
7. Utilisez les informations de la GitHub OAuth page pour remplir les autres invites `rosa create idp` interactives en exécutant la commande suivante. Remplacez <GITHUB_CLIENT_ID> et <GITHUB_CLIENT_SECRET> par les informations d'identification de votre GitHub OAuth application.

```
...
? 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**
>
> L'activation de la configuration du fournisseur d'identité peut prendre environ deux minutes. Si vous avez configuré un `cluster-admin` utilisateur, vous pouvez courir `oc get pods -n openshift-authentication --watch` pour regarder les OAuth pods se redéployer avec la configuration mise à jour.

8. Vérifiez que le fournisseur d'identité est correctement configuré.

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

Accorder à l'utilisateur l'accès à un cluster

Vous pouvez accorder à un utilisateur l'accès à votre cluster compte en l'ajoutant au fournisseur d'identité configuré.

La procédure suivante ajoute un utilisateur à une GitHub organisation configurée pour l'attribution d'identités au cluster.

1. Accédez à github.com et connectez-vous à votre GitHub compte.
2. Invitez les utilisateurs qui ont besoin cluster d'accéder à votre GitHub organisation. Pour plus d'informations, consultez la section Inviter des utilisateurs à rejoindre votre organisation dans la GitHub documentation.

Configurer les autorisations `cluster-admin`

1. Accordez les `cluster-admin` autorisations en exécutant la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et de cluster.

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

2. Vérifiez que l'utilisateur est répertorié comme membre du `cluster-admins` groupe.

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

Configurer les autorisations `dedicated-admin`

1. Accordez les `dedicated-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et votre cluster nom en exécutant la commande suivante.

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

2. Vérifiez que l'utilisateur est répertorié comme membre du `cluster-admins` groupe.

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

Accédez à un cluster via la console Red Hat Hybrid Cloud

Après avoir créé un utilisateur cluster administrateur ou ajouté un utilisateur à votre fournisseur d'identité configuré, vous pouvez vous connecter à votre compte cluster via la Red Hat Hybrid Cloud Console.

1. Obtenez l'URL de la console correspondante cluster à l'aide de la commande suivante. Remplacez `<CLUSTER_NAME>` par le nom de votre cluster.

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

2. Accédez à l'URL de la console dans la sortie et connectez-vous.
   - Si vous avez créé un `cluster-admin` utilisateur, connectez-vous à l'aide des informations d'identification fournies.
   - Si vous avez configuré un fournisseur d'identité pour vous cluster, choisissez le nom du fournisseur d'identité dans la boîte de dialogue Se connecter avec... et répondez à toutes les demandes d'autorisation présentées par votre fournisseur.

Déployer une application depuis le catalogue des développeurs

À partir de la console Red Hat Hybrid Cloud, vous pouvez déployer une application de test Developer Catalog et l'exposer à l'aide d'un itinéraire.

1. Accédez à Red Hat Hybrid Cloud Console et choisissez le cluster dans lequel vous souhaitez déployer l'application.
2. Sur la page du cluster, choisissez Open console.
3. Du point de vue de l'administrateur, choisissez Accueil > Projets > Créer un projet.
4. Entrez un nom pour votre projet et ajoutez éventuellement un nom d'affichage et une description.
5. Choisissez Create pour créer le projet.
6. Passez au point de vue Développeur et choisissez +Ajouter. Assurez-vous que le projet sélectionné est bien celui qui vient d'être créé.
7. Dans la boîte de dialogue Developer Catalog, sélectionnez Tous les services.
8. Sur la page du catalogue pour développeurs, choisissez Langues > dans le JavaScriptmenu.
9. Choisissez Node.js, puis sélectionnez Créer une application pour ouvrir la page Créer Source-to-Image une application.

> **Note**
>
> Vous devrez peut-être choisir Effacer tous les filtres pour afficher l'option Node.js.

10. Dans la section Git, choisissez Try Sample.

11. Dans le champ Nom, ajoutez un nom unique.
12. Choisissez Créer.

> **Note**
>
> Le déploiement de la nouvelle application prend plusieurs minutes.

13. Lorsque le déploiement est terminé, choisissez l'URL de route pour l'application.

    Un nouvel onglet du navigateur s'ouvre avec un message similaire au suivant.

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

14. (Facultatif) Supprimez l'application et nettoyez les ressources :
    a. Du point de vue de l'administrateur, choisissez Accueil > Projets.
    b. Ouvrez le menu d'actions de votre projet et choisissez Supprimer le projet.

Révoquer **`cluster-admin`** les autorisations d'un utilisateur

1. Révoquez les `cluster-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et votre cluster nom.

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

2. Vérifiez que l'utilisateur n'est pas répertorié comme membre du `cluster-admins` groupe.

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

Révoquer **`dedicated-admin`** les autorisations d'un utilisateur

1. Révoquez les `dedicated-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et votre cluster nom.

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

2. Vérifiez que l'utilisateur n'est pas répertorié comme membre du `dedicated-admins` groupe.

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

Révoquer l'accès d'un utilisateur à un cluster

Vous pouvez révoquer cluster l'accès d'un utilisateur du fournisseur d'identité en le supprimant du fournisseur d'identité configuré.

Vous pouvez configurer différents types de fournisseurs d'identité pour votre cluster. La procédure suivante révoque cluster l'accès d'un membre d'une GitHub organisation.

1. Accédez à github.com et connectez-vous à votre GitHub compte.
2. Supprimez l'utilisateur de votre GitHub organisation. Pour plus d'informations, consultez la section Suppression d'un membre de votre organisation dans la GitHub documentation.

Supprimer un cluster et des AWS STS ressources

Vous pouvez utiliser la ROSA CLI pour supprimer un cluster qui utilise AWS Security Token Service (AWS STS). Vous pouvez également utiliser la ROSA CLI pour supprimer les IAM rôles et le fournisseur OIDC créés par ROSA. Pour supprimer les IAM politiques créées par ROSA, vous pouvez utiliser la IAM console.

> **Important**
>
> IAM les rôles et les politiques créés par ROSA peuvent être utilisés par d'autres ROSA clusters du même compte.

1. cluster Supprimez-les et observez les journaux. Remplacez <CLUSTER_NAME> par le nom ou l'identifiant de votre cluster.

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

> **Important**
>
> Vous devez attendre que la suppression cluster soit complète avant de supprimer les IAM rôles, les politiques et le fournisseur OIDC. Les rôles IAM du compte sont nécessaires

pour supprimer les ressources créées par le programme d'installation. Les rôles IAM des opérateurs sont nécessaires pour nettoyer les ressources créées par les OpenShift opérateurs. Les opérateurs utilisent le fournisseur OIDC pour s'authentifier.

2. Supprimez le fournisseur OIDC que les cluster opérateurs utilisent pour s'authentifier en exécutant la commande suivante.

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

3. Supprimez les rôles d'opérateur spécifiques au cluster. IAM

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

4. Supprimez les rôles IAM du compte à l'aide de la commande suivante. `<PREFIX>`Remplacez-le par le préfixe du compte IAM roles à supprimer. Si vous avez spécifié un préfixe personnalisé lors de la création des rôles IAM du compte, spécifiez le préfixe par défaut`ManagedOpenShift`.

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

5. Supprimez les IAM politiques créées par ROSA.
   a. Connectez-vous à la console IAM.
   b. Dans le menu de gauche, sous Gestion des accès, sélectionnez Politiques.
   c. Sélectionnez la politique que vous souhaitez supprimer, puis sélectionnez Actions > Supprimer.
   d. Entrez le nom de la politique et choisissez Supprimer.
   e. Répétez cette étape pour supprimer chacune des politiques IAM pour le cluster.

Créez un cluster ROSA classique qui utilise AWS PrivateLink

Les clusters ROSA Classic peuvent être déployés de différentes manières : en public, en privé ou en mode privé avec AWS PrivateLink. Pour plus d'informations sur ROSA classic, voirthe section called "Architecture". Pour les cluster configurations publiques et privées, ils OpenShift cluster ont accès à Internet et la confidentialité est définie sur les charges de travail des applications au niveau de la couche application.

Si vous souhaitez que les charges de travail cluster et les charges de travail des applications soient privées, vous pouvez les configurer AWS PrivateLink avec ROSA classic. AWS PrivateLink est une technologie hautement disponible et évolutive qui permet ROSA de créer une connexion privée

entre le ROSA service et les ressources du cluster dans le compte AWS client. L'équipe d' AWS PrivateLink ingénierie de fiabilité des sites (SRE) de Red Hat peut ainsi accéder au cluster à des fins de support et de correction en utilisant un sous-réseau privé connecté au point de terminaison du AWS PrivateLink cluster.

Pour plus d'informations AWS PrivateLink, voir Qu'est-ce que c'est AWS PrivateLink ?

Rubriques

Conditions préalables

Effectuez les actions préalables répertoriées dansthe section called “Configuration”.

Création d'une Amazon VPC architecture

La procédure suivante crée une Amazon VPC architecture qui peut être utilisée pour héberger un cluster. Toutes les cluster ressources sont hébergées dans le sous-réseau privé. Le sous-réseau public achemine le trafic sortant du sous-réseau privé via une passerelle NAT vers l'Internet public. Cet exemple utilise le bloc CIDR `10.0.0.0/16` pour le Amazon VPC. Cependant, vous pouvez

choisir un autre bloc CIDR. Pour de plus amples informations, veuillez consulter Dimensionnement d'un VPC.

> **Important**
>
> Si Amazon VPC les exigences ne sont pas satisfaites, la création du cluster échoue.

Example

Amazon VPC console

1. Ouvrez la Amazon VPC console.
2. Sur le tableau de bord VPC, choisissez Create VPC (Créer un VPC).
3. Sous Ressources à créer, choisissez VPC et plus encore.
4. Maintenez l'option Génération automatique de balise de nom sélectionnée pour créer des balises de nom pour les ressources VPC, ou désactivez-la pour fournir vos propres balises de nom pour les ressources VPC.
5. Pour le bloc IPv4 CIDR, entrez une plage d' IPv4 adresses pour le VPC. Un VPC doit avoir une plage d' IPv4 adresses.
6. (Facultatif) Pour prendre en charge IPv6 le trafic, choisissez le bloc IPv6 CIDR, le bloc CIDR fourni par Amazon IPv6 .
7. Laissez la location telle **`Default`** quelle.
8. Pour Nombre de zones de disponibilité (AZs), choisissez le nombre dont vous avez besoin. Pour les déploiements multi-AZ, ROSA trois zones de disponibilité sont nécessaires. Pour choisir le AZs pour vos sous-réseaux, développez Personnaliser AZs.

   > **Note**
   >
   > Certains types d' ROSA instances ne sont disponibles que dans certaines zones de disponibilité. Vous pouvez utiliser la `rosa list instance-types` commande ROSA CLI pour répertorier tous les types d' ROSA instances disponibles. Pour vérifier si un type d'instance est disponible pour une zone de disponibilité donnée, utilisez la AWS CLI commande`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters`

```
Name=location,Values=<availability_zone> --region <region> --
output text | egrep "<instance_type>".
```

9. Pour configurer vos sous-réseaux, choisissez des valeurs pour Nombre de sous-réseaux publics et Nombre de sous-réseaux privés. Pour choisir les plages d'adresses IP pour vos sous-réseaux, développez Personnaliser les blocs CIDR des sous-réseaux.

> **Note**
>
> ROSA exige que les clients configurent au moins un sous-réseau privé par zone de disponibilité utilisée pour créer des clusters.

10. Pour accorder aux ressources du sous-réseau privé l'accès à l'Internet public via IPv4, pour les passerelles NAT, choisissez le nombre de AZs passerelles NAT à créer. En production, nous vous recommandons de déployer une passerelle NAT dans chaque zone de disponibilité avec des ressources nécessitant un accès à l'Internet public.
11. (Facultatif) Si vous devez accéder Amazon S3 directement depuis votre VPC, choisissez les points de terminaison du VPC, S3 Gateway.
12. Laissez les options DNS par défaut sélectionnées. ROSA nécessite la prise en charge du nom d'hôte DNS sur le VPC.
13. Sélectionnez Create VPC (Créer un VPC).

AWS CLI

1. Créez un VPC avec un bloc d'adresse CIDR `10.0.0.0/16`.

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

La commande précédente renvoie l'ID du VPC. Voici un exemple de sortie.

```
vpc-1234567890abcdef0
```

2. Stockez l'ID du VPC dans une variable d'environnement.

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

3. Créez une `Name` balise pour le VPC à l'aide de la variable d'`VPC_ID`environnement.

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

4. Activez la prise en charge des noms d'hôte DNS sur le VPC.

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

5. Créez un sous-réseau public et privé dans le VPC, en spécifiant les zones de disponibilité dans lesquelles les ressources doivent être créées.

> **Important**
>
> ROSA exige que les clients configurent au moins un sous-réseau privé par zone de disponibilité utilisée pour créer des clusters. Pour les déploiements multi-AZ, trois zones de disponibilité sont requises. Si ces exigences ne sont pas satisfaites, la création du cluster échoue.

> **Note**
>
> Certains types d' ROSA instances ne sont disponibles que dans certaines zones de disponibilité. Vous pouvez utiliser la `rosa list instance-types` commande ROSA CLI pour répertorier tous les types d' ROSA instances disponibles. Pour vérifier si un type d'instance est disponible pour une zone de disponibilité donnée, utilisez la AWS CLI commande`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
```

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

6. Stockez les sous-réseaux public et privé IDs dans des variables d'environnement.

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

7. Créez une passerelle Internet et une table de routage pour le trafic sortant. Créez une table de routage et une adresse IP élastique pour le trafic privé.

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

8. Stockez les IDs dans les variables d'environnement.

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

9. Connectez la passerelle Internet au VPC.

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

10. Associez la table de routage publique au sous-réseau public et configurez le trafic pour qu'il soit acheminé vers la passerelle Internet.

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

11. Créez la passerelle NAT et associez-la à l'adresse IP élastique pour activer le trafic vers le sous-réseau privé.

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

12. Associez la table de routage privée au sous-réseau privé et configurez le trafic pour qu'il soit acheminé vers la passerelle NAT.

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

13. (Facultatif) Pour les déploiements multi-AZ, répétez les étapes ci-dessus pour configurer deux autres zones de disponibilité avec des sous-réseaux publics et privés.

Créez un cluster ROSA classic à l'aide de la ROSA CLI et AWS PrivateLink

Vous pouvez utiliser la ROSA CLI AWS PrivateLink pour créer une zone cluster de disponibilité unique (mono-AZ) ou plusieurs zones de disponibilité (multi-AZ). Dans les deux cas, la valeur CIDR de votre machine doit correspondre à la valeur CIDR de votre VPC.

La procédure suivante utilise la `rosa create cluster` commande pour créer un ROSA classic cluster. Pour créer un Multi-AZ cluster, spécifiez-le `--multi-az` dans la commande, puis sélectionnez le sous-réseau privé IDs que vous souhaitez utiliser lorsque vous y êtes invité.

> **Note**
>
> Si vous utilisez un pare-feu, vous devez le configurer de manière à ROSA pouvoir accéder aux sites dont il a besoin pour fonctionner.
> Pour plus d'informations, consultez la section Exigences relatives à l'utilisation des AWS PrivateLink clusters dans la documentation Red Hat.

1. Créez les rôles et politiques de IAM compte requis à l'aide de `--mode auto` ou`--mode manual`.
   -
     ```
     rosa create account-roles --classic --mode auto
     ```
   -
     ```
     rosa create account-roles --classic --mode manual
     ```

     > **Note**
     >
     > Si votre jeton d'accès hors ligne a expiré, la ROSA CLI affiche un message d'erreur indiquant que votre jeton d'autorisation doit être mis à jour. Pour connaître les étapes à suivre pour résoudre les problèmes, consultezthe section called “Résoudre les problèmes liés aux jetons d'accès hors ligne expirés de la ROSA CLI”.
2. Créez un cluster en exécutant l'une des commandes suivantes.
   - Mono-AZ

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

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

> **Note**
>
> Pour créer un cluster qui utilise des informations d'identification de courte durée AWS PrivateLink with AWS Security Token Service (AWS STS), ajoutez `--sts --mode auto` ou `--sts --mode manual` à la fin de la `rosa create cluster` commande.

3. Créez les IAM rôles d' cluster opérateur en suivant les instructions interactives.

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

4. Créez le fournisseur OpenID Connect (OIDC) que les cluster opérateurs utilisent pour s'authentifier.

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

5. Vérifiez l'état de votre cluster.

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

> **Note**
>
> L'affichage du `ready` statut dans le cluster `State` champ peut prendre jusqu'à 40 minutes. Si le provisionnement échoue ou ne s'affiche pas au `ready` bout de 40 minutes, consultezRésolution des problèmes. Pour contacter le support Red Hat Support ou obtenir de l'aide, consultezthe section called “Obtention de support”.

6. Suivez la progression de la cluster création en consultant les journaux du OpenShift programme d'installation.

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

Configurer le transfert AWS PrivateLink DNS

Les clusters utilisés AWS PrivateLink créent une zone hébergée publique et une zone hébergée privée dans Route 53. Les enregistrements de la zone hébergée Route 53 privée ne peuvent être résolus que depuis le VPC auquel ils sont assignés.

La validation Let's Encrypt DNS-01 nécessite une zone publique afin que des certificats valides et approuvés par le public puissent être émis pour le domaine. Les enregistrements de validation sont supprimés une fois la validation de Let's Encrypt terminée. La zone est toujours requise pour la délivrance et le renouvellement de ces certificats, qui sont généralement requis tous les 60 jours. Bien que ces zones semblent généralement vides, une zone publique joue un rôle essentiel dans le processus de validation.

Pour plus d'informations sur les zones hébergées AWS privées, consultez la section Utilisation des zones privées. Pour plus d'informations sur les zones hébergées publiques, consultez la section Utilisation des zones hébergées publiques.

Configuration d'un point de Route 53 Resolver terminaison entrant

1. Pour autoriser des enregistrements tels que `api.<cluster_domain>` et pour les `*.apps.<cluster_domain>` résoudre en dehors du VPC, configurez un point de terminaison Route 53 Resolver entrant.

   > **Note**
   >
   > Lorsque vous configurez un point de terminaison entrant, vous devez spécifier au moins deux adresses IP à des fins de redondance. Nous vous recommandons de spécifier des adresses IP dans au moins deux zones de disponibilité. Si vous le souhaitez, vous pouvez spécifier des adresses IP supplémentaires dans ces zones de disponibilité ou dans d'autres.

2. Lorsque vous configurez le point de terminaison entrant, sélectionnez le VPC et les sous-réseaux privés utilisés lors de la création du cluster.

Configurer le transfert DNS pour le cluster

Une fois le point de terminaison Route 53 Resolver interne associé et opérationnel, configurez le transfert DNS afin que les requêtes DNS puissent être traitées par les serveurs désignés sur votre réseau.

1. Configurez votre réseau d'entreprise pour transférer les requêtes DNS vers les adresses IP du domaine de premier niveau, telles que`drow-pl-01.htno.p1.openshiftapps.com`.
2. Si vous transférez des requêtes DNS d'un VPC à un autre VPC, suivez les instructions de la section Gestion des règles de transfert.
3. Si vous configurez le serveur DNS de votre réseau distant, consultez la documentation de votre serveur DNS spécifique pour configurer le transfert DNS sélectif pour le domaine de cluster installé.

Configuration d'un fournisseur d'identité et autorisation cluster d'accès

ROSA inclut un OAuth serveur intégré. Une fois votre ROSA cluster identifiant créé, vous devez le configurer OAuth pour utiliser un fournisseur d'identité. Vous pouvez ensuite ajouter des utilisateurs à votre fournisseur d'identité configuré pour leur accorder l'accès à votre cluster. Vous pouvez accorder ces utilisateurs `cluster-admin` ou `dedicated-admin` autorisations selon les besoins.

Vous pouvez configurer différents types de fournisseurs d'identité pour votre cluster. Les types pris en charge incluent GitHub Enterprise GitHub, Google GitLab, LDAP, OpenID Connect et les fournisseurs HTPasswd d'identité.

> **Important**
>
> Le fournisseur HTPasswd d'identité est inclus uniquement pour permettre la création d'un seul utilisateur administrateur statique. HTPasswd n'est pas pris en charge en tant que fournisseur d'identité à usage général pour. ROSA

La procédure suivante configure un fournisseur d' GitHub identité à titre d'exemple. Pour obtenir des instructions sur la configuration de chacun des types de fournisseurs d'identité pris en charge, consultez la section Configuration des fournisseurs d'identité pour AWS STS.

1. Accédez à github.com et connectez-vous à votre GitHub compte.
2. Si vous n'avez aucune GitHub organisation à utiliser pour vous fournir des identités ROSA cluster, créez-en une. Pour plus d'informations, consultez les étapes décrites dans la GitHub documentation.
3. À l'aide du mode interactif de l' ROSA interface de ligne de commande, configurez un fournisseur d'identité pour votre cluster en exécutant la commande suivante.

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

4. Suivez les instructions de configuration affichées dans le résultat pour restreindre cluster l'accès aux membres de votre GitHub organisation.

```
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. Ouvrez l'URL dans la sortie, en la `<GITHUB_ORG_NAME>` remplaçant par le nom de votre GitHub organisation.
6. Sur la page GitHub Web, choisissez Enregistrer une application pour enregistrer une nouvelle OAuth application dans votre GitHub organisation.
7. Utilisez les informations de la GitHub OAuth page pour remplir les autres invites `rosa create idp` interactives, en remplaçant `<GITHUB_CLIENT_ID>` et `<GITHUB_CLIENT_SECRET>` par les informations d'identification de votre GitHub OAuth application.

```
...
? 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**
>
> L'activation de la configuration du fournisseur d'identité peut prendre environ deux minutes. Si vous avez configuré un `cluster-admin` utilisateur, vous pouvez exécuter la `oc get pods -n openshift-authentication --watch` commande pour voir les OAuth pods se redéployer avec la configuration mise à jour.

8. Vérifiez que le fournisseur d'identité a été correctement configuré.

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

Accorder à l'utilisateur l'accès à un cluster

Vous pouvez accorder à un utilisateur l'accès à votre cluster compte en l'ajoutant au fournisseur d'identité configuré.

La procédure suivante ajoute un utilisateur à une GitHub organisation configurée pour l'attribution d'identités au cluster.

1. Accédez à github.com et connectez-vous à votre GitHub compte.
2. Invitez les utilisateurs qui ont besoin cluster d'accéder à votre GitHub organisation. Pour plus d'informations, consultez la section Inviter des utilisateurs à rejoindre votre organisation dans la GitHub documentation.

Configurer les autorisations **`cluster-admin`**

1. Accordez les `cluster-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et de cluster.

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

2. Vérifiez que l'utilisateur est répertorié comme membre du `cluster-admins` groupe.

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

Configurer les autorisations `dedicated-admin`

1. Accordez les `dedicated-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et votre cluster nom.

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

2. Vérifiez que l'utilisateur est répertorié comme membre du `cluster-admins` groupe.

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

Accédez à un cluster via la console Red Hat Hybrid Cloud

Après avoir créé un utilisateur cluster administrateur ou ajouté un utilisateur à votre fournisseur d'identité configuré, vous pouvez vous connecter à votre compte cluster via la Red Hat Hybrid Cloud Console.

1. Obtenez l'URL de la console correspondante cluster à l'aide de la commande suivante. Remplacez `<CLUSTER_NAME>` par le nom de votre cluster.

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

2. Accédez à l'URL de la console dans la sortie et connectez-vous.
   - Si vous avez créé un `cluster-admin` utilisateur, connectez-vous à l'aide des informations d'identification fournies.
   - Si vous avez configuré un fournisseur d'identité pour vous cluster, choisissez le nom du fournisseur d'identité dans la boîte de dialogue Se connecter avec... et répondez à toutes les demandes d'autorisation présentées par votre fournisseur.

Déployer une application depuis le catalogue des développeurs

À partir de la console Red Hat Hybrid Cloud, vous pouvez déployer une application de test Developer Catalog et l'exposer à l'aide d'un itinéraire.

1. Accédez à Red Hat Hybrid Cloud Console et choisissez le cluster dans lequel vous souhaitez déployer l'application.
2. Sur la page du cluster, choisissez Ouvrir la console.
3. Du point de vue de l'administrateur, choisissez Accueil > Projets > Créer un projet.
4. Entrez un nom pour votre projet et ajoutez éventuellement un nom d'affichage et une description.
5. Choisissez Create pour créer le projet.
6. Passez au point de vue Développeur et choisissez +Ajouter. Assurez-vous que le projet sélectionné est bien celui qui vient d'être créé.
7. Dans la boîte de dialogue Developer Catalog, sélectionnez Tous les services.
8. Sur la page du catalogue pour développeurs, choisissez Langues > dans le JavaScriptmenu.
9. Choisissez Node.js, puis sélectionnez Créer une application pour ouvrir la page Créer Source-to-Image une application.

> **Note**
>
> Vous devrez peut-être choisir Effacer tous les filtres pour afficher l'option Node.js.

10. Dans la section Git, choisissez Try Sample.
11. Dans le champ Nom, ajoutez un nom unique.
12. Choisissez Créer.

> **Note**
>
> Le déploiement de la nouvelle application prend plusieurs minutes.

13. Lorsque le déploiement est terminé, choisissez l'URL de route pour l'application.

    Un nouvel onglet du navigateur s'ouvre avec un message similaire au suivant.

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

14. (Facultatif) Supprimez l'application et nettoyez les ressources.
    a. Du point de vue de l'administrateur, choisissez Accueil > Projets.
    b. Ouvrez le menu d'actions de votre projet et choisissez Supprimer le projet.

Révoquer **`cluster-admin`** les autorisations d'un utilisateur

1. Révoquez les `cluster-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et votre cluster nom.

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

2. Vérifiez que l'utilisateur n'est pas répertorié comme membre du `cluster-admins` groupe.

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

Révoquer **`dedicated-admin`** les autorisations d'un utilisateur

1. Révoquez les `dedicated-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre nom d'utilisateur et votre cluster nom.

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

2. Vérifiez que l'utilisateur n'est pas répertorié comme membre du `dedicated-admins` groupe.

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

Révoquer l'accès d'un utilisateur à un cluster

Vous pouvez révoquer cluster l'accès d'un utilisateur du fournisseur d'identité en le supprimant du fournisseur d'identité configuré.

Vous pouvez configurer différents types de fournisseurs d'identité pour votre cluster. La procédure suivante révoque cluster l'accès d'un membre d'une GitHub organisation.

1. Accédez à github.com et connectez-vous à votre GitHub compte.
2. Supprimez l'utilisateur de votre GitHub organisation. Pour plus d'informations, consultez la section Suppression d'un membre de votre organisation dans la GitHub documentation.

Supprimer un cluster et des AWS STS ressources

Vous pouvez utiliser la ROSA CLI pour supprimer un cluster qui utilise AWS Security Token Service (AWS STS). Vous pouvez également utiliser la ROSA CLI pour supprimer les IAM rôles et le fournisseur OIDC créés par ROSA. Pour supprimer les IAM politiques créées par ROSA, vous pouvez utiliser la IAM console.

> **Important**
>
> IAM les rôles et les politiques créés par ROSA peuvent être utilisés par d'autres ROSA clusters du même compte.

1. cluster Supprimez-les et observez les journaux. Remplacez `<CLUSTER_NAME>` par le nom ou l'identifiant de votre cluster.

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

> **Important**
>
> Vous devez attendre que la suppression cluster soit complète avant de supprimer les IAM rôles, les politiques et le fournisseur OIDC. Les rôles IAM du compte sont nécessaires pour supprimer les ressources créées par le programme d'installation. Les rôles IAM des opérateurs sont nécessaires pour nettoyer les ressources créées par les OpenShift opérateurs. Les opérateurs utilisent le fournisseur OIDC pour s'authentifier.

2. Supprimez le fournisseur OIDC que les cluster opérateurs utilisent pour s'authentifier en exécutant la commande suivante.

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

3. Supprimez les rôles d'opérateur spécifiques au cluster. IAM

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

4. Supprimez les rôles IAM du compte à l'aide de la commande suivante. `<PREFIX>`Remplacez-le par le préfixe du compte IAM roles à supprimer. Si vous avez spécifié un préfixe personnalisé lors de la création des rôles IAM du compte, spécifiez le préfixe par défaut`ManagedOpenShift`.

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

5. Supprimez les IAM politiques créées par ROSA.
   a. Connectez-vous à la console IAM.
   b. Dans le menu de gauche, sous Gestion des accès, sélectionnez Politiques.
   c. Sélectionnez la politique que vous souhaitez supprimer, puis sélectionnez Actions > Supprimer.
   d. Entrez le nom de la politique et choisissez Supprimer.
   e. Répétez cette étape pour supprimer chacune des politiques IAM pour le cluster.

Sécurité dans ROSA

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci en tant que sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à ROSA, consultez Services AWS la section Portée par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par Service AWS ce que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation ROSA. Il vous explique comment procéder à la configuration ROSA pour atteindre vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres outils Services AWS qui vous aident à surveiller et à sécuriser vos ROSA ressources.

Table des matières

Protection des données dans ROSA

La the section called “Responsabilités” documentation et le modèle de responsabilitéAWS partagée définissent la protection des données dans ROSA. AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. Red Hat est chargé de protéger l'infrastructure du cluster et

la plate-forme de services sous-jacente. Le client est responsable du contrôle du contenu hébergé sur cette infrastructure. Ce contenu inclut la configuration de la sécurité et les tâches de gestion pour le Services AWS produit que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) relatives à la confidentialité des données. Pour plus d'informations sur la protection des données en Europe, veuillez consulter le billet de blog Modèle de responsabilité partagée AWS et RGPD sur la page Blog Security AWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels que Amazon Macie, qui aident à découvrir et à sécuriser les données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons vivement de ne jamais placer d'informations identifiables sensibles, telles que les numéros de compte de vos clients, dans des champs de formulaire comme Name (Nom). Cela inclut lorsque vous travaillez avec ROSA ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez ROSA ou d'autres services peuvent être récupérées pour être incluses dans les journaux de diagnostic. Lorsque vous fournissez une URL à un serveur externe, n'incluez pas les informations d'identification non chiffrées dans l'URL pour valider votre demande adressée au serveur.

Rubriques

Protection des données à l'aide du chiffrement

La protection des données fait référence à la protection des données en transit (lors de leur trajet aller-retour ROSA) et au repos (lorsqu'elles sont stockées sur des disques dans AWS des centres de données).

Red Hat OpenShift Service on AWS fournit un accès sécurisé aux volumes de stockage Amazon Elastic Block Store (Amazon EBS) attachés aux Amazon EC2 instances pour le plan de ROSA contrôle, l'infrastructure et les nœuds de travail, ainsi qu'aux volumes persistants Kubernetes pour le stockage persistant. ROSA chiffre les données en volume au repos et en transit, et utilise AWS Key Management Service (AWS KMS) pour protéger vos données chiffrées. Le service utilise Amazon S3 le stockage du registre des images de conteneurs, qui est chiffré au repos par défaut.

> **Important**
>
> Parce que ROSA c'est un service géré, AWS et Red Hat gère l'infrastructure qui l' ROSA utilise. Les clients ne doivent pas essayer d'arrêter manuellement les Amazon EC2 instances ROSA utilisées depuis la AWS console ou la CLI. Cette action peut entraîner une perte de données client.

Chiffrement des données pour les Amazon EBS volumes de stockage sauvegardés

Red Hat OpenShift Service on AWS utilise le framework de volumes persistants (PV) Kubernetes pour permettre aux administrateurs de clusters de fournir un stockage persistant à un cluster. Les volumes persistants, ainsi que le plan de contrôle, l'infrastructure et les nœuds de travail, sont soutenus par Amazon Elastic Block Store (Amazon EBS) des volumes de stockage attachés aux Amazon EC2 instances.

Pour les volumes ROSA persistants et les nœuds soutenus par Amazon EBS, les opérations de chiffrement sont effectuées sur les serveurs hébergeant les instances EC2, garantissant ainsi la sécurité des données au repos et des données en transit entre une instance et son stockage attaché. Pour plus d'informations, consultez la section sur le Amazon EBS chiffrement dans le guide de Amazon EC2 l'utilisateur.

Chiffrement des données pour le pilote Amazon EBS CSI et le pilote Amazon EFS CSI

ROSA par défaut, le pilote Amazon EBS CSI est utilisé pour Amazon EBS provisionner le stockage. Le pilote Amazon EBS CSI et l'opérateur de pilote Amazon EBS CSI sont installés sur le cluster par défaut dans l'`openshift-cluster-csi-drivers`espace de noms. Le pilote et l'opérateur Amazon EBS CSI vous permettent de provisionner dynamiquement des volumes persistants et de créer des instantanés de volumes.

ROSA est également capable de provisionner des volumes persistants à l'aide du pilote Amazon EFS CSI et de l'opérateur de pilote Amazon EFS CSI. Le Amazon EFS pilote et l'opérateur vous permettent également de partager les données du système de fichiers entre des pods ou avec d'autres applications au sein ou en dehors de Kubernetes.

Les données de volume sont sécurisées en transit pour le pilote Amazon EBS CSI et le pilote Amazon EFS CSI. Pour plus d'informations, consultez la section Utilisation de l'interface de stockage de conteneurs (CSI) dans la documentation Red Hat.

> **Important**
>
> Lors du provisionnement dynamique de volumes ROSA persistants à l'aide du pilote Amazon EFS CSI, tenez Amazon EFS compte de l'ID utilisateur, de l'ID de groupe (GID) et IDs du groupe secondaire du point d'accès lors de l'évaluation des autorisations du système de fichiers. Amazon EFS remplace l'utilisateur et le groupe IDs sur les fichiers par l'utilisateur et le groupe IDs sur le point d'accès et ignore le client NFS. IDs Par conséquent, ignore Amazon EFS silencieusement les paramètres`fsGroup`. ROSA n'est pas en mesure GIDs de remplacer les fichiers en utilisant`fsGroup`. Tout pod pouvant accéder à un point d' Amazon EFS accès monté peut accéder à n'importe quel fichier du volume. Pour plus d'informations, consultez la section Utilisation des points Amazon EFS d'accès dans le guide de Amazon EFS l'utilisateur.

cryptage etcd

ROSA offre la possibilité d'activer le chiffrement des valeurs `etcd` clés dans le `etcd` volume lors de la création du cluster, en ajoutant une couche de chiffrement supplémentaire. Une fois `etcd` le chiffrement effectué, vous devrez supporter une surcharge de performance d'environ 20 %. Nous vous recommandons d'activer `etcd` le chiffrement uniquement si vous en avez spécifiquement besoin pour votre cas d'utilisation. Pour plus d'informations, consultez la section chiffrement etcd dans la définition du ROSA service.

Gestion des clés

ROSA permet KMS keys de gérer en toute sécurité le plan de contrôle, l'infrastructure et les volumes de données des employés, ainsi que les volumes persistants pour les applications des clients. Lors de la création du cluster, vous avez le choix d'utiliser la clé AWS gérée par défaut KMS key fournie par Amazon EBS ou de spécifier votre propre clé gérée par le client. Pour de plus amples informations, veuillez consulter the section called “Gestion des clés”.

Chiffrement des données pour le registre d'images intégré

ROSA fournit un registre d'images de conteneur intégré pour stocker, récupérer et partager des images de conteneurs via le stockage par Amazon S3 bucket. Le registre est configuré et géré par l'opérateur de registre OpenShift d'images. Il fournit une out-of-the-box solution permettant aux utilisateurs de gérer les images qui exécutent leurs charges de travail et s'exécute au-dessus de l'infrastructure de cluster existante. Pour plus d'informations, consultez la section Registre dans la documentation Red Hat.

ROSA propose des registres d'images publics et privés. Pour les applications d'entreprise, nous vous recommandons d'utiliser un registre privé afin de protéger vos images contre toute utilisation par des utilisateurs non autorisés. Pour protéger les données de votre registre au repos, ROSA utilise le chiffrement côté serveur par défaut avec des clés Amazon S3 gérées (SSE-S3). Cela ne nécessite aucune action de votre part et est proposé sans frais supplémentaires. Pour plus d'informations, consultez la section Protection des données à l'aide du chiffrement côté serveur avec des clés de chiffrement Amazon S3 gérées (SSE-S3) dans le guide de l'utilisateur. Amazon S3

ROSA utilise le protocole TLS (Transport Layer Security) pour sécuriser les données en transit vers et depuis le registre d'images. Pour plus d'informations, consultez la section Registre dans la documentation Red Hat.

Confidentialité du trafic inter-réseau

Red Hat OpenShift Service on AWS utilise Amazon Virtual Private Cloud (Amazon VPC) pour créer des limites entre les ressources de votre ROSA cluster et contrôler le trafic entre celles-ci, votre réseau local et Internet. Pour plus d'informations sur Amazon VPC la sécurité, consultez la section Confidentialité du trafic interréseau Amazon VPC dans le Guide de l' Amazon VPC utilisateur.

Dans le VPC, vous pouvez configurer vos ROSA clusters pour utiliser un serveur proxy HTTP ou HTTPS afin de refuser l'accès direct à Internet. Si vous êtes administrateur de cluster, vous pouvez également définir des politiques réseau au niveau du pod qui limitent le trafic interréseau aux pods de

votre ROSA cluster. Pour de plus amples informations, veuillez consulter the section called "Sécurité de l'infrastructure".

Chiffrement des données grâce à KMS

ROSA utilise AWS KMS pour gérer en toute sécurité les clés des données cryptées. Les volumes du plan de contrôle, de l'infrastructure et des nœuds de travail sont chiffrés par défaut à l'aide du AWS système géré KMS key fourni par Amazon EBS. Cela KMS key porte le pseudonyme`aws/ebs`. Les volumes persistants qui utilisent la classe de stockage gp3 par défaut sont également chiffrés par défaut à l'aide de cette KMS key classe.

Les ROSA clusters nouvellement créés sont configurés pour utiliser la classe de stockage gp3 par défaut pour chiffrer les volumes persistants. Les volumes persistants créés à l'aide d'une autre classe de stockage ne sont chiffrés que si la classe de stockage est configurée pour être chiffrée. Pour plus d'informations sur les classes ROSA de stockage prédéfinies, consultez la section Configuration du stockage persistant dans la documentation Red Hat.

Lors de la création du cluster, vous pouvez choisir de chiffrer les volumes persistants de votre cluster à l'aide de la clé Amazon EBS fournie par défaut ou de spécifier votre propre système symétrique géré par le client. KMS key Pour plus d'informations sur la création de clés, consultez la section Création de clés KMS de chiffrement symétriques dans le manuel du AWS KMS développeur.

Vous pouvez également chiffrer des volumes persistants pour des conteneurs individuels au sein d'un cluster en définissant un KMS key. Cela est utile lorsque vous disposez de directives de conformité et de sécurité explicites lors du déploiement vers AWS. Pour plus d'informations, consultez la section Chiffrer les volumes persistants de conteneurs AWS avec un KMS key dans la documentation Red Hat.

Les points suivants doivent être pris en compte lors du chiffrement de volumes persistants à l'aide des vôtres KMS keys :

- Lorsque vous utilisez le chiffrement KMS avec le vôtre KMS key, la clé doit se trouver au même Région AWS endroit que votre cluster.
- Il y a un coût associé à la création et à l'utilisation des vôtres KMS keys. Pour en savoir plus, consultez Pricing AWS Key Management Service (Tarification).

Gestion des identités et des accès pour ROSA

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAM les administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ROSA ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction du travail que vous effectuez ROSA.

Utilisateur du service : si vous utilisez le ROSA service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles ROSA fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. Si vous comprenez bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans ROSA, consultezthe section called "Résolution des problèmes".

Administrateur du service - Si vous êtes responsable des ROSA ressources de votre entreprise, vous avez probablement un accès complet à ROSA. C'est à vous de déterminer les ROSA fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base de IAM.

IAM administrateur - Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur les politiques utilisées pour gérer l'accès à ROSA. Pour consulter des exemples de politiques

ROSA basées sur l'identité que vous pouvez utiliser dans IAM, consultez. the section called " ROSA exemples de politiques basées sur l'identité"

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur Compte AWS root Utilisateur IAM, ou en assumant un IAM rôle.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center (IAM Identity Center) les utilisateurs, l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre Compte AWS compte dans le guide de l'utilisateur de AWS connexion.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes d' AWS API dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être également fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez les sections Authentification multifactorielle du Guide de l'utilisateur d' AWS IAM Identity Center (successeur du Single Sign-On) et Utilisation de l'authentification multifactorielle (MFA) dans AWS le Guide de l'utilisateur IAM. AWS

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité

est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, voir Qu'est-ce qu'IAM Identity Center ? dans le guide de l'utilisateur d' AWS IAM Identity Center (successeur du Single Sign-On). AWS

Utilisateurs IAM et groupes

An Utilisateur IAMest une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous fier à des informations d'identification temporaires plutôt que de créer des Utilisateurs IAM personnes possédant des informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme Utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un IAM groupe est une identité qui spécifie une collection de Utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez la section Quand créer un rôle Utilisateur IAM (au lieu d'un rôle) dans le guide de l'utilisateur IAM.

IAM rôles

Un IAM rôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un Utilisateur IAM, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de l'utilisateur IAM.

IAM les rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous devez créer un rôle et définir des autorisations pour ce rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les ensembles d'autorisations, consultez la section Ensembles d'autorisations du AWS guide de l'utilisateur d'IAM Identity Center (successeur de AWS Single Sign-On).
- Utilisateur IAM Autorisations temporaires - Un Utilisateur IAM homme peut assumer un IAM rôle en assumant temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le

principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section En quoi les IAM rôles diffèrent des politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

- Accès multiservices : certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications Amazon EC2 ou y stocke des objets Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction du service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) - Lorsque vous utilisez un rôle Utilisateur IAM ou pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transfert des sessions d'accès.
  - Rôle de service - Un rôle de service est un IAM rôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieur IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service - Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre IAM compte et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une Amazon EC2 instance et qui envoient AWS CLI des demandes AWS d'API. Cela est préférable au stockage des clés d'accès dans l' Amazon EC2 instance. Pour attribuer un AWS rôle à une Amazon EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' Amazon EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des Amazon EC2 instances dans le Guide de l'utilisateur IAM.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, consultez la section Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAM les politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un Utilisateur IAM rôle ou un groupe. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs

utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les IAM politiques de confiance de rôle et des Amazon S3 politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 AWS WAF, et Amazon VPC sont des exemples de services qui soutiennent ACLs. Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations - Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (Utilisateur IAM ou à un rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations obtenues représentent la combinaison des politiques basées sur

l'identité de l'entité et de ses limites d'autorisations. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCPs) : SCPs sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités des comptes membres, y compris pour chaque utilisateur Compte AWS root. Pour plus d'informations sur les Organizations SCPs, voir Politiques de contrôle des services (SCPs) dans le Guide de AWS Organizations l'utilisateur.
- Stratégies de session - Les stratégies de session sont des stratégies avancées que vous transmettez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la session obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de session. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

ROSA exemples de politiques basées sur l'identité

Par défaut, Utilisateurs IAM les rôles ne sont pas autorisés à créer ou à modifier AWS des ressources. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un IAM administrateur doit créer des IAM politiques qui accordent aux utilisateurs et aux rôles l'autorisation d'effectuer des opérations d'API spécifiques sur les ressources spécifiques dont ils ont besoin. L'administrateur doit ensuite associer ces politiques au Utilisateurs IAM ou aux groupes qui nécessitent ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de stratégie JSON, consultez la section Création de politiques dans l'onglet JSON du guide de l'utilisateur IAM.

Utilisation de la ROSA console

Pour s'abonner ROSA depuis la console, votre principal IAM doit disposer des AWS Marketplace autorisations requises. Les autorisations permettent au principal de s'abonner et de se désabonner de la liste des ROSA produits AWS Marketplace et de consulter AWS Marketplace les abonnements. Pour ajouter les autorisations requises, accédez à la ROSA console et attachez la politique AWS gérée `ROSAManageSubscription` à votre principal IAM. Pour plus d'informations sur `ROSAManageSubscription`, consultez the section called "AWS politique gérée : ROSAManage Abonnement".

Autoriser ROSA with HCP à gérer les ressources AWS

ROSA avec plans de contrôle hébergés (HCP) utilise des politiques AWS gérées avec des autorisations requises pour le fonctionnement et le support du service. Vous utilisez la ROSA CLI ou IAM la console pour associer ces politiques aux rôles de service de votre Compte AWS.

Pour de plus amples informations, veuillez consulter the section called " AWS politiques gérées".

Autoriser ROSA Classic à gérer les ressources AWS

ROSA classic utilise des politiques IAM gérées par le client avec des autorisations prédéfinies par le service. Vous utilisez la ROSA CLI pour créer ces politiques et les associer à des rôles de service dans votre Compte AWS. ROSA exige que ces politiques soient configurées comme définies par le service afin de garantir un fonctionnement et un support de service continus.

> **Note**
>
> Vous ne devez pas modifier les politiques classiques de ROSA sans consulter au préalable Red Hat. Cela pourrait annuler le contrat de niveau de service de 99,95 % de disponibilité du cluster conclu par Red Hat. ROSA avec plans de contrôle hébergés utilise des politiques AWS gérées avec un ensemble d'autorisations plus limité. Pour de plus amples informations, veuillez consulter the section called " AWS politiques gérées".

Il existe deux types de politiques gérées par le client pour ROSA : les politiques de compte et les politiques d'opérateur. Les politiques de compte sont associées aux IAM rôles que le service utilise

pour établir une relation de confiance avec Red Hat en matière de support technique (SRE), de création de clusters et de fonctionnalités de calcul. Les politiques d'opérateur sont associées aux IAM rôles que OpenShift les opérateurs utilisent pour les opérations de cluster liées à l'entrée, au stockage, au registre d'images et à la gestion des nœuds. Les politiques de compte sont créées une fois par cluster Compte AWS, tandis que les politiques d'opérateur sont créées une fois par cluster.

Pour plus d'informations, consultez the section called "Politiques relatives aux comptes ROSA Classic" et the section called "Politiques des opérateurs ROSA Classic".

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment vous pouvez créer une politique qui Utilisateurs IAM permet de visualiser les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du. AWS CLI

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

```
            "Resource": "*"
        }
    ]
}
```

Politiques relatives aux comptes ROSA Classic

Cette section fournit des détails sur les politiques de compte requises pour ROSA Classic. Ces autorisations sont nécessaires pour que ROSA classic puisse gérer les AWS ressources sur lesquelles les clusters s'exécutent et permettre à l'ingénieur de fiabilité des sites Red Hat de prendre en charge les clusters. Vous pouvez attribuer un préfixe personnalisé aux noms des politiques, mais ces politiques doivent sinon être nommées comme indiqué sur cette page (par exemple,`ManagedOpenShift-Installer-Role-Policy`).

Les politiques de compte sont spécifiques à une version OpenShift mineure et sont rétrocompatibles. Avant de créer ou de mettre à niveau un cluster, vous devez vérifier que la version de la politique et la version du cluster sont identiques en exécutant`rosa list account-roles`. Si la version de la politique est inférieure à la version du cluster, exécutez `rosa upgrade account-roles` pour mettre à niveau les rôles et les politiques associées. Vous pouvez utiliser les mêmes politiques de compte et les mêmes rôles pour plusieurs clusters de la même version mineure.

[Préfixe] -Installer-Role-Policy

Vous pouvez attacher `[Prefix]-Installer-Role-Policy` à vos entités IAM. Avant de créer un cluster ROSA classic, vous devez d'abord associer cette politique à un rôle IAM nommé`[Prefix]-Installer-Role`. Cette politique accorde les autorisations requises qui permettent au ROSA programme d'installation de gérer les AWS ressources nécessaires à la création du cluster.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

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

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

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

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

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

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

[Préfixe] - ControlPlane -Role-Policy

Vous pouvez attacher `[Prefix]-ControlPlane-Role-Policy` à vos entités IAM. Avant de créer un cluster ROSA classic, vous devez d'abord associer cette politique à un rôle IAM nommé`[Prefix]-ControlPlane-Role`. Cette politique accorde les autorisations requises à ROSA classic pour gérer Amazon EC2 les Elastic Load Balancing ressources hébergeant le plan de ROSA contrôle, ainsi que pour lire KMS keys.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

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

```
    ]
}
```

[Préfixe] -Worker-Role-Policy

Vous pouvez attacher `[Prefix]-Worker-Role-Policy` à vos entités IAM. Avant de créer un cluster ROSA classic, vous devez d'abord associer cette politique à un rôle IAM nommé`[Prefix]-Worker-Role`. Cette politique accorde les autorisations requises à ROSA classic pour décrire les instances EC2 exécutées en tant que nœuds de travail.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

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

[Préfixe] -Support-Role-Policy

Vous pouvez attacher `[Prefix]-Support-Role-Policy` à vos entités IAM. Avant de créer un cluster ROSA classic, vous devez d'abord associer cette politique à un rôle IAM nommé`[Prefix]-Support-Role`. Cette politique accorde les autorisations requises à l'ingénierie de fiabilité des sites Red Hat pour observer, diagnostiquer et prendre en charge les AWS ressources utilisées par les clusters ROSA Classic, y compris la possibilité de modifier l'état des nœuds du cluster.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

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

Politiques des opérateurs ROSA Classic

Cette section fournit des détails sur les politiques d'opérateur requises pour ROSA classic. Avant de créer un cluster ROSA classic, vous devez d'abord associer ces politiques aux rôles d'opérateur concernés. Un ensemble unique de rôles d'opérateur est requis pour chaque cluster.

Ces autorisations sont nécessaires pour permettre aux OpenShift opérateurs de gérer les nœuds de cluster ROSA Classic. Vous pouvez attribuer un préfixe personnalisé aux noms des politiques pour simplifier la gestion des politiques (par exemple,`ManagedOpenShift-openshift-ingress-operator-cloud-credentials`).

[Préfixe] - -credentials openshift-ingress-operator-cloud

Vous pouvez attacher `[Prefix]-openshift-ingress-operator-cloud-credentials` à vos entités IAM. Cette politique accorde les autorisations requises à l'opérateur d'entrée pour provisionner et gérer les équilibreurs de charge et les configurations DNS pour l'accès au cluster externe. La politique permet également à l'opérateur d'entrée de lire et de filtrer les valeurs Route 53 des balises de ressources afin de découvrir les zones hébergées. Pour plus d'informations sur l'opérateur, voir OpenShift Ingress Operator dans la OpenShift GitHub documentation.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

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

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

Vous pouvez attacher `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` à vos entités IAM. Cette politique accorde les autorisations requises à l'opérateur du pilote Amazon EBS CSI pour installer et gérer le pilote Amazon EBS CSI sur un cluster ROSA classic. Pour plus d'informations sur l'opérateur, consultez aws-ebs-csi-driver-operator dans la OpenShift GitHub documentation.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

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

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

Vous pouvez attacher `[Prefix]-openshift-machine-api-aws-cloud-credentials` à vos entités IAM. Cette politique accorde les autorisations requises à l'opérateur Machine Config pour décrire, exécuter et mettre fin aux Amazon EC2 instances gérées en tant que nœuds de travail. Cette politique accorde également des autorisations permettant le chiffrement du disque du volume racine du nœud de travail utilisé AWS KMS keys. Pour plus d'informations sur l'opérateur, consultez machine-config-operatorla OpenShift GitHub documentation.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

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

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

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

Vous pouvez attacher `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` à vos entités IAM. Cette politique accorde les autorisations requises à l'opérateur d'identification du cloud pour récupérer des Utilisateur IAM informations, notamment la clé d'accès IDs, les documents de politique intégrés joints, la date de création de l'utilisateur, le chemin, l'ID utilisateur et le nom de ressource Amazon (ARN). Pour plus d'informations sur l'opérateur, consultez cloud-credential-operatorla OpenShift GitHub documentation.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

```
{
```

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

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

Vous pouvez attacher `[Prefix]-openshift-image-registry-installer-cloud-credentials` à vos entités IAM. Cette politique accorde les autorisations requises à l'opérateur du registre d'images pour fournir et gérer les ressources du registre d'images intégré au cluster de ROSA Classic et des services dépendants, notamment Amazon S3. Cela est nécessaire pour que l'opérateur puisse installer et maintenir le registre interne d'un cluster ROSA classic. Pour plus d'informations sur l'opérateur, consultez la section Opérateur de registre d'images dans la OpenShift GitHub documentation.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

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

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

Vous pouvez attacher `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` à vos entités IAM. Cette politique accorde les autorisations requises à l'opérateur Cloud Network Config Controller pour provisionner et gérer les ressources réseau destinées à être utilisées par la superposition réseau de clusters ROSA Classic. L'opérateur utilise ces autorisations pour gérer les adresses IP privées des Amazon EC2 instances dans le cadre du cluster ROSA Classic. Pour plus d'informations sur l'opérateur, voir C loud-network-config-controller dans la OpenShift GitHub documentation.

Politique d'autorisations

Les autorisations définies dans ce document de politique précisent quelles actions sont autorisées ou refusées.

```
{
    "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 politiques gérées pour ROSA

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants. Pour plus d'informations, consultez la section Politiques AWS gérées dans le Guide de IAM l'utilisateur.

AWS politique gérée : ROSAManage Abonnement

Vous pouvez associer la `ROSAManageSubscription` politique à vos IAM entités. Avant de procéder ROSA à l'activation dans la AWS ROSA console, vous devez d'abord associer cette politique à un rôle IAM.

Cette politique vous accorde les AWS Marketplace autorisations nécessaires pour gérer l' ROSA abonnement.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `aws-marketplace:Subscribe`- Accorde l'autorisation de s'abonner au AWS Marketplace produit pour ROSA.
- `aws-marketplace:Unsubscribe`- Permet aux donneurs d'ordre de supprimer les abonnements aux AWS Marketplace produits.
- `aws-marketplace:ViewSubscriptions`- Permet aux principaux de consulter les abonnements depuis AWS Marketplace. Cela est nécessaire pour que le IAM principal puisse consulter les AWS Marketplace abonnements disponibles.

Pour consulter le document de politique JSON complet, consultez la section ROSAManageAbonnement dans le Guide de référence des politiques AWS gérées.

Politiques relatives aux comptes ROSA with HCP

Cette section fournit des détails sur les politiques de compte requises pour ROSA avec des plans de contrôle hébergés (HCP). Ces politiques AWS gérées ajoutent les autorisations utilisées par ROSA avec les rôles HCP IAM. Les autorisations sont requises pour le support technique de l'ingénierie de fiabilité des sites (SRE) Red Hat, l'installation du cluster, le plan de contrôle et les fonctionnalités de calcul.

> **Note**
>
> AWS les politiques gérées sont destinées à être utilisées par ROSA avec des plans de contrôle hébergés (HCP). Les clusters ROSA Classic utilisent des politiques IAM gérées par le client. Pour plus d'informations sur les politiques classiques de ROSA, consultez the section called "Politiques relatives aux comptes ROSA Classic" etthe section called "Politiques des opérateurs ROSA Classic".

AWS politique gérée : ROSAWorker InstancePolicy

Vous pouvez les `ROSAWorkerInstancePolicy` rattacher à vos IAM entités. Avant de créer un cluster, vous devez disposer d'un rôle IAM associé à cette politique. Un service ROSA passe des appels à d'autres Services AWS personnes en votre nom. Ils le font pour gérer les ressources que vous utilisez avec chaque cluster.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent aux nœuds de travail ROSA d'effectuer les tâches suivantes :

- `ec2`— Évaluez Région AWS les détails de l' Amazon EC2 instance dans le cadre de la gestion du cycle de vie des nœuds du cluster ROSA.
- `ecr`- Évaluez et obtenez des images à partir de référentiels ECR gérés par Rosa qui sont nécessaires à l'installation du cluster et à la gestion du cycle de vie des nœuds de travail.

Pour consulter le document de politique JSON complet, consultez ROSAWorkerInstancePolicyle Guide de référence des politiques AWS gérées.

AWS stratégie gérée : ROSASRESupport Politique

Vous pouvez attacher `ROSASRESupportPolicy` à vos entités IAM.

Avant de créer un cluster ROSA avec plans de contrôle hébergés, vous devez d'abord associer cette politique à un rôle IAM. Cette politique accorde les autorisations requises aux ingénieurs de fiabilité des sites Red Hat (SREs) pour observer, diagnostiquer et prendre directement en charge les AWS ressources associées aux ROSA clusters, y compris la possibilité de modifier l'état des nœuds du ROSA cluster.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent SREs à Red Hat d'effectuer les tâches suivantes :

- `cloudtrail`— Lisez AWS CloudTrail les événements et les sentiers pertinents pour le cluster.
- `cloudwatch`— Lisez Amazon CloudWatch les métriques pertinentes pour le cluster.
- `ec2`— Lisez, décrivez et passez en revue Amazon EC2 les composants liés à l'état du cluster, tels que les groupes de sécurité, les connexions aux points de terminaison VPC et l'état des volumes. Lancez, arrêtez, redémarrez et mettez fin à Amazon EC2 des instances.
- `elasticloadbalancing`— Lisez, décrivez et passez en revue Elastic Load Balancing les paramètres liés à l'état de santé du cluster.
- `iam`— Évaluez IAM les rôles liés à l'état de santé du cluster.
- `route53`— Vérifiez les paramètres DNS liés à l'état du cluster.
- `sts`— `DecodeAuthorizationMessage` — Lit IAM les messages à des fins de débogage.

Pour consulter le document de politique JSON complet, voir ROSASRESupportPolitique dans le Guide de référence des politiques AWS gérées.

AWS stratégie gérée : ROSAInstaller Politique

Vous pouvez les `ROSAInstallerPolicy` rattacher à vos IAM entités.

Avant de créer un cluster ROSA avec plans de contrôle hébergés, vous devez d'abord associer cette politique à un rôle IAM nommé`[Prefix]-ROSA-Worker-Role`. Cette politique permet aux entités d'ajouter n'importe quel rôle qui suit le `[Prefix]-ROSA-Worker-Role` modèle à un profil d'instance. Cette politique accorde les autorisations nécessaires au programme d'installation pour gérer les AWS ressources qui prennent en charge l'installation ROSA du cluster.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent au programme d'installation d'effectuer les tâches suivantes :

- `ec2`— Exécutez Amazon EC2 des instances à l'aide d'un serveur AMIs hébergé Comptes AWS appartenant à Red Hat et géré par Red Hat. Décrivez les Amazon EC2 instances, les volumes et les ressources réseau associés aux Amazon EC2 nœuds. Cette autorisation est requise pour que le plan de contrôle Kubernetes puisse joindre des instances à un cluster et que le cluster puisse évaluer sa présence au sein de celui-ci. Amazon VPC Consultez Amazon EC2 Capacity Reservations pour prendre en charge la nouvelle fonctionnalité de réservation de capacité de ROSA. Marquez et supprimez des balises sur les sous-réseaux en utilisant la correspondance `"kubernetes.io/cluster/*"` des clés de balise. Cela est nécessaire pour garantir que l'équilibreur de charge utilisé pour l'entrée du cluster est créé uniquement dans les sous-réseaux applicables et pour gérer les balises d'identification du cluster Kubernetes.
- `elasticloadbalancing`— Ajoutez des équilibreurs de charge aux nœuds cibles d'un cluster. Supprimez les équilibreurs de charge des nœuds cibles d'un cluster. Cette autorisation est requise pour que le plan de contrôle Kubernetes puisse approvisionner dynamiquement les équilibreurs de charge demandés par les services Kubernetes et les services d'application. OpenShift
- `kms`— Lisez une AWS KMS clé, créez et gérez les autorisations et Amazon EC2 renvoyez une clé de données symétrique unique à utiliser en dehors de AWS KMS. Cela est nécessaire pour l'utilisation de `etcd` données chiffrées lorsque le `etcd` chiffrement est activé lors de la création du cluster.
- `iam`— Validez les rôles et les politiques IAM. Provisionnez et gérez de manière dynamique les profils d' Amazon EC2 instance pertinents pour le cluster. Ajoutez des balises à un profil d'instance

IAM à l'aide de l'`iam:TagInstanceProfile`autorisation. Fournissez des messages d'erreur du programme d'installation lorsque l'installation du cluster échoue en raison de l'absence d'un fournisseur OIDC de cluster spécifié par le client.

- `route53`— Gérez les Route 53 ressources nécessaires à la création de clusters.
- `servicequotas`— Évaluez les quotas de service requis pour créer un cluster.
- `sts`— Créez des AWS STS informations d'identification temporaires pour ROSA les composants. Supposez les informations d'identification nécessaires à la création du cluster.
- `secretsmanager`— Lisez une valeur secrète pour autoriser en toute sécurité la configuration OIDC gérée par le client dans le cadre du provisionnement du cluster.

Pour consulter le document de politique JSON complet, voir ROSAInstallerPolitique dans le Guide de référence des politiques AWS gérées.

AWS stratégie gérée : ROSAShared VPCRoute53 Politique

Vous pouvez les `ROSASharedVPCRoute53Policy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM pour permettre à un cluster ROSA de passer des appels à d'autres utilisateurs Services AWS dans des environnements VPC partagés.

Cette politique permet au programme d'installation ROSA de configurer les enregistrements de la Route 53. Cette politique est destinée à être utilisée sur un VPC partagé et fournit un sous-ensemble d'autorisations Route 53 adaptées aux cas d'utilisation d'un VPC partagé.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent au programme d'installation de ROSA d'effectuer les tâches suivantes :

- `route53`— Lisez les informations de zone DNS et les enregistrements DNS existants pour comprendre la configuration DNS actuelle. Créez, modifiez et supprimez des enregistrements DNS, mais uniquement pour des modèles de domaine spécifiques liés à ROSA`.hypershift.local`, notamment, `.openshiftapps.com` `.devshift.org.openshiftusgov.com`, et. `.devshiftusgov.com` Ajoutez, modifiez ou supprimez des balises sur les ressources Route 53 pour la gestion et l'organisation des ressources.
- `tag`— Découvrez et listez AWS les ressources en fonction de leurs balises, ce qui est utile pour identifier les ressources gérées par ROSA.

Pour plus de détails sur la politique, y compris la dernière version du document de politique JSON, consultez la section ROSASharedVPCRoute53Politique dans le Guide de référence des politiques AWS gérées.

AWS stratégie gérée : ROSAShared VPCEndpoint Politique

Vous pouvez les `ROSASharedVPCEndpointPolicy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM pour permettre à un cluster ROSA de passer des appels à d'autres utilisateurs Services AWS dans des environnements VPC partagés.

Cette politique permet au programme d'installation ROSA de configurer des points de terminaison et des groupes de sécurité VPC dans des environnements VPC partagés.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent au programme d'installation de ROSA d'effectuer les tâches suivantes :

- `ec2`— Autorisations en lecture seule pour décrire les ressources liées au VPC, y compris les points de terminaison VPC et les groupes de sécurité afin de VPCs comprendre l'environnement réseau. Créez, supprimez et modifiez des groupes de sécurité avec des restrictions basées sur des balises, ce qui permet à ROSA de créer et de gérer des groupes de sécurité pour le réseau de clusters tout en limitant les opérations aux seules ressources étiquetées ROSA. Créez, modifiez et supprimez des points de terminaison VPC avec des restrictions basées sur des balises, ce qui permet à ROSA de créer et de gérer des points de terminaison VPC pour une connectivité privée dans des environnements VPC partagés. Services AWS Appliquez des balises aux points de terminaison et aux groupes de sécurité VPC nouvellement créés lors de la création pour une identification et une gestion appropriées des ressources.

Pour plus de détails sur la politique, y compris la dernière version du document de politique JSON, consultez la section ROSASharedVPCEndpointPolitique dans le Guide de référence des politiques AWS gérées.

ROSA avec les politiques des opérateurs HCP

Cette section fournit des détails sur les politiques d'opérateur requises pour ROSA avec des plans de contrôle hébergés (HCP). Vous pouvez associer ces politiques AWS gérées aux rôles d'opérateur nécessaires pour utiliser ROSA avec HCP. Les autorisations sont requises pour permettre aux OpenShift opérateurs de gérer ROSA avec des nœuds de cluster HCP.

> **Note**
>
> AWS les politiques gérées sont destinées à être utilisées par ROSA avec des plans de contrôle hébergés (HCP). Les clusters ROSA Classic utilisent des politiques IAM gérées par le client. Pour plus d'informations sur les politiques classiques de ROSA, consultez the section called "Politiques relatives aux comptes ROSA Classic" etthe section called "Politiques des opérateurs ROSA Classic".

AWS politique gérée : ROSAAmazon EBSCSIDriver OperatorPolicy

Vous pouvez les `ROSAAmazonEBSCSIDriverOperatorPolicy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM d'opérateur pour permettre à un cluster ROSA avec plans de contrôle hébergés de passer des appels à d'autres Services AWS. Un ensemble unique de rôles d'opérateur est requis pour chaque cluster.

Cette politique accorde les autorisations nécessaires à l'opérateur du pilote Amazon EBS CSI pour installer et gérer le pilote Amazon EBS CSI sur un ROSA cluster. Pour plus d'informations sur l'opérateur, voir aws-ebs-csi-driver opérateur dans la OpenShift GitHub documentation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent au Amazon EBS chauffeur opérateur d'effectuer les tâches suivantes :

- `ec2`— Créez, modifiez, attachez, détachez et supprimez Amazon EBS des volumes attachés à des Amazon EC2 instances. Créez et supprimez des instantanés de Amazon EBS volume et listez Amazon EC2 les instances, les volumes et les instantanés.

Pour consulter le document de politique JSON complet, consultez ROSAAmazonEBSCSIDriverOperatorPolicyle Guide de référence des politiques AWS gérées.

AWS politique gérée : ROSAIngress OperatorPolicy

Vous pouvez les `ROSAIngressOperatorPolicy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM d'opérateur pour permettre à un cluster ROSA avec plans de contrôle hébergés de passer des appels à d'autres Services AWS. Un ensemble unique de rôles d'opérateur est requis pour chaque cluster.

Cette politique accorde les autorisations requises à l'opérateur d'entrée pour provisionner et gérer les équilibreurs de charge et les configurations DNS pour les ROSA clusters. La politique autorise l'accès en lecture aux valeurs des balises. L'opérateur filtre ensuite les valeurs des balises pour les Route 53 ressources afin de découvrir les zones hébergées. Pour plus d'informations sur l'opérateur, voir OpenShift Ingress Operator dans la OpenShift GitHub documentation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent à l'opérateur d'entrée d'effectuer les tâches suivantes :

- `elasticloadbalancing`— Décrivez l'état des équilibreurs de charge provisionnés.
- `route53`— Répertoriez les zones Route 53 hébergées et modifiez les enregistrements qui gèrent le DNS contrôlé par le cluster ROSA.
- `tag`— Gérez les ressources étiquetées en utilisant l'`tag:GetResources`autorisation.

Pour consulter le document de politique JSON complet, consultez ROSAIngressOperatorPolicyle Guide de référence des politiques AWS gérées.

AWS politique gérée : ROSAImage RegistryOperatorPolicy

Vous pouvez les `ROSAImageRegistryOperatorPolicy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM d'opérateur pour permettre à un cluster ROSA avec plans de contrôle hébergés de passer des appels à d'autres Services AWS. Un ensemble unique de rôles d'opérateur est requis pour chaque cluster.

Cette politique accorde les autorisations requises à l'opérateur de registre d'images pour fournir et gérer les ressources pour le registre ROSA d'images du cluster et les services dépendants, y compris S3. Cela est nécessaire pour que l'opérateur puisse installer et gérer le registre interne d'un ROSA cluster. Pour plus d'informations sur l'opérateur, consultez la section Opérateur de registre d'images dans la OpenShift GitHub documentation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent à l'opérateur du registre d'images d'effectuer les actions suivantes :

- `s3`— Gérez et évaluez les Amazon S3 buckets en tant que stockage permanent pour le contenu des images du conteneur et les métadonnées du cluster.

Pour consulter le document de politique JSON complet, consultez ROSAImageRegistryOperatorPolicyle Guide de référence des politiques AWS gérées.

AWS politique gérée : ROSACloud NetworkConfigOperatorPolicy

Vous pouvez les `ROSACloudNetworkConfigOperatorPolicy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM d'opérateur pour permettre à un cluster ROSA avec plans de contrôle hébergés de passer des appels à d'autres Services AWS. Un ensemble unique de rôles d'opérateur est requis pour chaque cluster.

Cette politique accorde les autorisations requises à l'opérateur Cloud Network Config Controller pour provisionner et gérer les ressources réseau pour la superposition réseau du ROSA cluster. L'opérateur utilise ces autorisations pour gérer les adresses IP privées Amazon EC2 des instances faisant partie du ROSA cluster. Pour plus d'informations sur l'opérateur, voir C loud-network-config-controller dans la OpenShift GitHub documentation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent à l'opérateur Cloud Network Config Controller d'effectuer les tâches suivantes :

- `ec2`— Lisez, attribuez et décrivez les configurations pour connecter Amazon EC2 des instances, Amazon VPC des sous-réseaux et des interfaces réseau élastiques dans un ROSA cluster.

Pour consulter le document de politique JSON complet, consultez ROSACloudNetworkConfigOperatorPolicyle Guide de référence des politiques AWS gérées.

AWS politique gérée : ROSAKube ControllerPolicy

Vous pouvez les `ROSAKubeControllerPolicy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM d'opérateur pour permettre à un cluster ROSA avec plans de contrôle hébergés de passer des appels à d'autres Services AWS. Un ensemble unique de rôles d'opérateur est requis pour chaque cluster.

Cette politique accorde les autorisations requises au contrôleur Kube pour gérer Amazon EC2 Elastic Load Balancing, et les AWS KMS ressources nécessaires à un cluster ROSA avec plans de contrôle hébergés. Pour plus d'informations sur ce contrôleur, consultez la section Architecture du contrôleur dans la OpenShift documentation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent au contrôleur Kube d'effectuer les tâches suivantes :

- `ec2`— Créez, supprimez et ajoutez des balises aux groupes de sécurité des Amazon EC2 instances. Ajoutez des règles de trafic entrant aux groupes de sécurité. Décrivez les zones de disponibilité, Amazon EC2 les instances, les tables de routage VPCs, les groupes de sécurité et les sous-réseaux.
- `elasticloadbalancing`— Créez et gérez les équilibreurs de charge et leurs politiques. Créez et gérez des écouteurs d'équilibrage de charge. Enregistrez et annulez les cibles auprès des groupes cibles et gérez les groupes cibles. Enregistrez et désenregistrez Amazon EC2 les instances auprès d'un équilibreur de charge, et ajoutez des balises aux équilibreurs de charge.
- `kms`— Récupère des informations détaillées sur une AWS KMS clé. Cela est nécessaire pour l'utilisation de `etcd` données chiffrées lorsque le `etcd` chiffrement est activé lors de la création du cluster.

Pour consulter le document de politique JSON complet, consultez ROSAKubeControllerPolicyle Guide de référence des politiques AWS gérées.

AWS politique gérée : ROSANode PoolManagementPolicy

Vous pouvez les `ROSANodePoolManagementPolicy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM d'opérateur pour permettre à un cluster ROSA avec plans de contrôle hébergés de passer des appels vers d'autres AWS services. Un ensemble unique de rôles d'opérateur est requis pour chaque cluster.

Cette politique accorde les autorisations requises au NodePool contrôleur pour décrire, exécuter et mettre fin aux Amazon EC2 instances gérées en tant que nœuds de travail. Cette politique accorde également des autorisations pour autoriser le chiffrement du disque du volume racine du nœud de travail à l'aide de AWS KMS clés, pour baliser l'interface elastic network attachée au nœud de travail et pour accéder aux réservations de capacité Amazon EC2. Pour plus d'informations sur ce contrôleur, consultez la section Architecture du contrôleur dans la OpenShift documentation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent au NodePool contrôleur d'effectuer les tâches suivantes :

- `ec2`— Exécutez Amazon EC2 des instances à l'aide d'un serveur AMIs hébergé Comptes AWS appartenant à Red Hat et géré par Red Hat. Gérez les cycles de vie EC2 dans le cluster. ROSA

Créez et intégrez dynamiquement des nœuds de travail avec Elastic Load Balancing Amazon VPC Route 53, Amazon EBS,, et Amazon EC2. Accédez aux réservations de capacité et décrivez-les pour prendre en charge la fonctionnalité de réservation de capacité de ROSA.

- `iam`— À utiliser Elastic Load Balancing via le rôle lié au service nommé. `AWSServiceRoleForElasticLoadBalancing` Attribuez des rôles aux profils d' Amazon EC2 instance.
- `kms`— Lisez une AWS KMS clé, créez et gérez les autorisations et Amazon EC2 renvoyez une clé de données symétrique unique à utiliser en dehors de AWS KMS. Cela est nécessaire pour permettre le chiffrement du disque du volume racine du nœud de travail.

Pour consulter le document de politique JSON complet, consultez ROSANodePoolManagementPolicyle Guide de référence des politiques AWS gérées.

AWS stratégie gérée : ROSAKMSProvider Politique

Vous pouvez les `ROSAKMSProviderPolicy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM d'opérateur pour permettre à un cluster ROSA avec plans de contrôle hébergés de passer des appels à d'autres Services AWS. Un ensemble unique de rôles d'opérateur est requis pour chaque cluster.

Cette politique accorde les autorisations requises au fournisseur de AWS chiffrement intégré pour gérer les AWS KMS clés qui prennent en charge le chiffrement `etcd` des données. Cette politique permet d' Amazon EC2 utiliser les clés KMS fournies par le fournisseur de AWS chiffrement pour chiffrer et déchiffrer `etcd` les données. Pour plus d'informations sur ce fournisseur, consultez la section Fournisseur de AWS chiffrement dans la documentation de Kubernetes GitHub .

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent au fournisseur de AWS chiffrement d'effectuer les tâches suivantes :

- `kms`— Chiffrez, déchiffrez et récupérez une AWS KMS clé. Cela est nécessaire pour l'utilisation de `etcd` données chiffrées lorsque le `etcd` chiffrement est activé lors de la création du cluster.

Pour consulter le document de politique JSON complet, voir ROSAKMSProviderPolitique dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : ROSAControl PlaneOperatorPolicy

Vous pouvez les `ROSAControlPlaneOperatorPolicy` rattacher à vos IAM entités. Vous devez associer cette politique à un rôle IAM d'opérateur pour permettre à un cluster ROSA avec plans de contrôle hébergés de passer des appels à d'autres Services AWS. Un ensemble unique de rôles d'opérateur est requis pour chaque cluster.

Cette politique accorde les autorisations requises à l'opérateur du plan de contrôle pour gérer Amazon EC2 et affecter les Route 53 ressources à ROSA avec des clusters de plans de contrôle hébergés. Pour plus d'informations sur cet opérateur, consultez la section Architecture du contrôleur dans la OpenShift documentation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent à l'opérateur du plan de contrôle d'effectuer les tâches suivantes :

- `ec2`— Créez et gérez des Amazon VPC points de terminaison.
- `route53`— Répertoriez et modifiez les ensembles d' Route 53 enregistrements et listez les zones hébergées.

Pour consulter le document de politique JSON complet, consultez ROSAControlPlaneOperatorPolicyle Guide de référence des politiques AWS gérées.

ROSA mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées ROSA depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS de la page Historique de la documentation.

Modifier	Description	Date
ROSANodePoolManagementPolicy — Politique mise à jour	ROSA a mis à jour la politique afin d'ajouter l'accès aux ressources pour les réservations de capacité Amazon EC2. Cette modification permet au NodePool contrôleur d'accéder aux réservations de capacité	3 septembre 2025

Modifier	Description	Date
	et de les décrire afin d'amélior er la gestion des ressources. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSANode PoolManag ementPolicy".	
ROSASharedVPCEndpo intPolitique — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique permettant à l' ROSA installateur de configurer les points de terminaison et les groupes de sécurité VPC dans les environnements VPC partagés. Cette politique fournit un sous-ensemble d'autorisations EC2 adaptées aux cas d'utilisation de VPC partagés. Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSAShared VPCEndpoint Politique".	7 août 2025

Modifier	Description	Date
ROSASharedVPCRoute 53Politique — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique permettant à l' ROSA installateur de configurer les enregistrements Route 53 dans des environnements VPC partagés. Cette politique fournit un sous-ensemble d'autorisations Route 53 adaptées aux cas d'utilisation de VPC partagés. Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSAShared VPCRoute53 Politique".	7 août 2025

Modifier	Description	Date
ROSAInstallerPolitique — Politique mise à jour	ROSA a mis à jour la politique afin de permettre à l' ROSA installateur d'inspecter les réservations de capacité Amazon EC2 afin de prendre en charge la nouvelle fonctionnalité de réservation de capacité de ROSA. Cette mise à jour permet également au programme d'installation de supprimer des balises sur les sous-réseaux à l'aide de clés de balise correspondantes `"kubernetes.io/cluster/*"` pour améliorer la gestion des balises du cluster Kubernetes. Pour en savoir plus, veuillez consulter la section the section called “AWS stratégie gérée : ROSAInstaller Politique”.	7 août 2025

Modifier	Description	Date
ROSAImageRegistryOperatorPolicy — Politique mise à jour	ROSA a mis à jour la politique afin que les autorisations soient limitées au niveau des ressources du compartiment S3. Cette modification répond aux exigences de stockage ROSA pour les zones AWS commerciales et GovCloud régionales. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAImage RegistryOperatorPolicy".	19 mai 2025
ROSANodePoolManagementPolicy — Politique mise à jour	ROSA a mis à jour la politique afin d'autoriser le balisage de l'interface Elastic network attachée au nœud de travail. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSANode PoolManagementPolicy".	5 mai 2025

Modifier	Description	Date
ROSAImageRegistryOperatorPolicy — Politique mise à jour	ROSA a mis à jour la politique afin de permettre à l'opérateur de registre OpenShift d'images Red Hat de provisionner et de gérer des buckets et des objets Amazon S3 dans AWS GovCloud les régions afin qu'ils soient utilisés par le registre d'images intégré au cluster ROSA. Cette modification répond aux exigences de stockage ROSA pour les AWS GovCloud régions. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAImage RegistryOperatorPolicy".	16 avril 2025
ROSAWorkerInstancePolicy — Politique mise à jour	ROSA a mis à jour la politique afin de permettre aux nœuds de travail d'évaluer et d'obtenir des images à partir de référentiels ECR gérés par ROSA qui sont nécessaires à l'installation du cluster et à la gestion du cycle de vie des nœuds de travail. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAWorker InstancePolicy".	3 mars 2025

Modifier	Description	Date
ROSANodePoolManagementPolicy — Politique mise à jour	ROSA a mis à jour la politique pour permettre aux interfaces réseau élastiques d'être étiquetées de la même manière que les instances EC2 uniquement pendant les RunInstances appels ec2 : lorsque la demande inclut la balise. `red-hat-managed: true` Ces autorisations sont nécessaires pour prendre en charge ROSA avec les clusters HCP 4.17. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSANode PoolManagementPolicy".	24 février 2025
ROSAAmazonEBSCSIDriverOperatorPolicy — Politique mise à jour	ROSA a mis à jour la politique pour prendre en charge la nouvelle API d'autorisation des Amazon EBS instantanés. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAAmazon EBSCSIDriver OperatorPolicy".	17 janvier 2025

Modifier	Description	Date
ROSANodePoolManagementPolicy — Politique mise à jour	ROSA a mis à jour la politique pour permettre au gestionnaire de pool de ROSA nœuds de décrire les ensembles d'options DHCP afin de définir les noms DNS privés appropriés. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSANodePoolManagementPolicy".	2 mai 2024
ROSAInstallerPolitique — Politique mise à jour	ROSA a mis à jour la politique pour permettre au ROSA programme d'installation d'ajouter des balises aux sous-réseaux en utilisant la correspondance `"kubernetes.io/cluster/*"` des clés de balise. Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSAInstaller Politique".	24 avril 2024

Modifier	Description	Date
ROSASRESupportPolitique — Politique mise à jour	ROSA a mis à jour la politique pour permettre au rôle SRE de récupérer des informations sur les profils d'instance marqués ROSA commered-hat-managed . Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSASRESupport Politique".	10 avril 2024
ROSAInstallerPolitique — Politique mise à jour	ROSA a mis à jour la politique pour permettre au ROSA programme d'installation de valider que les politiques AWS gérées pour ROSA sont attachées aux IAM rôles utilisés par ROSA. Cette mise à jour permet également au programme d'installation de déterminer si des politiques gérées par le client ont été associées aux ROSA rôles. Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSAInstaller Politique".	10 avril 2024

Modifier	Description	Date
ROSAInstallerPolitique — Politique mise à jour	ROSA a mis à jour la politique pour permettre au service de fournir des messages d'alerte au programme d'installation lorsque l'installation du cluster échoue en raison de l'absence d'un fournisseur OIDC de cluster spécifié par le client. Cette mise à jour permet également au service de récupérer les serveurs de noms DNS existants afin que les opérations de provisionnement de clusters soient idempotentes. Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSAInstaller Politique".	26 janvier 2024
ROSASRESupportPolitique — Politique mise à jour	ROSA a mis à jour la politique pour permettre au service d'effectuer des opérations de lecture sur les groupes de sécurité à l'aide de l' DescribeSecurityGroups API. Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSASRESupport Politique".	22 janvier 2024

Modifier	Description	Date
ROSAImageRegistryOperatorPolicy — Politique mise à jour	ROSA a mis à jour la politique afin de permettre à l'opérateur du registre d'images d'effectuer des actions sur les Amazon S3 compartiments dans les régions portant des noms à 14 caractères. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAImage RegistryOperatorPolicy".	12 décembre 2023
ROSAKubeControllerPolicy — Politique mise à jour	ROSA a mis à jour la politique pour permettre kube-controller-manager de décrire les zones de disponibilité, Amazon EC2 les instances, les tables de routage VPCs, les groupes de sécurité et les sous-réseaux. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAKube ControllerPolicy".	16 octobre 2023
ROSAManageAbonnement — Politique mise à jour	ROSA a mis à jour la politique pour ajouter le ROSA avec des plans de contrôle hébergés ProductId. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAManage Abonnement".	1er août 2023

Modifier	Description	Date
ROSAKubeControllerPolicy — Politique mise à jour	ROSA a mis à jour la politique pour permettre de kube-controller-manager créer des équilibreurs de charge réseau en tant qu'équilibreurs de charge de service Kubernetes. Les équilibreurs de charge réseau offrent une meilleure capacité à gérer les charges de travail volatiles et prennent en charge les adresses IP statiques pour l'équilibreur de charge. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAKubeControllerPolicy".	13 juillet 2023
ROSANodePoolManagementPolicy — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique permettant au NodePool contrôleur de décrire, d'exécuter et de mettre fin aux Amazon EC2 instances gérées en tant que nœuds de travail. Cette politique permet également le chiffrement du disque du volume racine du nœud de travail à l'aide de AWS KMS clés. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSANodePoolManagementPolicy".	8 juin 2023

Modifier	Description	Date
ROSAInstallerPolitique — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique pour permettre au programme d'installation de gérer les AWS ressources qui prennent en charge l'install ation du cluster. Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSAInstaller Politique".	6 juin 2023
ROSASRESupportPolitique — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique permettant à Red Hat SREs d'observer, de diagnostiquer et de prendre directement en charge les AWS ressources associées aux ROSA clusters, y compris la possibilité de modifier l'état des nœuds du ROSA cluster. Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSASRESupport Politique".	1er juin 2023

Modifier	Description	Date
ROSAKMSProviderPolitique — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique pour permettre au fournisseur de AWS chiffrement intégré de gérer les AWS KMS clés afin de prendre en charge le chiffrement des données etcd. Pour en savoir plus, veuillez consulter la section the section called "AWS stratégie gérée : ROSAKMSProvider Politique".	27 avril 2023
ROSAKubeControllerPolicy — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique pour permettre au contrôleur Kube de gérer les clusters de plans de contrôle ROSA hébergés Amazon EC2 Elastic Load Balancing , ainsi que les AWS KMS ressources nécessaires. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAKube ControllerPolicy".	27 avril 2023

Modifier	Description	Date
ROSAImageRegistryOperatorPolicy — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique permettant à l'opérateur de registre d'images de fournir et de gérer les ressources pour le registre d'images ROSA intégré au cluster et les services dépendants, y compris S3. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAImage RegistryOperatorPolicy".	27 avril 2023
ROSAControlPlaneOperatorPolicy — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique permettant à l'opérateur du plan de contrôle de gérer les clusters de plans de contrôle ROSA hébergés Amazon EC2 et de gérer les Route 53 ressources nécessaires. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAControl PlaneOperatorPolicy".	24 avril 2023

Modifier	Description	Date
ROSACloudNetworkConfigOperatorPolicy — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique permettant à l'opérateur Cloud Network Config Controller de provisionner et de gérer les ressources réseau pour la superposition réseau du ROSA cluster. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSACloud NetworkConfigOperatorPolicy".	20 avril 2023
ROSAIngressOperatorPolicy — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique permettant à l'opérateur d'entrée de provisionner et de gérer les équilibreurs de charge et les configurations DNS pour les ROSA clusters. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAIngress OperatorPolicy".	20 avril 2023
ROSAAmazonEBSCSIDriverOperatorPolicy — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique permettant à l'opérateur du pilote Amazon EBS CSI d'installer et de gérer le pilote Amazon EBS CSI sur un ROSA cluster. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAAmazon EBSCSIDriver OperatorPolicy".	20 avril 2023

Modifier	Description	Date
ROSAWorkerInstancePolicy — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique pour permettre au service de gérer les ressources du cluster. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAWorker InstancePolicy".	20 avril 2023
ROSAManageAbonnement — Ajout d'une nouvelle politique	ROSA a ajouté une nouvelle politique pour accorder les AWS Marketplace autorisations nécessaires à la gestion de l' ROSA abonnement. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : ROSAManage Abonnement".	11 avril 2022
Red Hat OpenShift Service on AWS a commencé à suivre les modifications	Red Hat OpenShift Service on AWS a commencé à suivre les modifications apportées AWS à ses politiques gérées.	2 mars 2022

Résolution des problèmes ROSA d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec ROSA et IAM.

AWS Organizations la politique de contrôle des services refuse AWS Marketplace les autorisations requises

Si votre politique AWS Organizations de contrôle des services (SCP) n'autorise pas les autorisations AWS Marketplace d'abonnement requises lorsque vous tentez de les activer ROSA, l'erreur de console suivante se produit.

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

Si ce message d'erreur s'affiche, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui gère les comptes de votre organisation. Demandez à cette personne de faire ce qui suit :

1. Configurez le SCP pour autoriser `aws-marketplace:Subscribeaws-marketplace:Unsubscribe`, et `aws-marketplace:ViewSubscriptions` autorisations. Pour plus d'informations, consultez la section Mise à jour d'un SCP dans le guide de AWS Organizations l'utilisateur.
2. Activez ROSA dans le compte de gestion de l'organisation.
3. Partagez l' ROSA abonnement avec les comptes des membres qui nécessitent un accès au sein de l'organisation. Pour plus d'informations, consultez la section Partage des abonnements au sein d'une organisation dans le Guide de AWS Marketplace l'acheteur.

L'utilisateur ou le rôle ne dispose pas des AWS Marketplace autorisations requises

Si votre IAM principal ne dispose pas des autorisations AWS Marketplace d'abonnement requises lorsque vous tentez de l'activer ROSA, l'erreur de console suivante se produit.

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

Pour résoudre ce problème, procédez comme suit :

1. Accédez à la IAM console et associez la politique AWS gérée `ROSAManageSubscription` à votre identité IAM. Pour plus d'informations, consultez la section ROSAManageAbonnement dans le Guide de référence des politiques AWS gérées.
2. Suivez la procédure décrite dans the section called “Activer ROSA et configurer les AWS prérequis”.

Si vous n'êtes pas autorisé à consulter ou à mettre à jour les autorisations définies IAM ou si vous recevez un message d'erreur, vous devez contacter votre administrateur pour obtenir de l'aide. Demandez à cette personne de `ROSAManageSubscription` s' IAM identifier et de suivre la

procédure décrite dansthe section called "Activer ROSA et configurer les AWS prérequis". Lorsqu'un administrateur exécute cette action, elle l'active ROSA en mettant à jour l'ensemble d'autorisations pour toutes les IAM identités relevant du Compte AWS.

AWS Marketplace Autorisations requises bloquées par un administrateur

Si l'administrateur de votre compte a bloqué les autorisations AWS Marketplace d'abonnement requises, l'erreur de console suivante se produit lorsque vous tentez de les activer ROSA.

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

Si ce message d'erreur s'affiche, vous devez contacter votre administrateur pour obtenir de l'aide. Demandez à cette personne de faire ce qui suit :

1. Accédez à la ROSA console et associez la politique AWS gérée `ROSAManageSubscription` à votre identité IAM. Pour plus d'informations, consultez la section ROSAManageAbonnement dans le Guide de référence des politiques AWS gérées.
2. Suivez la procédure the section called "Activer ROSA et configurer les AWS prérequis" pour l'activer ROSA. Cette procédure est activée ROSA en mettant à jour l'ensemble d'autorisations pour toutes les IAM identités relevant du Compte AWS.

Erreur lors de la création de l'équilibreur de charge : AccessDenied

Si vous n'avez pas créé d'équilibreur de charge, le rôle `AWSServiceRoleForElasticLoadBalacing` lié au service n'existe peut-être pas dans votre compte. L'erreur suivante se produit si vous tentez de créer un rôle ROSA cluster sans le `AWSServiceRoleForElasticLoadBalacing` rôle dans votre compte.

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

Pour résoudre ce problème, procédez comme suit :

1. Vérifiez si le `AWSServiceRoleForElasticLoadBalancing` rôle est attribué à votre compte.

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

2. Si vous ne possédez pas ce rôle, suivez les instructions pour créer le rôle figurant dans la section Créer le rôle lié à un service dans le Guide de l' Elastic Load Balancing utilisateur.

Résilience dans ROSA

AWS résilience des infrastructures mondiales

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées via un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

ROSA offre aux clients la possibilité d'exécuter le plan de contrôle et le plan de données Kubernetes dans une seule zone de AWS disponibilité ou dans plusieurs zones de disponibilité. Bien que les clusters mono-AZ puissent être utiles à des fins d'expérimentation, les clients sont invités à exécuter leurs charges de travail dans plusieurs zones de disponibilité. Cela garantit que les applications peuvent résister même à une défaillance complète de la zone de disponibilité, un événement très rare en soi.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

ROSA résilience des clusters

Le plan de ROSA contrôle comprend au moins trois nœuds du plan OpenShift de contrôle. Chaque nœud du plan de contrôle est composé d'une instance de serveur API, d'une `etcd` instance et de contrôleurs. En cas de défaillance d'un nœud du plan de contrôle, toutes les demandes d'API sont automatiquement acheminées vers les autres nœuds disponibles afin de garantir la disponibilité du cluster.

Le plan de ROSA données comprend au moins deux nœuds OpenShift d'infrastructure et deux nœuds OpenShift de travail. Les nœuds d'infrastructure exécutent des pods qui prennent en charge les composants de l'infrastructure du OpenShift cluster tels que le routeur par défaut, le OpenShift registre intégré et les composants pour les métriques et la surveillance du cluster. OpenShift les nœuds de travail exécutent des pods d'applications pour les utilisateurs finaux.

Les ingénieurs de fiabilité des sites Red Hat (SREs) gèrent entièrement le plan de contrôle et les nœuds d'infrastructure. Red Hat surveille le ROSA cluster de SREs manière proactive et est responsable du remplacement des nœuds du plan de contrôle et des nœuds d'infrastructure défaillants. Pour de plus amples informations, veuillez consulter the section called "Responsabilités".

> **Important**
>
> Étant donné qu' ROSA il s'agit d'un service géré, Red Hat est responsable de la gestion de l' AWS infrastructure sous-jacente qu'il ROSA utilise. Les clients ne doivent pas essayer d'arrêter manuellement les Amazon EC2 instances ROSA utilisées depuis la AWS console ou AWS CLI. Cette action peut entraîner une perte de données client.

Si un nœud de travail tombe en panne sur le plan de données, le plan de contrôle déplace les pods non planifiés vers le ou les nœuds de travail fonctionnels jusqu'à ce que le nœud défaillant soit récupéré ou remplacé. Les nœuds de travail défaillants peuvent être remplacés manuellement ou automatiquement en activant le dimensionnement automatique des machines d'un cluster. Pour plus d'informations, consultez la section Mise à l'échelle automatique du cluster dans la documentation Red Hat.

Résilience des applications déployées par le client

Bien qu'il ROSA fournisse de nombreuses protections pour garantir la haute disponibilité du service, les clients ont la responsabilité de développer leurs applications déployées dans un souci de haute disponibilité afin de protéger les charges de travail contre les temps d'arrêt. Pour plus d'informations, consultez À propos de la disponibilité ROSA dans la documentation Red Hat.

Sécurité de l'infrastructure dans ROSA

En tant que service géré, Red Hat OpenShift Service on AWS il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, voir Protection de l'infrastructure dans Security Pillar — AWS Well-Architected Framework.

Vous utilisez des appels d'API AWS publiés pour accéder ROSA via le AWS réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.

- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Isolation du réseau en cluster

Les ingénieurs de fiabilité des sites Red Hat (SREs) sont responsables de la gestion continue et de la sécurité réseau du cluster et de la plate-forme d'application sous-jacente. Pour plus d'informations sur les responsabilités de Red Hat en matière de ROSA, consultezthe section called "Responsabilités".

Lorsque vous créez un nouveau cluster, ROSA vous avez la possibilité de créer un point de terminaison et des routes d'application du serveur d'API Kubernetes public ou un point de terminaison d'API Kubernetes privé et des routes d'application. Cette connexion est utilisée pour communiquer avec votre cluster (à l'aide d'outils OpenShift de gestion tels que les CLI et OpenShift CLI ROSA). Une connexion privée permet à toutes les communications entre vos nœuds et le serveur d'API de rester au sein de votre VPC. Si vous activez l'accès privé au serveur d'API et aux routes d'application, vous devez utiliser un VPC existant et AWS PrivateLink connecter le VPC au service principal. OpenShift

L'accès au serveur d'API Kubernetes est sécurisé à l'aide d'une combinaison de Gestion des identités et des accès AWS (IAM) et d'un contrôle d'accès basé sur les rôles (RBAC) Kubernetes natif. Pour plus d'informations sur Kubernetes RBAC, consultez la section Utilisation de l'autorisation RBAC dans la documentation de Kubernetes.

ROSA vous permet de créer des itinéraires d'application sécurisés à l'aide de plusieurs types de terminaison TLS pour délivrer des certificats au client. Pour plus d'informations, consultez la section Routes sécurisées dans la documentation Red Hat.

Si vous créez un ROSA cluster dans un VPC existant, vous spécifiez les sous-réseaux VPC et les zones de disponibilité que votre cluster doit utiliser. Vous définissez également les plages d'adresses CIDR que le réseau de clusters doit utiliser et vous associez ces plages d'adresses CIDR aux sous-réseaux VPC. Pour plus d'informations, consultez les définitions des plages CIDR dans la documentation Red Hat.

Pour les clusters qui utilisent le point de terminaison d'API public, votre VPC ROSA doit être configuré avec un sous-réseau public et privé pour chaque zone de disponibilité dans laquelle vous souhaitez déployer le cluster. Pour les clusters qui utilisent le point de terminaison d'API privé, seuls les sous-réseaux privés sont requis.

Si vous utilisez un VPC existant, vous pouvez configurer vos ROSA clusters pour qu'ils utilisent un serveur proxy HTTP ou HTTPS pendant ou après la création du cluster afin de chiffrer le trafic Web du cluster, ajoutant ainsi un niveau de sécurité supplémentaire à vos données. Lorsque vous activez un proxy, l'accès direct à Internet est refusé aux composants principaux du cluster. Le proxy ne refuse pas l'accès à Internet pour les charges de travail des utilisateurs. Pour plus d'informations, consultez la section Configuration d'un proxy à l'échelle du cluster dans la documentation Red Hat.

Isolation du réseau de pods

Si vous êtes administrateur de cluster, vous pouvez définir des politiques réseau au niveau du pod qui limitent le trafic aux pods de votre ROSA cluster.

ROSA quotas de service

Red Hat OpenShift Service on AWS (ROSA) utilise des quotas de service pour Amazon EC2, Amazon Virtual Private Cloud Amazon Elastic Block Store, et Elastic Load Balancing pour approvisionner des clusters. Pour plus d'informations, consultez la section Red Hat OpenShift Service on AWS Points de terminaison et quotas dans le Guide de référence AWS général.

AWS services intégrés à ROSA

ROSA travaille avec d'autres Services AWS pour fournir des solutions supplémentaires aux défis de votre entreprise. Cette rubrique identifie les services utilisés ROSA pour ajouter des fonctionnalités ou les services ROSA utilisés pour effectuer des tâches.

Rubriques

- Comment ROSA fonctionne avec AWS Marketplace

Comment ROSA fonctionne avec AWS Marketplace

AWS Marketplace est un catalogue numérique organisé que vous pouvez utiliser pour trouver, acheter, déployer et gérer les logiciels, données et services tiers dont vous avez besoin pour créer des solutions et gérer votre entreprise. AWS Marketplace simplifie les licences et les achats de logiciels grâce à des options de tarification flexibles et à de multiples méthodes de déploiement.

ROSA utilisations AWS Marketplace pour le comptage et la facturation des services. Le ROSA classic est mesuré et facturé via un produit basé sur AWS Marketplace Amazon Machine Image (AMI), tandis que le ROSA avec plans de contrôle hébergés (HCP) est mesuré et facturé via un produit basé sur le AWS Marketplace logiciel en tant que service (SAAS).

Cette page explique comment ROSA fonctionne le système AWS Marketplace pour les paiements, la facturation, les abonnements et les achats de contrats.

Terminologie

Cette page utilise les termes suivants pour discuter de l'intégration de ROSA avec AWS Marketplace.

Amazon Machine Image (AMI)

> Image d'un serveur, y compris un système d'exploitation et des logiciels supplémentaires, qui s'exécute sur AWS.

Abonnement AMI

> Dans AWS Marketplace, les produits logiciels basés sur l'AMI tels que ROSA Classic utilisent un modèle de tarification horaire avec abonnement annuel. La tarification horaire est le modèle de tarification par défaut, mais vous avez la possibilité d'acheter l'équivalent d'un an d'utilisation à l'avance pour un type d' Amazon EC2 instance.

Abonnement SaaS

Dans AWS Marketplace, les produits software-as-a-service (SaaS) tels que ROSA with HCP adoptent un modèle d'abonnement basé sur l'utilisation. Le vendeur du logiciel suit votre utilisation et vous ne payez que pour ce que vous utilisez.

Offre publique

Les offres publiques vous permettent d'acheter des AWS Marketplace logiciels et des services directement auprès du AWS Management Console.

Offre privée

Les offres privées sont un programme d'achat qui permet aux vendeurs et aux acheteurs de négocier des prix personnalisés et les conditions du contrat de licence utilisateur final (EULA) pour les achats en AWS Marketplace.

ROSA frais de service

Frais liés à ROSA la gestion des OpenShift logiciels et des clusters par les ingénieurs de fiabilité des sites Red Hat (SREs). ROSA les frais de service sont mesurés AWS Marketplace et apparaissent sur votre AWS facture.

AWS frais d'infrastructure

Frais standard AWS facturés pour les ROSA clusters Services AWS sous-jacents, y compris Amazon EC2 Amazon EBS, Amazon S3, et Elastic Load Balancing. Les frais sont mesurés en fonction de l' Service AWS utilisation et apparaissent sur votre AWS facture.

ROSA paiements et facturation

ROSA s'intègre AWS Marketplace pour permettre le comptage et la facturation des frais de ROSA service. ROSA les frais de service couvrent l'accès aux OpenShift logiciels et à la gestion des clusters par les ingénieurs de fiabilité des sites Red Hat (SREs). ROSA les frais de service sont uniformes dans toutes les régions AWS standard prises en charge. Les frais de service ROSA avec HCP s'accumulent par défaut sur demande à un taux horaire fixe basé sur le nombre de clusters en cours d'exécution et sur le nœud de travail v CPUs exécuté dans ces clusters. Les frais de service ROSA Classic s'accumulent à la demande en fonction du nombre de nœuds de travailleurs CPUs v. ROSA classic ne facture pas de frais de service pour le plan de contrôle ou les nœuds d'infrastructure requis.

ROSA les clients paient également AWS des frais d'infrastructure standard pour les ROSA clusters Services AWS sous-jacents Amazon EC2, notamment Amazon EBS, Amazon S3, et Elastic Load Balancing. AWS les frais d'infrastructure constituent un élément de facturation distinct des frais de ROSA service qui sont mesurés. AWS Marketplace AWS les frais d'infrastructure varient Région AWS et sont basés sur l'utilisation horaire par défaut. Pour réaliser des économies supplémentaires sur les coûts d' AWS infrastructure, vous pouvez acheter des plans Amazon EC2 d'épargne ou des instances réservées. Pour plus d'informations, consultez la section Compute Savings Plans and Reserved Instances dans le guide de Amazon EC2 l'utilisateur.

ROSA ne facture pas de frais tant que vous n'avez pas créé un ROSA cluster ou acheté un ROSA contrat. Pour en savoir plus, consultez Pricing Red Hat OpenShift Service on AWS (Tarification).

Vous pouvez consulter les frais ROSA de service et les frais d' AWS infrastructure et gérer les paiements dans la AWS Billing console. Vous pouvez également consulter gratuitement vos coûts et suivre l'utilisation à l'aide de l' AWS Cost Explorer Service interface. Pour plus d'informations, voir Consulter votre facture dans le guide de l' AWS Billing and Cost Management utilisateur et Analyser vos coûts AWS Cost Explorer Service dans le guide de l'utilisateur de la gestion des AWS coûts.

Abonnement aux listings ROSA Marketplace via la console

Lorsque vous l'activez ROSA dans la ROSA console, vous Compte AWS êtes abonné aux listes ROSA classic et ROSA with HCP activées AWS Marketplace. L'activation des ROSA abonnements est gratuite.

Pour AWS Organizations les utilisateurs, vous ROSA permet de partager les abonnements ROSA Classic avec d'autres comptes de votre organisation. Pour plus d'informations, consultez la section Partage des abonnements au sein d'une organisation dans le Guide de AWS Marketplace l'acheteur.

Acheter un ROSA contrat

ROSA utilise AWS Marketplace pour fournir des contrats optionnels pour ROSA avec HCP et ROSA classic. Les contrats permettent de réaliser des économies sur ROSA les frais de service des nœuds de travail. ROSA les contrats n'ont aucune incidence sur les frais facturés pour AWS l'infrastructure.

Contrats de 12 mois

Vous pouvez acheter des contrats d'offre publique de 12 mois pour ROSA Classic et ROSA avec HCP depuis la ROSA console.

> **Note**
>
> ROSA classic doit être activé sur votre compte pour que vous puissiez acheter des contrats de 12 mois depuis la console.

> **Note**
>
> Les contrats de 12 mois ne peuvent pas être transférés à une offre privée.

Acheter un contrat ROSA Classic de 12 mois

Lorsque vous souscrivez un contrat ROSA Classic de 12 mois, vous effectuez un paiement initial pour une durée annuelle et vous ne payez aucun frais de service horaire pendant les 12 prochains mois pour les instances couvertes. Le coût du contrat est basé sur le type d' Amazon EC2 instance et le nombre d'instances que vous sélectionnez. Le contrat ne couvre pas les ROSA frais d' AWS infrastructure facturés pour le Services AWS sous-jacent utilisé. Pour plus d'informations, consultez Tarification d'Red Hat OpenShift Service on AWS.

Le contrat couvre uniquement les types d'instances que vous spécifiez lors de la création du contrat (m5.xlarge par exemple). Vous pouvez acheter des contrats supplémentaires de 12 mois pour réaliser des économies sur plusieurs types d' Amazon EC2 instances. Toute utilisation en dehors de votre contrat de 12 mois entraîne des frais ROSA de service au tarif à la demande.

> **Note**
>
> Les contrats ROSA Classic de 12 mois ne se renouvellent pas automatiquement.

Pour acheter un contrat de 12 mois pour ROSA classic

> **Note**
>
> Si vous utilisez la ROSA console dans une région qui ne prend pas encore en charge ROSA avec HCP, ce flux de travail n'est pas encore disponible. Pour une liste des régions qui prennent en charge le ROSA avec le HCP, voirthe section called "Comparaison entre ROSA, HCP et ROSA classic".

Pour acheter des contrats ROSA Classic dans des régions sans ROSA avec support HCP, accédez à la ROSA console, choisissez Acheter un contrat logiciel et consultez les contrats existants.

1. Accédez à la console ROSA.
2. Dans le volet de navigation de gauche, sélectionnez Contracts.
3. Choisissez Contracts for ROSA Classic.
4. Choisissez le contrat d'achat.
5. Sélectionnez le type d' EC2 instance et le nombre d'instances dont vous avez besoin.
6. Choisissez Revoir le contrat.
7. Passez en revue les détails du contrat et choisissez Contrat d'achat.

Note

ROSA Les contrats de 12 mois ne peuvent pas être rétrogradés ou annulés après leur création à l'aide de la console. Si vous devez rétrograder ou annuler le contrat pendant la durée active du contrat, rendez-vous dans le Support Centre et ouvrez un dossier d'assistance.

Acheter un contrat de 12 mois avec ROSA avec HCP

Lorsque vous activez ROSA avec HCP dans la console, un contrat ROSA avec HCP gratuit de 12 mois est initialement créé sur votre compte pour faciliter la facturation à la demande. Si vous choisissez d'acheter un contrat ROSA avec HCP pour économiser sur les frais de service du nœud de travail, le contrat initial est modifié pour couvrir les coûts d'utilisation du nœud de travail v CPUs et des plans de contrôle que vous spécifiez.

Lorsque vous achetez un contrat ROSA with HCP de 12 mois, vous effectuez un paiement initial pour une durée annuelle et vous ne payez aucun frais d'utilisation horaire pendant les 12 prochains mois pour le nœud de travail v CPUs et les plans de contrôle couverts. Le coût du contrat est basé sur le nombre de nœuds de travail v CPUs et de plans de contrôle que vous sélectionnez. Le contrat couvre uniquement le nœud de travail v CPUs et les plans de contrôle que vous spécifiez lors de la création du contrat. Le contrat ne couvre pas les ROSA frais d' AWS infrastructure facturés pour le Services

AWS sous-jacent utilisé. Pour plus d'informations, consultez Tarification d'Red Hat OpenShift Service on AWS.

Quota d'utilisation mensuel

À l'achat, vos avions de télévision CPUs et de contrôle prépayés sont convertis en un quota d'utilisation mensuel. Les taux d'utilisation horaires à la demande s'appliquent pour l'utilisation des vCPU et du plan de contrôle qui dépasse le quota mensuel. ROSA with HCP utilise les formules suivantes pour calculer le quota mensuel associé au contrat :

- Nœud de travail v CPUs : nombre de v CPUs x 24 heures x 365 jours/12 mois
- Plans de contrôle : nombre de plans de contrôle x 24 heures x 365 jours/12 mois

Par exemple, l'achat de 4 000 nœuds de travail v CPUs et de 8 plans de contrôle se convertirait en un quota mensuel de 2 920 000 heures de vCPU de nœud de travail et de 5 840 heures de plan de contrôle consommables par mois.

Pour acheter un contrat de 12 mois avec ROSA with HCP

> **Note**
>
> Si vous utilisez la Red Hat OpenShift Service on AWS console dans une région qui ne prend pas encore en charge ROSA avec des plans de contrôle hébergés, ce flux de travail n'est pas encore disponible. Pour une liste des régions qui prennent en charge le ROSA avec le HCP, voirthe section called "Comparaison entre ROSA, HCP et ROSA classic".

1. Accédez à la console ROSA.
2. Dans le volet de navigation de gauche, sélectionnez Contracts.
3. Choisissez Contracts for ROSA with HCP.
4. Choisissez le contrat d'achat.
5. Entrez le nombre de v CPUs à acheter. Spécifiez en multiples de 4.
6. Entrez le nombre de plans de contrôle à acheter.
7. Choisissez Revoir le contrat.
8. Passez en revue les détails du contrat et choisissez Contrat d'achat.

> **Note**
>
> ROSA Les contrats de 12 mois ne peuvent pas être rétrogradés ou annulés après leur création à l'aide de la console. Si vous devez rétrograder ou annuler le contrat pendant la durée active du contrat, rendez-vous dans le Support Centre et ouvrez un dossier d'assistance.

Mise à niveau d'un contrat ROSA avec HCP de 12 mois

Vous pouvez à tout moment améliorer votre contrat ROSA with HCP actif de 12 mois avec un nœud de travail V CPUs et des plans de contrôle supplémentaires. Lorsque vous mettez à niveau votre contrat ROSA with HCP de 12 mois, vous effectuez un paiement initial au prorata pour les ressources supplémentaires. Les montants au prorata sont calculés en fonction du nombre de jours restant au contrat. Le contrat couvre uniquement le nœud de travail v CPUs et les plans de contrôle que vous spécifiez lors de la création du contrat. Les mises à niveau contractuelles n'ont aucune incidence sur les frais facturés pour AWS l'infrastructure.

Lors de la mise à niveau, les plans v CPUs et de contrôle ajoutés sont convertis en un quota d'utilisation mensuel en utilisant les mêmes formules que celles du contrat d'achat initial. Les taux d'utilisation horaires à la demande s'appliquent pour l'utilisation des vCPU et du plan de contrôle qui dépasse le quota mensuel. Pour de plus amples informations, veuillez consulter the section called "Quota d'utilisation mensuel".

Pour mettre à niveau un contrat de 12 mois avec ROSA with HCP

1. Accédez à la console ROSA.
2. Dans le volet de navigation de gauche, sélectionnez Contracts.
3. Choisissez Contracts for ROSA with HCP.
4. Choisissez Upgrade (Mise à niveau).
5. Entrez le nombre de v CPUs à ajouter. Spécifiez en multiples de 4.
6. Entrez le nombre de plans de contrôle à ajouter au contrat.
7. Choisissez Revoir la mise à niveau.
8. Consultez les détails du contrat et choisissez Acheter une mise à niveau.

> **Note**
>
> Les contrats ROSA Classic de 12 mois ne peuvent pas être revalorisés. Des contrats ROSA Classic supplémentaires de 12 mois peuvent être achetés à tout moment à l'aide de la ROSA console.

Obtention d'une offre privée

Vous pouvez demander une offre AWS Marketplace privée pour ROSA with HCP ou ROSA classic afin de bénéficier des prix des produits et des termes du contrat de licence utilisateur final (EULA) négociés avec Red Hat. Pour plus d'informations, consultez la section Offres privées dans le Guide de AWS Marketplace l'acheteur.

Pour obtenir une offre ROSA privée

> **Note**
>
> Si vous êtes un AWS Organizations utilisateur et que vous avez reçu une offre privée émise sur vos comptes payeur et membre, suivez la procédure ci-dessous pour vous abonner ROSA directement sur chaque compte de votre organisation.
> Si vous recevez une offre privée ROSA Classic uniquement émise sur le compte AWS Organizations payeur, vous devrez partager l'abonnement avec les comptes des membres de votre organisation. Pour plus d'informations, consultez la section Partage des abonnements au sein d'une organisation dans le Guide de AWS Marketplace l'acheteur.

1. Une fois qu'une offre privée a été émise, connectez-vous à la AWS Marketplace console.
2. Ouvrez l'e-mail contenant un lien ROSA d'offre privé.
3. Suivez le lien pour accéder directement à l'offre privée.

   > **Note**
   >
   > Si vous suivez ce lien avant de vous connecter au bon compte, une erreur Page note found (404) s'affichera.

4. Consultez les conditions générales.
5. Choisissez Accepter les conditions.

> **Note**
>
> Si une offre AWS Marketplace privée n'est pas acceptée, les frais de ROSA service AWS Marketplace continueront d'être facturés au taux horaire public.

6. Pour vérifier les détails de l'offre, sélectionnez Afficher les détails dans la liste des produits.
7. Pour commencer à utiliser ROSA, choisissez Continuer vers la configuration. Vous allez être redirigé vers la ROSA console.

Private Marketplace

Private Marketplace permet aux administrateurs de créer des catalogues numériques personnalisés de produits approuvés à partir de AWS Marketplace. Les administrateurs peuvent créer des ensembles uniques de logiciels approuvés disponibles AWS Marketplace pour les unités AWS organisationnelles ou différents Comptes AWS au sein de leur organisation à l'achat.

Si votre organisation utilise une place de marché privée, un administrateur doit ajouter les AWS Marketplace listes ROSA pour cette place de marché privée avant que les utilisateurs puissent activer le service. Pour plus d'informations, consultez la section Commencer à utiliser un marché privé dans le Guide de AWS Marketplace l'acheteur.

Résolution des problèmes

La page suivante décrit certains problèmes courants rencontrés lors de la création ou de la gestion de ROSA clusters.

Rubriques

Accédez aux journaux ROSA de débogage du cluster

Pour commencer à résoudre les problèmes liés à votre application, consultez d'abord les journaux de débogage. Les journaux de débogage de la ROSA CLI fournissent des détails sur les messages d'erreur produits en cas d' cluster échec de création d'un.

Pour afficher les informations de cluster débogage, exécutez la commande ROSA CLI suivante. Dans la commande, remplacez `<cluster_name>` par le nom de votre cluster.

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

ROSA le cluster échoue à la vérification des quotas de AWS service lors de cluster la création

Pour pouvoir être utilisés ROSA, les quotas de service de votre compte devront peut-être être augmentés. Pour plus d'informations, consultez Points de terminaison et quotas Red Hat OpenShift Service on AWS.

1. Exécutez la commande suivante pour identifier les quotas de votre compte.

```
rosa verify quota
```

> **Note**
>
> Les quotas sont différents Régions AWS. Assurez-vous de vérifier chacun des quotas pour vos régions.

2. Si vous devez augmenter votre quota, accédez à la Service Quotas console.
3. Dans le volet de navigation, sélectionnez AWS services.
4. Choisissez le service qui nécessite une augmentation de quota.
5. Sélectionnez le quota qui doit être augmenté, puis choisissez Demander une augmentation du quota.
6. Pour Demander une augmentation du quota, entrez le montant total que vous souhaitez attribuer au quota et choisissez Demander.

Résoudre les problèmes liés aux jetons d'accès hors ligne expirés de la ROSA CLI

Si vous utilisez la ROSA CLI et que votre jeton d'accès hors ligne api.openshift.com expire, un message d'erreur s'affiche. Cela se produit lorsque sso.redhat.com invalide le jeton.

1. Accédez à la page OpenShift Cluster Manager API Token et choisissez Load Token.
2. Copiez et collez la commande d'authentification suivante dans le terminal.

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

Impossible de créer un fichier cluster avec une osdCcsAdmin erreur

> **Note**
>
> Cette erreur se produit uniquement lorsque vous utilisez la méthode non STS pour provisionner des clusters ROSA . Pour éviter ce problème, provisionnez vos ROSA clusters à l'aide de AWS STS. Pour de plus amples informations, veuillez consulter the section called "Création d'un cluster classique ROSA - CLI".

Si vous cluster ne parvenez pas à créer, le message d'erreur suivant peut s'afficher :

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

1. Supprimer la pile.

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

2. Réinitialisez votre compte.

   ```
   rosa init
   ```

Étapes suivantes

- Consultez la OpenShift documentation.
- Ouvrez un Support étui ou un dossier Red Hat Support.
- Trouvez les réponses aux questions fréquemment posées sur Red Hat OpenShift Service on AWS.
- Pour plus d'informations sur le modèle de support de ROSA, consultezthe section called “Obtention de support”.

Obtenir de ROSA l'aide

Avec ROSA, vous pouvez bénéficier de l'assistance de la part Support des équipes d'assistance de Red Hat. Support : les dossiers d'assistance peuvent être ouverts auprès de l'une ou l'autre organisation et sont acheminés vers l'équipe appropriée pour résoudre votre problème.

Ouvrez un Support étui

Un plan de support aux AWS développeurs est nécessaire pour ouvrir des dossiers ROSA techniques, mais un plan de support AWS Business, Enterprise ou Enterprise On-Ramp est recommandé pour un accès continu au support ROSA technique et aux conseils architecturaux. Red Hat utilise l' Support API pour ouvrir des dossiers aux clients lorsque cela est nécessaire. AWS Les plans de support Business, Enterprise et Enterprise On-Ramp permettent aux ingénieurs de support d'accéder en permanence au téléphone, au Web et au chat. Pour plus d'informations sur Support les forfaits, consultez Support.

Pour connaître les étapes d'activation d'un Support plan, voir Comment m'inscrire à un Support plan ?

Pour plus d'informations sur la création d'un Support dossier, voir Création de dossiers d'assistance et gestion des dossiers.

Ouvrez un dossier Red Hat Support

ROSA inclut le Support Red Hat Premium. Pour bénéficier du support Red Hat Premium, accédez au portail client Red Hat et utilisez l'outil de demande d'assistance pour créer un ticket d'assistance. Pour plus d'informations, consultez Comment contacter le support Red Hat.

Historique du document

Le tableau suivant décrit les modifications importantes apportées à la documentation . Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Mis à jour ROSAKubeController Policy	Mise à jour de la politique AWS gérée ROSAKube ControllerPolicy afin de clarifier les autorisations d'Elastic Load Balancing pour l'enregistrement et le désenregistrement de cibles auprès de groupes cibles. Pour plus d'informations, voir les ROSA mises à jour des politiques AWS gérées.	5 mars 2026
Mis à jour ROSANodePoolManagementPolicy	ROSA a mis à jour la politique gérée `ROSANodePoolManagementPolicy` afin d'ajouter l'accès aux ressources pour les réservations de capacité afin de prendre en charge la fonctionnalité de réservation de capacité. Pour plus d'informations, voir les ROSA mises à jour des politiques AWS gérées.	3 septembre 2025
ROSAInstallerPolitique mise à jour	Mise à jour de la ROSAInstaller politique de AWS gestion pour prendre en charge la nouvelle fonctionnalité de réservation de capacité	7 août 2025

	de ROSA et améliorer la gestion des balises du cluster Kubernetes. Pour plus d'informations, voir les ROSA mises à jour des politiques AWS gérées.	
Nouvelle ROSAShared VPCRoute53 politique	ROSA a publié une nouvelle politique gérée `ROSAShare dVPCRoute53Policy` pour permettre au programme d'installation ROSA de configurer les enregistrements Route 53 dans des environnements VPC partagés. Pour plus d'informations, voir les ROSA mises à jour des politiques AWS gérées.	7 août 2025
Nouvelle ROSAShared VPCEndpoint politique	ROSA a publié une nouvelle politique gérée `ROSAShare dVPCEndpointPolicy` pour permettre au programme d'installation ROSA de configurer les points de terminaison et les groupes de sécurité VPC dans des environnements VPC partagés. Cette politique fournit un sous-ensemble d'autorisations EC2 adaptées aux cas d'utilisation de VPC partagés. Pour plus d'informations, voir les ROSA mises à jour des politiques AWS gérées.	7 août 2025

Mis à jour ROSAImage RegistryOperatorPolicy	Mise à jour de la politique AWS gérée ROSAImage RegistryOperatorPolicy.	19 mai 2025
Mis à jour ROSANodeP oolManagementPolicy	Mise à jour de la politique AWS gérée ROSANodeP oolManagementPolicy .	5 mai 2025
Mis à jour ROSAImage RegistryOperatorPolicy	Mise à jour de la politique AWS gérée ROSAImage RegistryOperatorPolicy.	16 avril 2025
Mis à jour ROSAWorke rInstancePolicy	Mise à jour de la politique AWS gérée ROSAWorke rInstancePolicy.	3 mars 2025
Mis à jour ROSANodeP oolManagementPolicy	Mise à jour de la politique AWS gérée ROSANodeP oolManagementPolicy.	24 février 2025
Mis à jour ROSAAmazo nEBSCSIDriverOperatorPolicy	Mise à jour de la politique AWS gérée ROSAAmazon EBSCSIDriverOperatorPolicy.	17 janvier 2025
ROSA avec extension HCP Région AWS	ROSA avec plans de contrôle hébergés (HCP) est désormais disponible au Moyen-Orient (Émirats arabes unis). Région AWS	13 mai 2024
ROSA avec extension HCP Région AWS	ROSA avec plans de contrôle hébergés (HCP) est désormais disponible en Europe (Paris). Région AWS	6 mai 2024
Mis à jour ROSANodeP oolManagementPolicy	Mise à jour de la politique AWS gérée ROSANodeP oolManagementPolicy.	2 mai 2024

ROSA avec extension HCP Région AWS	ROSA avec plans de contrôle hébergés (HCP) est désormais disponible en Europe (Espagne). Région AWS	29 avril 2024
ROSAInstallerPolitique mise à jour	Mise à jour de la ROSAInstaller politique AWS gérée.	24 avril 2024
ROSA avec extension HCP Région AWS	ROSA avec plans de contrôle hébergés (HCP) est désormais disponible en Europe (Zurich). Région AWS	19 avril 2024
ROSA avec extension HCP Région AWS	ROSA avec plans de contrôle hébergés (HCP) est désormais disponible en Asie-Pacifique (Osaka). Région AWS	17 avril 2024
ROSAInstallerPolitique et ROSASRESupport politique mises à jour	Mise à jour des politiques AWS gérées ROSAInstaller Policy and ROSASRESupport Policy.	10 avril 2024
ROSA avec extension HCP Région AWS	ROSA avec plans de contrôle hébergés (HCP) est désormais disponible en Asie-Pacifique (Hong Kong). Région AWS	8 avril 2024
ROSA avec extension HCP Région AWS	ROSA avec plans de contrôle hébergés (HCP) est désormais disponible en Amérique du Sud (São Paulo). Région AWS	1er avril 2024
ROSA avec extension HCP Région AWS	ROSA avec avions de contrôle hébergés (HCP) est désormais disponible au Moyen-Orient (Bahreïn). Région AWS	25 mars 2024

ROSA avec extension HCP Région AWS	ROSA avec plans de contrôle hébergés (HCP) est désormais disponible en Asie-Pacifique (Séoul). Région AWS	14 mars 2024
ROSA avec extension HCP Région AWS	ROSA avec plans de contrôle hébergés (HCP) est désormais disponible en Afrique (Cape Town). Région AWS	5 mars 2024
ROSAInstallerPolitique mise à jour	Mise à jour de la ROSAInstaller politique AWS gérée.	26 janvier 2024
ROSASRESupportPolitique mise à jour	Mise à jour de la ROSASRESupport politique AWS gérée.	22 janvier 2024
Mis à jour ROSAImage RegistryOperatorPolicy	Mise à jour de la politique AWS gérée ROSAImage RegistryOperatorPolicy.	12 décembre 2023
Mis à jour ROSAKubeController Policy	Mise à jour de la politique AWS gérée ROSAKubeController Policy.	16 octobre 2023
ROSAManageAbonnement mis à jour	Mise à jour de l' ROSAManageabonnement AWS à la politique gérée.	1er août 2023
Mis à jour ROSAKubeController Policy	Mise à jour de la politique AWS gérée ROSAKubeController Policy.	13 juillet 2023
Pages de sécurité ROSA ajoutées	La résilience dans les pages ROSA, la sécurité de l'infrastructure dans ROSA et la protection des données dans les pages ROSA ont été ajoutées.	30 juin 2023

Ajout de la page des options de déploiement	La page des options de déploiement a été ajoutée.	9 juin 2023
Ajout d'une nouvelle politique AWS gérée ROSANode PoolManagementPolicy	Une nouvelle politique AWS gérée ROSANode PoolManagementPolicy a été ajoutée.	8 juin 2023
Ajout d'une nouvelle ROSAInstaller politique AWS gérée	Une nouvelle ROSAInstaller politique AWS gérée a été ajoutée.	6 juin 2023
Ajout d'une nouvelle ROSASRESupport politique AWS gérée	Une nouvelle ROSASRESupport politique AWS gérée a été ajoutée.	1er juin 2023
Ajout d'un aperçu des responsabilités de ROSA	Ajout de la page Aperçu des responsabilités pour ROSA.	26 mai 2023
Mis à jour Qu'est-ce que c'est Red Hat OpenShift Service on AWS ?	Mise à jour de la Red Hat OpenShift Service on AWS page Qu'est-ce que c'est ?	24 mai 2023
Ajout de nouvelles politiques AWS gérées pour les rôles d'opérateur ROSA	De nouvelles politiques AWS gérées ROSAImage RegistryOperatorPolicy ROSAKubeControllerPolicy, et une nouvelle ROSAKMSProvider politique ont été ajoutées.	27 avril 2023
Ajout d'une nouvelle politique AWS gérée ROSAControl PlaneOperatorPolicy	Une nouvelle politique AWS gérée ROSAControl PlaneOperatorPolicy a été ajoutée.	24 avril 2023

Ajout de nouvelles politiques AWS gérées pour les rôles liés aux comptes ROSA	De nouvelles pages de politiques AWS gérées pour le compte ROSA et la page des rôles d'opérateur ont été ajoutées.	20 avril 2023
Ajout de la page des quotas de service ROSA	La page des quotas de service ROSA a été ajoutée.	22 décembre 2022
Pages de résolution des problèmes ajoutées	Des pages de résolution des problèmes ont été ajoutées.	1er novembre 2022
Pages de démarrage ajoutées	Des pages de démarrage ont été ajoutées.	12 août 2022
Ajout d'une nouvelle politique AWS gérée ROSAManage Abonnement	Un nouvel ROSAManage abonnement aux politiques AWS gérées a été ajouté.	11 avril 2022
Première version	La version initiale du guide de l' Red Hat OpenShift Service on AWS utilisateur.	24 mars 2021

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.